SJSU SAN JOSÉ STATE UNIVERSITY

MTI MINETA TRANSPORTATION INSTITUTE

Surface Transportation Supply Chain Security: Creating a Blueprint for Future Research

Frances L. Edwards, MUP, PhD, CEM
Joseph Szyliowicz, PhD
Dan Goodrich, MPA, CEM
William Medigovich, MS
Liz Lange, MPA
Autumn Anderton, MA

MINETA TRANSPORTATION INSTITUTE

Founded in 1991, the Mineta Transportation Institute (MTI), an organized research and training unit in partnership with the Lucas College and Graduate School of Business at San José State University (SJSU), increases mobility for all by improving the safety, efficiency, accessibility, and convenience of our nation's transportation system. Through research, education, workforce development, and technology transfer, we help create a connected world. MTI leads the Mineta Consortium for Transportation Mobility (MCTM) funded by the U.S. Department of Transportation and the California State University Transportation Consortium (CSUTC) funded by the State of California through Senate Bill 1. MTI focuses on three primary responsibilities:

Research

MTI conducts multi-disciplinary research focused on surface transportation that contributes to effective decision making. Research areas include: active transportation; planning and policy; security and counterterrorism; sustainable transportation and land use; transit and passenger rail; transportation engineering; transportation finance; transportation technology; and workforce and labor. MTI research publications undergo expert peer review to ensure the quality of the research.

Education and Workforce Development

To ensure the efficient movement of people and products, we must prepare a new cohort of transportation professionals who are ready to lead a more diverse, inclusive, and equitable transportation industry. To help achieve this, MTI sponsors a suite of workforce development and education opportunities. The Institute supports educational programs offered by the Lucas Graduate School of Business: a Master of Science in Transportation Management, plus graduate certificates that include High-Speed and Intercity Rail Management and Transportation Security Management. These flexible programs offer live online classes so that working transportation professionals can pursue an advanced degree regardless of their location.

Information and Technology Transfer

MTI utilizes a diverse array of dissemination methods and media to ensure research results reach those responsible for managing change. These methods include publication, seminars, workshops, websites, social media, webinars, and other technology transfer mechanisms. Additionally, MTI promotes the availability of completed research to professional organizations and works to integrate the research findings into the graduate education program. MTI's extensive collection of transportation-related publications is integrated into San José State University's world-class Martin Luther King, Jr. Library.

Report 21-06

Surface Transportation Supply Chain Security: Creating a Blueprint for Future Research

Frances L. Edwards, MUP, PhD, CEM
Joseph Szyliowicz, PhD
Dan Goodrich, MPA, CEM
Bill Medigovich, MS
Liz Lange, MPA
Autumn Anderton, MA

March 2021

A publication of the
Mineta Transportation Institute
Created by Congress in 1991

College of Business
San José State University
San José, CA 951920219

TECHNICAL REPORT DOCUMENTATION PAGE

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.	
21-06			
4. Title and Subtitle Surface Transportation Supply Chain Security: Creating a Blueprint for Future Research		**5. Report Date** March 2021 **6. Performing Organization Code**	
7. Authors Frances Edwards, https://orcid.org/0000-0002-0446-5556 Joseph Szyliowicz, https://orcid.org/0000-0001-6120-6000 Dan Goodrich, https://orcid.org/0000-0002-8123-6554 William Medigovich, https://orcid.org/0000-0003-1984-8805 Liz Lange, https://orcid.org/0000-0001-5308-770X Autumn Anderton		**8. Performing Organization Report** CA-MTI-1937	
9. Performing Organization Name and Address Mineta Transportation Institute College of Business, San José State University San José, CA 95192-0219		**10. Work Unit No.** **11. Contract or Grant No.** 69A3551747127	
12. Sponsoring Agency Name and Address U.S. Department of Transportation Office of the Assistant Secretary for Research and Technology University Transportation Centers Program 1200 New Jersey Avenue, SE Washington, DC 20590		**13. Type of Report and Period Covered** Final Report **14. Sponsoring Agency Code**	
15. Supplemental Notes DOI: 10.31979/mti.2021.1937			
16. Abstract Ninety percent of the world's trade goods travel by surface transportation, using maritime, road and rail assets. The security of the goods in transit, the infrastructure supporting the movement, and the vehicles, are required to ensure that international commerce proceeds successfully. Much has been written about the surface supply chain itself, but little has focused on the security of these components. This report provides a guide for those wanting an increased understand-ing of the security issues that supply chain surface transportation systems confront and a blueprint to guide their future research.			
17. Key Words Cargo security, Intermodal transportation, Multimodal transportation, Security measures, Supply chain management	**18. Distribution Statement** No restrictions. This document is available to the public through The National Technical Information Service, Springfield, VA 22161		
19. Security Classif. (of this report) Unclassified	**20. Security Classif. (of this page)** Unclassified	**21. No. of Pages** 133	**22. Price**

Form DOT F 1700.7 (8-72)

DOI: 10.31979/mti.2021.1937

Mineta Transportation Institute
College of Business
San José State University
San José, CA 95192-0219

Tel: (408) 924-7560
Fax: (408) 924-7565
Email: mineta-institute@sjsu.edu

transweb.sjsu.edu/research/1937

ACKNOWLEDGMENTS

In the spring of 2019, Dr. Karen Philbrick agreed to support this novel research, which is designed to create a blueprint and resources for other researchers to use as a basis for their own work. Without her vision and guidance, this work would not have been possible. The authors are forever in her debt.

Ash Padwal, P.E., J.D., Chief Risk Officer for Allied Telesis, Inc., hosted the workshop at the company's San José headquarters, and provided the presentation on cybersecurity issues in surface transportation supply chain management. We are deeply grateful for the gracious hospitality and support that he provided, without which the workshop would not have been possible.

The only way to develop a blueprint for further truly useful research is to consult the experts in the field, those whose professional practice involves the management of the intricate system that makes up the global surface supply chain, and who deeply understand its need for security. Using their extensive professional networks, the authors assembled a workshop based on Skulmoski, Hartman and Krahn's[1] approach to the Delphi method. Experts from the US Coast Guard, US Department of Transportation (retired), the European Union, the California Department of Transportation, the California Office of Emergency Services, Matson Lines, Allied Telesis and the Mineta Transportation Institute joined the authors for two days of presentations and discussions. The information that was shared formed the basis for the blueprint for further research in surface transportation supply chain security that is part of this report. The authors are most grateful for their generous sharing of their time and expertise. Their biographies are found in Appendix B.

The Mineta Transportation Institute was the direct sponsor of the project. We are grateful to Research Director Dr. Hilary Nixon, who provided support for the creation of the report. Thanks also to the MTI staff for their assistance with the workshop and the publication of this report.

CONTENTS

LIST OF FIGURES

List of Tables

Executive Summary

Ninety percent of the world's trade goods travel by surface transportation, using maritime, road and rail assets.[2] The security of the goods in transit, the infrastructure supporting the movement, and the vehicles are all required to ensure that international commerce proceeds successfully. The criticality of the global supply chains to the economies of most nations makes their study essential, yet to date, the focus has been on individual modes of transportation. But today's large container ships, complex port operations and carefully choreographed forward movement of the cargo require a more integrated approach to understanding how to improve the security of the surface transportation supply chain.

Much has been written about the surface supply chain itself and the need for security and resiliency, but little has focused on the security of the integrated components of the system. Ports with super cranes that time the arrival of trucks and the dispersal of goods require less than an hour in a port, making it impossible to x-ray or inspect every container. Efficiency has the potential to weaken security steps in surface transportation supply chain management, yet ending human trafficking, drug trafficking and inventory shrinkage during movement from producer to consumer also requires new technologies and approaches to ensure security. Numerous global factors, ranging from geo-political conflicts to climate change, are creating new challenges. The melting of the Arctic Ocean's ice sheets, for example, is opening up new trade routes through treacherous waters, involving mineral extraction activities that threaten the pristine environment.

While these potentials for interference are just new and more sophisticated versions of long-standing trade challenges, the introduction of information technology into the integral operation of the vehicles in the supply chain poses novel challenges. Mega container ships with over 20,000 TEUs are navigated using global positioning systems (GPS) and cyber-based charts. Hacking, spoofing and malware are new security challenges not experienced when navigation used paper charts and the stars. Many of the ship's systems are cyber-based and may be vulnerable to attack through crew members charging their cell phones or playing games at sea. Super-cranes use cyber-based management to organize containers to move from cargo vessel to trucks with maximum efficiency, adding a cyber vulnerability to container tracking systems. Chinese introduction of a new version of GPS in June of 2020 has the potential to greatly enhance the complexity of navigation.

Terrorism influences decisions about which ships will be allowed in which ports, the types of licensing and training that the crew members must have, and the routes that ships take. Pirates in the Straits of Malacca and along the Somali coast continue a long tradition of sea-borne thieves, creating a rationale for a Chinese Maritime Silk Road system of ports that can accommodate both commercial vessels and military vessels, such as destroyers. Modern cruise ship and container ship berths can hold small aircraft carriers.

The Delphi workshop revealed these and other challenges that require new approaches to security, not as individual issues but as the integrated space in which the global supply chain operates. A blueprint was developed from the workshop deliberations to encourage transportation researchers to undertake these essential areas. It is hoped that it will serve as a useful guide to the development of proposals for public and private funding sources, for projects that will enhance the global supply chain's security, and the economic security of the manufacturers and consumers that rely on it.

I. Introduction

The global economy relies on surface transportation for its supply chain. A supply chain is "the socio-technical network that identifies, targets, and fulfills demand. It is the process of deciding what, when, and how much should move to where."[3] A review of the scholarly literature suggests that while surface supply chain security has been studied as an economic and risk management (insurance) challenge, the integration of the transportation mechanisms, and their role in security, is often overlooked. Raw materials get moved to factories, and finished products get moved to consumers, using surface transportation assets of trucks, trains and ships. While air cargo is an important element in the movement of valuable goods, most of the world's cargo moves on the surface for economic reasons, so this research will not address air cargo.

More needs to be understood about how the surface transportation infrastructure can be made secure in the evolving realities of Arctic Ocean melting, Chinese Belt and Road initiatives, and cyber networks' role. More recently, the significance of a pandemic for global supply chain security became clear as nations competed for medical protective equipment, ventilators and chemical components for pharmaceuticals and viral test kit reagents.

This project aligns with the Mineta Transportation Institute's two Research Emphasis Areas, as follows:

- Safety and security of transportation systems
- Intermodal connectivity and integration

This research focused on the multiple modal relationships (usually labelled as intermodal and multi-modal) that form the international surface transportation-based supply chains in order to look at ways to enhance the security of all elements of the system as goods pass through it. With the international focus on climate change and sustainability, the newer term synchromodal is also being used.

Table 1. Supply Chain Definitions

Type	Definition
Intermodal	The movement of freight from origin to destination, involving the transfer from one mode of transport to another, without handling the goods, characterized by separate ticketing or contract for each mode; also used to refer to containerized rail transportation. This mode is largely dependent on rail and maritime due to economies of scale.
Multimodal	The movement of freight from origin to destination, involving the transfer from one mode of transport to another, without handling the goods, using one contract for the whole trip; requiring integration between carriers and terminal operators.
Synchromodal	"The best possible combination of transport modes is selected for each trip…to minimize cost, delay and CO2 emissions" (Mes and Iacob); "…synchromodal transport aims at the integration and cooperation among transport services and modes" (Zhang and Pel). This mode is generally facilitated by information technology systems.

Sources: Rodrigue and Slack, 2020; Mes and Iacob, 2016; Zhang and Pel, 2015.

Thus, it addresses multiple US Department of Transportation (US DOT) surface modal research priorities, including highway, motor carrier, railroad and maritime.

However, the US DOT focuses on the functionality of the transportation vehicle and its communication links in most of its research initiatives, rather than on the interconnectedness of the system. Furthermore, issues related to the security of the goods in transit are not addressed. This research focuses on the security of the whole system: the asset being moved (cargo), the asset doing the moving (truck, train, cargo containers, ship), the asset in which the move is occurring (port, warehouse), the route that is used, and the security implications for each dimension: truck/port/ship/cargo/route. Security is viewed in this multi-dimensional frame.

Security analysis frames the question of transportation's role in supply chain security by examining issues of likelihood of disruption, frequency of disruption, vulnerability when disruption occurs, and steps that can be taken to address each vulnerability and prevent or lessen its impact.

Research Questions:

1. What is the scope of existing knowledge in the field? What is the background and current state of the research in supply chain security's transportation dimension? What work has been completed by existing transportation and supply chain scholars and organizations, and published in either peer reviewed or professional journals? (Bibliography)
2. What are the current issues in the practice of surface transportation supply chain security (STSCS) that need additional research and development? What is transportation's role in supply chain security, protecting all elements of the chain from technological and human-caused hazards? (Workshop)

3. What practical measures can be adopted by operators and government agencies in order to enhance the future security and resilience of STSCS? (Blueprint)

II. Background

2.1 Supply Chain Research

At no time (except for the two world wars) have supply chains been subjected to such challenges as are evident today. It is increasingly obvious that the global environment that emerged in recent decades and facilitated the creation of global supply chain networks is undergoing significant changes, changes that are impacting their transportation systems. These are the essential components that enable supply chains to operate nationally and internationally. They constitute the physical link between all the components in any supply chain since raw materials are shipped to one or more production facilities from where the output is shipped to other nodes and ultimately to a consumer. Any disruption in any part of these systems has implications not only for the specific supply chain but for national economies as well. The prosperity of the United States (US), indeed its security, is dependent upon their effective and efficient functioning.

The central role of transportation and its associated systems in achieving and maintaining a high level of supply chain security has been clearly recognized by the US government, whose "National Strategy for Global Supply Chain Security" states: "our focus… is the worldwide network of transportation, postal, and shipping pathways, assets, and infrastructures by which goods are moved from the point of manufacture until they reach an end consumer, as well as supporting communications infrastructure and systems."[4]

Numerous potentially disruptive factors to the existing global supply chain system can be identified, ranging from shifts in the political and economic balance of power, the rise of non-state actors, including those who engage in criminal and terrorist activity, the emergence of new political and economic powers and groupings, the continuing development and global dissemination of information and other technologies and such environmental factors as climate change.

2.2 Frameworks and Focus

Supply Chain

The globalization of the economy has created new risks for surface transportation supply chain security (STSCS). Components of products are created in multiple locations, often in multiple nations, and have to be moved to a location for assembly, then along a different supply chain for delivery to the consumer sector, which can include another long distribution system. These long supply chains depend on a variety of transportation modes, facilities and systems, each of which offers an opportunity for tampering, criminal enterprise and terrorist activity.

In 1999 Lummus and Vokurka defined a supply chain as "a term increasingly used by logistics professionals—encompasses every effort involved in producing and delivering a final product, from the supplier's supplier to the customer's customer."[5] Mentzer, DeWitt, Keebler et al. noted in 2011 that a consensus definition of supply chain is critical before managing its elements can be

undertaken. One suggestion is "several independent firms involved…in manufacturing a product and placing it in the hands of the end user…raw materials and components producers, product assemblers, wholesalers, retail merchants and transportation companies."[6]

The global impact of supply chains was forcefully demonstrated by the Hanshin-Awaji earthquake in Japan in 1995, when the impact of the earthquake made it impossible to ship the car brakes from metropolitan Kobe, closing down Toyota automobile assembly lines in South America.[7] The world's supply of lighted electronic diode (LED) lights used in appliances, electronics and automobiles was also made in the Kobe area, and the shipments were delayed for weeks, holding up production lines around the world.[8] In both cases, the supply chain was damaged due to the loss of the relatively new port facility in Kobe that experienced liquefaction, resulting in the quays sinking and the large gantry cranes subsiding into the bay. The potential alternative supply chain segment—by road to the Port of Yokohama—was also lost when the Hanshin Expressway fell over 90 degrees due to lack of sheer strength in the supports.[9]

Business literature describes the role of supply chains in the provision of goods around the world, while this research focuses on one aspect of supply chains: the security of the surface transportation system moving raw materials to finished products.

Surface Transportation

Surface transportation includes multiple modes. Water transportation supply chain elements include ports, harbor pilots, cranes, cargo containers and various types of ships and barges. Land transportation supply chain elements include trucks, terminals, roads and bridges, fuel and repair facilities, and traffic control devices. Rail transportation supply chain elements include freight depots, railroad infrastructure and signals. Ancillary systems include warehouses and customs facilities, and information technology applications including SCADA systems, maritime navigation, communications across the modes, and scheduling programs to achieve synchronous modal goods movement.

These work in concert to move goods from the raw materials' source to the manufacturing point, to the port, onto the ship. At the receiving port, goods are transferred to rail or truck for further delivery to wholesalers and retailers,[10] or to the other end of the US "land bridge"[11] connecting cargo from China to consumers in Europe. Cargo is loaded onto another ship in an East Coast port bound for European ports.[12] All these cargo transfers occur without the finished goods being handled except as a sealed container, eliminating the need for stevedores at the port and inventory "shrinkage" through loss and theft at intervening transfer points.

Definitions of Security

Workshop participants noted that in many languages, safety and security are expressed by the same word, yet there is a distinct difference between the two concepts. Safety relates to the prevention of accidental damage to an asset. Accidents can be studied to understand which system failed or

what misjudgment was made by a human in the use or operation of a device, system or vehicle, and training or redesign can be implemented to prevent a repetition of the accident in the future.

Security, on the other hand, involves protecting something valuable from any form of deliberate interference, usually requiring a physical response to an external conscious threat, whether technological or human caused.[13] Security systems may be established to respond to a loss of the power source, loss of cyber services, crime, or terrorism. Security must also be ready to respond to the impact of pandemics on supply chains, including the disruption of the supply chain through workers' illness or through quarantine orders, leaving valuable goods unattended in unprotected places,[14] creating vulnerabilities that may be exploited.

The Transportation Security Administration (TSA) set up a system of capturing raw threats via the trucking industry using State Threat Assessment Centers as gathering points for threats. Thousands of reports are generated every year from the transportation sectors. The Intermodal Security Training and Exercise Program (I-Step) has involved more than 3,345 participants "from the nation's mass transit, freight rail, highway, and pipeline sectors,"[15] but their focus has been more on homeland security and counter-terrorism than intermodal vulnerabilities in the systems themselves.

Currently, the drug cartels in Northern Mexico are using a river model to smuggle drugs across the border. They break the shipment down into 10 to 15-kilo loads rather than larger consignments that would have a greater impact on their operation if intercepted. With this disbursed model, shipments that are seized have a small or insignificant impact on their operations. As such, their primary concern, from a security perspective, is the interception of this river of drugs by a rival group. Since something else is being used as the cover to smuggle their cargo, that item falls under the protection of the cartel by default, meaning that security for certain vehicles is covered by not only law enforcement but also criminal enterprise.

Access to surface transportation routes, lines and ports is critical for the elements of the supply chain. Goods need to move through the supply chain with as few impediments as possible. Supply chain management is focused on keeping down the time and cost of goods movement and minimizing the release of greenhouse gasses (GHG), each of which creates an argument against barriers within the supply chain. However, inspections of goods and bills of lading, and sampling contents of containers, may be required to meet national customs requirements, prevent human trafficking and deter drug transportation. Each barrier and inspection adds time to the supply chain, and potentially adds cost and GHG emissions.[16]

New Elements of STSCS

China's "Belt and Road" project is explicitly designed to develop new trade routes and economic spheres of influence to challenge existing economic patterns, which have been traditionally centered around the US, the European Union (EU), and Japan. Its two dimensions, one designed to enhance transportation from China across Central Asia to Europe, the other developing port

and related infrastructure to create new maritime routes, represent the largest and costliest investments and infrastructure development in history and ranges across Asia, Europe, Africa, the Middle East, and the Americas.[17]

This infrastructure-building plan includes the construction of new trade routes and resources in areas not currently served or needing enhancements. Examples include a new Maritime Silk Road that would connect China to the Mediterranean Sea through a series of new or enhanced ports, an enhanced rail line that connects China to Europe through connections in Kazakhstan, Poland and into Spain, and road and rail construction projects across the Eastern Hemisphere. In some cases, the partnerships are joint ventures, while in other cases, the receiving nation borrows funds from China and uses the funds to pay Chinese enterprises to build the facilities. Particular concern has been raised about South Pacific island nations that have borrowed large amounts that they may be unable to repay.[18]

Melting of the Arctic Ocean's ice has permitted Russia to open areas of its north shore to extraction industries and allowed for the passage of a container ship for several months each summer. There are concerns about the use of the Bering Strait, the only access from the Pacific Ocean to the Arctic Ocean, for increased commercial shipping, due to its narrow passages. The Arctic Sea is rough, and even when there is open water, there is also sea ice, requiring the presence of ice pilots on ships transiting the area.[19] Environmentalists worry that accidents could result in fuel spills leading to pollution in an area that is difficult to access and with limited rescue capacity.[20]

Information technology (IT) is being applied to all aspects of the surface transportation supply chain, pointing out the need for enhanced cybersecurity for the supply chain enterprise. IT has long been a staple in transportation management, from supervisory control and data acquisition (SCACA) systems that run the railroads to enterprise-wide systems that schedule port calls and freight forwarding, to communications systems such as voice over internet protocol (VOIP), email and signaling operations, and geographical positioning systems (GPS) that geo-locate vehicles on their routes and navigate ships at sea. Every one of these systems is potentially subject to hacking by hostile actors, disrupting economies, and even endangering lives.[21] Technology is impacting an increasingly wide range of transportation operations, such as enabling super cranes in ports,[22] but every technological advance based on cyber-based functionalities also opens the door for hacking, damage and ransomware attacks.[23]

Most recently, the COVID-19 pandemic has demonstrated the damage that can be done to the supply chain's security, as port terminals are shuttered, leaving empty containers and chassis in warehouses instead of being shipped back to Asia. Illness in China caused a major slowdown in factory production, leading to the cancellation of sailings to the US ports, causing unemployment throughout the US portion of the supply chain's transportation sector.[24] Tires on the deck of a ship sailing from Africa to the US east coast are believed to have unwittingly imported mosquitoes carrying infectious diseases that were new to the Western Hemisphere, such as Zika.[25] All of these events point to a need for enhanced security for the idled infrastructure, to ensure that it is not

tampered with or stolen and ready for the anticipated resurgence in business when COVID-19 is overcome,[26] and for vigilance in the operation of the supply chain.

2.3 Research on Transportation Supply Chain Security

Considerable research and implementation work has already been undertaken on aspects of supply chain security with a nexus to transportation. For example, a chronological collection of some current relevant works from the Transportation Research Board's Transportation Research Database (TRID) is found in Table 2. However, most focus on just one mode, such as maritime, or look at one security issue across multiple modes, such as prevention of tampering.

Table 2. Chronological Examples of Related Scholarly Articles from TRID

Scenario analysis and disaster preparedness for port and maritime logistics risk management. 2019. Kwesi-Buor, John, Menachof, David A., and Talas, Risto. Accident Analysis & Prevention, Volume 123, Issue 0, 2019, pp. 433–447. http://www.sciencedirect.com/science/article/pii/S0001457516302421
Utilization Rate as a Resilience Index for Supply Chain Networks, 2019. Al Hajj Hassan, Lama, Chen, Ying, Mahmassani, Hani S. Transportation Research Board 98th Annual Meeting, 2019, 10p.
Risk and Failure Resilience of Interdependent Transportation Systems, 2018, Yodo, Nita, Wang, Pingfeng, Krishnan, Krishna, and Twomey, Janet. https://rosap.ntl.bts.gov/view/dot/36552
The Use of Violence in Cargo Theft: A Supply Chain Disruption Case. 2018. Ekwall, Daniel, and Lantz, Björn. Journal of Transportation Security, Volume 11, Issue 1–2, 2018, pp 3–21.
Next steps for CTPAT: CBP's post-9/11 supply chain security program is ready for an update, but industry remains concerned about implementing changes. Caldwell, Stephen L. American Shipper, 2018, pp. 30–35
Security of Air Cargo Shipments, Operations, and Facilities. 2018. Elias, Bart. Congressional Research Service, Washington, DC United States
Exploring Blockchain - Technology Behind Bitcoin and Implications for Transforming Transportation, 2018, Rajbhandari, Rajat. Texas A&M Transportation Institute. https://rosap.ntl.bts.gov/view/dot/34863

Source: Transportation Research Board, 2020. TRID. Retrieved from trid.trb.org

Research into the supply chain management literature revealed that over 40,000 books and articles had been published between 1982 and 2015. Yet, only one of the popular supply chain management textbooks dealt with transportation as a "promising future research area" in the supply chain's security, sustainability, risk or disruption studies.[27] In the field of supply chain risk management, there were 143 articles published between 2003 and 2013, yet only one article dealt with transportation.[28]

International scholars have created volumes that focus on supply chain risks and the security issues confronting transportation systems. Zamparini and Szyliowicz,[29] for example, have co-edited and co-authored three volumes that look at how different nations deal with maritime, aviation and multimodal security issues. The Mineta Transportation Institute workshop[30] that brought together academics, security officials and supply chain professionals considered how the rapidly changing

global environment impacts the security of surface transportation supply chain systems. This is a topic that is receiving increasing academic attention. Recently, a group of international academics presented papers on various dimensions of this topic at the University of Salentino, and in Sweden, Per Hilletofth (Jonkoping University), organized a special session entitled "Next Generation Intermodal Transportation Systems" at the 9th International Conference on Operations and Supply Chain Management in December 2019 in Vietnam.[31]

Yet, macro risks to surface transportation supply chain management exist in a number of spheres. At the geo-political level, nationalism and populism are clearly playing an increasing role in the politics of many nations, as evidenced by the United Kingdom's decision to exit the EU, leading to the need to create a 27-acre truck parking facility in Kent to process the 215 million customs declarations that will be required for cross-border transport of good from the European Union, at the cost of 7 billion British Pounds.[32] Another example is the "America First" policies advocated by the American President, as exemplified by the rejection of the Trans Pacific Partnership (TPP) and the new patterns of economic relations with China and other states.[33] The implications of these developments for existing trade patterns are not only being widely discussed but are already leading to changes within the global trading system as countries—and companies—seek to adjust to this new environment.

Furthermore, the power balance is changing as new economic powers have been emerging, including Brazil, India and China. As a result, new trade patterns are developing—and will continue to develop—with obvious implications for the location and structure of supply chains. These developments will be spurred by the policies regarding their transportation infrastructure that some countries are considering or have already adopted. Panama, for example, recently completed its expansion of the canal. Nicaragua is still considering the possibility of building a rival canal, and many African states are exploring ways to expand and integrate their railroad systems.[34] Nor can one overlook the problems caused by the ongoing conflicts in the Middle East and elsewhere, which pose obvious security challenges in the form of terrorism and piracy.

At the environmental level, climate change is already an important factor. It has affected the production of various agricultural products throughout the world, threatens the functioning of some ports through sea level rises, and the melting Arctic Ocean's ice sheet is reopening the fabled Northwest Passage between Europe and Asia.

Business writers credit a major earthquake in Japan in March of 2011 and flooding in Thailand at the end of 2011 for increasing the interest of globalized firms in understanding and assessing threats of losses to their supply chains. Supply chain impacts were estimated at $300 billion for the earthquake and $50 billion from the floods, with significant supply chain disruption.[35] Zurich Global Insurance surveyed its customers and discovered that 85% had experienced some supply chain disruption in 2011, with 50% reporting more than one disruption. Factors driving this experience included the "globalized nature of the supply chain, just-in-time inventory management, consolidation of vendors through strategic sourcing activities, and overall geo-

political changes."[36] All of these involve some role for transportation, yet transportation is never mentioned.

2.4 Bibliographic Research on Transportation Security

This research has developed a bibliography of current academic and related works to support an understanding of transportation's role in the supply chain security effort in order to provide a more comprehensive look at the interactions of goods, mode, modal interface and routes. It contains 113 works, of which 31% address the maritime sector, 8% address land transportation, and 53% address general transportation. Ships are the focus of 27% of the literature, 8% focus on land vehicles, 2% are about trains, and 4% are about trucks.

Security and risk assessments are a central focus for 65% of the articles, while 35% consider that these are management issues; 43% of the articles consider risk a high concern, 8% a moderate concern, 18% only a low concern, and 38% suggest that risk varies over time. It is notable that interest in external threats and vulnerabilities of the supply chain has risen over time, with interest developing in 2012 and accelerating after 2017.

The bibliography also reveals how the literature considers the variety of risk factors that can impact supply chain transportation systems. While 14% of threats to supply chain security come from organizational sources such as globalization and just-in-time management (listed above), 23% are from the threat of terrorist attack, 13% from natural disasters, 9% from geo-political factors, and 12% from crime and piracy. These and other findings are discussed in detail below in the section entitled "Bibliography Development and Literature Review."

One strategy for defeating criminal enterprise and terrorism is to understand how the potential perpetrators think. To this end, an additional bibliography of adversary literature was developed to inform researchers of the challenges to security plans and systems. This second bibliography includes the open source materials created by and about former criminals, national government agencies and terrorist organizations. It, too, is discussed in detail below.

2.5 Challenges to STSCS

New Economic Actors

The globalization of the economy has created a variety of new challenges for STSCS. While China's role in the world economy has grown significantly, Brazil, India and Vietnam have grown in economic importance internationally. The latest World Bank report shows the US with a $20 trillion GDP economy, China in second place with $13 trillion, India at #7 with $2.7 trillion, and Brazil at #9 with $1.8 trillion. Vietnam has breached the top 50 economies barrier (out of over 200 that are rated), at #46 with $2.5 billion.[37] It is notable that the balance of GDP has shifted regionally as well. The world economy was at $86 trillion in 2018, with the Asian Pacific region in the lead at $25.9 trillion through the powerhouse economies of China (#2), Japan (#3), and South Korea (#12), along with other smaller nations. Europe and Central Asia are at $23 trillion,

with Germany (#4), the United Kingdom (#5) and France (#6), Italy (#8) and the Russian Federation (#11) leading the region. North America is third with $22 trillion, including the US (#1), Canada (#10) and Mexico (#15) as the partners.[38]

This level of economic activity is based on globalized trade. In 2018 the US imported $539 billion in goods from China (#2 GDP), $142 billion from Japan (#3 GDP), $74 billion from South Korea (#12 GDP), and $49 billion from Vietnam (#49), among its larger trading partners, and all with a negative imbalance of trade. On a worldwide basis, in 2018, the US imported $2.5 trillion and exported $1.6 trillion in goods,[39] causing the US Chamber of Commerce to note that many of the 11 million cargo containers unloaded in US ports each year return to China empty.[40] Of the top ten busiest ports in the world, five, including Shanghai (#1), are in China, with Singapore #2, Hong Kong #5, Busan, Korea #6, and Dubai #9. Shanghai handles 37.17 million twenty-foot equivalent units (TEUs) each year,[41] while the largest port in the US is Los Angeles, handling 8.8 million TEUs, followed by Long Beach with 6.77 million TEUs annually. East Asian trade accounts for 90% of the cargo passing through Long Beach.[42]

China has initiatives to enhance its position as a worldwide trading partner. In 2010 it launched an initiative called "Made in China 2025" aimed at expanding its economic reach. The plan specifies "ten sectors, including aerospace, new materials and agricultural equipment," with development supported by "state guided funds," essentially subsidies that are illegal under World Trade Organization (WTO) rules.[43]

New Technologies

Technology continues to produce and disseminate new products, ranging from drones to autonomous and connected vehicles to data technologies that will probably impact existing supply chains and their transportation systems to an even greater degree than the container revolution did a few decades ago. While these technologies are in various stages of development and use, there is little doubt that they already have impacted and will continue to impact, the existing legal, regulatory, and security environments. Indeed, the consequences for transportation security are already widely felt, as cyber-attacks against supply chain and transportation companies have become commonplace, and cybersecurity has become a major national concern.

A variety of new transportation technologies are being introduced into the STSCS environment. Some, such as the cyber-enabled high-speed gantry cranes at ports, have cut down on GHG emissions through better management of goods movements. The cyber system permits the crane operator to "groom" the cargo on the ship to create the most efficient supply chain, enabling trucks to be loaded and released in under one hour.[44] New hull designs and the use of hybrid propulsion systems can reduce GHG emissions in ships, and new fuels such as biofuel, liquefied natural gas (LNG) and hydrogen are cleaner fuels than traditional bunker oil. The increase in ship capacity also lowers the emissions per TEU, which is important as the quantity of containers shipped annually continues to grow.[45] These changes may contribute to STSCS by creating quicker and

less polluting trips, but the new fuels could instead provide new challenges securing the new fuel sources.

Trucks carry more than 70% of America's freight.[46] They collect containers at ports and drop them off at railheads, warehouses, depots, or carry the goods to the factory. Self-driving trucks are on the horizon, with test drives having begun in March 2020. Locomotion, a self-driving truck firm, organizes their vehicles to drive in convoys, limiting the impact on other drivers. The first test drives carried freight between Oregon and Idaho for 400 miles. A human drives the lead truck, and cameras, lidar and radar keep the following trucks in their lane.[47] The trucking industry has suffered a driver shortage since 2003. Convoyed trucks with one human driver could double the capacity that one driver can manage. California has already issued 65 Autonomous Vehicle Testing Licenses to trucking companies, and an autonomous truck drove 2,800 miles in 41 hours from Tulare, California, to Quakertown, Pennsylvania, with a load of 41,000 pounds of butter in time for Thanksgiving.[48]

New Trade Routes

US Land Bridge

In 1972 the maritime industry led the development of the "land bridge" concept in the United States. Goods were placed in sealed cargo containers, shipped across the Pacific Ocean to US west coast ports, the container was off-loaded and placed on a train (or sometimes truck), travelled across the US to an east coast port, and the container was placed on another cargo container ship to sail to a European port, all without ever being emptied. Companies such as Seatrains Lines, Inc. pioneered the use of multimodal trips across land rather than through an all-maritime route through a canal or around the ends of a continent, saving time and money. Southern Pacific Railroad developed the double-decked rail car to carry the containers. The land bridge cut three or four days from the 21-day trip from Asian to US east coast ports. In the first five years of operation, "the flow of internationalized freight across U.S. rails has risen 350%."[49] By 2018, "at least 42 percent of the carloads and intermodal units railroads carry, and more than 35 percent of rail revenue, are directly associated with international trade."[50]

The multimodal approach to cargo movement has generated a new generation of large container ships called New Panamax, which are able to travel through the enhanced locks of the Panama Canal. A Panamax ship carried 5,000 twenty-foot equivalent units (TEU), while the New Panamax ships carry 13,000 TEUs. By 2012 the Triple E ship of Maersk Lines was carrying 18,000 TEUs, and the planned MalaccaMax will carry 30,000 containers and barely clear the confines of the Straits of Malacca's shipping lane. The largest ship in service is the Maersk Gulsun, which carries 23,756 TEUs, and its draft is 50 feet.[51] Its containers will fill three one-mile-long trains. Demand for these ever-growing container ship designs is driven by "the volume of goods produced in Asia and consumed in Europe and the US."[52]

To serve these large ships and speed the movement of cargo, new high-speed cranes have been developed with the capacity to lift two containers at once and to reach 22 containers across a vessel. The container management system uses software that integrates the crane and the vehicle receiving the shipment to enhance speed, with one port in Virginia reporting that 80% of its trucks picking up containerized imports are loaded in less than one hour. Rail loading is similarly speeded up.[53]

China's One Belt, One Road

The "historic" routes of the twentieth century put US ports on both coasts at the center of world trade. In February of 2020 *The Economist* noted that "China's flagship foreign policy is a way to put itself in the center again."[54] The plan launched in 2013,[55] known as One Belt, One Road, includes new rail lines, new and improved roads, and new ports around the world.[56] The name is meant to evoke images of the famous Silk Road from China to Europe, the trade route that carried Marco Polo. One focus of the policy is to develop a trans-continental set of connections between China and its European customers with no water element in the supply chain. Called the New European Land Bridge, it runs 7,500 miles from China to Duisberg[57] and Madrid, the longest rail route "in the history of the world."[58] In 2018 the rail links carried 4,000 trains per year westward with 350,000 containers,[59] part of the New Silk Road economic belt. The Maritime Silk Road runs to Africa and into the Mediterranean Sea. *Forbes* notes that the rail trip is expensive and takes two weeks of rough riding for cargo to arrive in Europe. The trains currently carry only 100,000 TEUs per year, four days' worth of Shanghai's shipping capacity. So it is clear that this part of the One Belt, One Road program is political, not economic.[60]

China's worldwide One Belt, One Road policy includes investments in many nations' transportation infrastructure. A map in *The Economist* showed that most of the Eastern Hemisphere's nations have signed on for some aspect of the One Belt, One Road infrastructure development program.[61] A number of European nations have given Chinese firms contracts "to set up and operate in their national port, logistics and rail infrastructure…Under the BRI, Chinese businesses, mostly state-owned, have built, acquired or been awarded maritime and rail infrastructure concessions in the main commercial transit points."[62] In 2019, 25 million cargo containers traveled from Asia to Europe, the third-largest cargo route in the world.[63] Concerns have been raised about China's port development investments in small Pacific island nations, putting them into debt that they are unlikely to be able to repay. International financial experts are concerned that, on default, China will take back control of the port, opening new opportunities for Chinese naval bases across the Pacific. Chinese companies already control services in 61 ports around the world. The 150-year-old Chinese Merchants Group runs 38 ports in 18 countries. It is notable that China has invested $20 billion in foreign ports.[64] Notably, either COSCO, a major Chinese shipping firm or the Chinese Merchants Group "manage port terminals around the world's five most important straits: Malacca, Hormuz, Gibraltar, Suez and Panama."[65]

While these investments and improvements make sense for a maritime trading power, the Chinese ownership poses security challenges for US agencies monitoring supply chain security overseas.

The ports are also a focus of military concern, as they offer options for projecting Chinese sea power across the world. The Straits of Malacca, long patrolled by the US Navy's 7th Fleet, are the crossroads of the world's oil route from the Middle Eastern oil producers to the Asian powerhouse economies, including 80% of Chinese oil. Nearly one-third of all maritime trades pass through the straits each year.[66] The need for enhanced supply chain security amidst the changing political dynamics of trade is clear.

The Melting Arctic

Another factor in the development of new trade routes is the opening of the fabled Northwest Passage from Europe to Asia. As climate change evolves, rising temperatures have opened the Arctic Ocean to shipping, with the Maersk Venta container ship sailing from Vladivostok in far eastern Russia on the Sea of Japan to Bremerhaven in Germany. The ship's transit included traveling through the Bering Strait between Russia and Alaska into the Arctic Ocean, marking a new route for container ship travel. The 23-day voyage westward across Russia's northern shore took place from August to September 2018, as the sea lanes in the Arctic Ocean are currently only clear from July through October.[67] Another landmark journey was made in the summer of 2016 by the luxury cruise ship *Crystal Serenity*, which sailed for 32 days from Seward, Alaska, eastward to New York City through the Arctic Ocean along the Alaskan and Canadian shores.[68] The opening of Arctic Sea routes will create both new competition for control of the northern waterways and also lead to overlapping national claims of sovereignty in the 200-mile exclusive economic zone under the United Nations' Law of the Sea Convention of 1982,[69] which came into force in 1994. Conservationists worry that the presence of floating sea ice and rough seas may lead to maritime accidents and ecological disasters.[70]

The Bering Strait is only 55 miles wide at its narrowest point, with depths ranging from 98 to 164 feet. The waterway also has a number of islands that complicate navigation. At the Diomedes Islands, the US and Russia are only five miles apart.[71] A PanaMax container ship has a draft of about 40 feet, while a New PanaMax has a draft of about 50 feet, leaving little room for error in navigating around islands. With the Russian interest in opening their northern shore for commercial development, the strait could become congested with commercial shipping. Managing the strait could become a challenge for the US Coast Guard and create STSCS challenges. Russia is developing its north shore for extraction activities, with plans to create logistics support at the Murmansk end of the Northern Sea Route, connecting its Far East to its western outlet into the Atlantic Ocean. In 2020, plans were developed for the creation of a new logistics support community at the Atlantic Ocean end, separate from the Murmansk Naval Base area.[72]

Sustainability

A critical element of all supply chains is the need for sustainability. In 2016 the UN noted that "supply chain sustainability can no longer be ignored."[73] Customers must be able to rely on the delivery of parts and products to maintain their businesses and perhaps even their own link in the supply chain. FEMA provides guidance on developing supply chain sustainability, focusing on the

role of supply chains as lifelines for communities. Transportation is acknowledged as "enabling the movement of goods and services" and supporting all other community lifelines.[74]

In the FEMA context, STSCS is threatened by natural hazards that damage or destroy the infrastructure on which the supply chain transportation depends, as noted in Kobe, Japan, after the 1995 earthquake.[75] Earthquakes, hurricanes and tsunamis all offer examples of significant disruption of transportation systems. From a security perspective, tampering, criminal enterprise, and terrorist activity during natural hazards events challenge security plan implementation. From the UN perspective, the partners in the supply chain should develop a resilience plan to ensure that their ability to produce the product continues, regardless of externalities. An element of resilience plans is: "understands and adapts to external factors that may impact a company's ability to produce a product or deliver a service."[76] So from a security perspective, this requires systems that can withstand natural, technological and human-caused disasters and still keep the cargo, container, vessel, port, road, rail and depot functional when the event has abated.

Today sustainability is also related to climate change, meaning the minimizing of environmental impacts from the operations. In 2016 the United Nations (UN) held a webinar called *The State of Sustainable Supply Chains: Building Responsible and Resilient Supply Chains* and issued a follow-on report.[77] Of the UN's 17 sustainable development goals, three relate to supply chains: sustainable cities and communities, responsible consumption and production, and climate action. The UN lists the elements that should be part of a sustainable supply chain as human rights, labor, environment, and anti-corruption. STSCS relates directly to anti-corruption, in working to prevent criminal enterprise, piracy, terrorist attack, adulteration of products, counterfeiting of goods, and bribery.

However, environmental consciousness can also inform the management of the supply chain, such as incorporating synchromodal strategies that focus on the lowest cost, shortest time and least CO2 emissions along the supply chain. While this can be viewed as a good business practice, such integrated supply chain management limits the amount of time that goods are in transit, thereby lessening exposure to all forms of interference with the successful delivery of the items. For example, the new super cranes include cyber elements that incorporate scheduling the pickup of containers in a port to speed the truck turn-around times to less than an hour.[78] With the goods loaded and sealed at the factory, and containers loaded onto delivery trucks directly from the container ship, there is little opportunity for tampering with the cargo. This means that security can be focused on the "last mile" delivery to a warehouse, or to the railhead, instead of consuming extensive resources at the docks.

Cybersecurity

Cybersecurity has a prominent role in the management of business and government activities. While it has achieved increased academic recognition, with degrees in cybersecurity being offered at major national universities,[79] not all agencies have developed complete cybersecurity systems. The Department of Homeland Security (DHS) has created the Cybersecurity and Infrastructure

Security Agency (CISA), a national risk management center for US critical infrastructure. The cybersecurity branch notes that "[c]yberspace and its underlying infrastructure are vulnerable to a wide range of risks stemming from both physical and cyber threats and hazards."[80] Palo Alto Networks has noted that the supply chain is the weakest link in cybersecurity. The cybersecurity of each partner in the chain is controlled within its own organization so that one partner with weak protections exposes the rest of the partners to hackers. New vulnerabilities are developing through the "Internet of Things, digital buyer-seller relationships, and robotic process automation," raising the need to know how you're your "suppliers, and their suppliers' suppliers, and so on down the value chain, have the same kind of protection."[81]

Within the surface transportation element of the global supply chain, there are multiple points of cyber vulnerability. SCADA systems have long been used to manage industrial systems and power grids and now operate the engines of merchant marine vessels. Navigation is carried out through cyber bases systems using global positioning systems (GPS). Cyber control of road and railroad signals, train and ship scheduling, and bridge operations offers further opportunities for hackers to interfere.[82] Damaging the navigation cyber connection can cause a ship to go off course or even get lost at sea. Disruption in train signals can cause derailments, which can lead to environmental damage, fires and impacts on communities along the tracks.

Recent incidents have demonstrated the cybersecurity threat to maritime transportation. In July 2019, the US Coast Guard assisted a vessel bound for New York that had been subjected to a malware attack. The ship's owners failed to provide adequate cyber protection for the on-board computer that was used for electronic charts, cargo management, and communication with the port, pilots and Coast Guard. They determined that the vessel's lack of appropriate cyber protection was "exposing critical vessel control systems to significant vulnerabilities."[83] A more serious attack occurred in December of 2019 when a ransomware attack dubbed Ryuk shut down a port facility for 30 hours. "The virus further burrowed into the industrial control systems that monitor and control cargo transfer and encrypted files critical to process operations. The impacts to the facility included a disruption of the entire corporate IT network (beyond the footprint of the facility), disruption of camera and physical access control systems, and loss of critical process control monitoring systems."[84] A Singapore-based cybersecurity firm warned that ransomware attacks against ports could cost the world economy $110 billion.[85]

The Department of Homeland Security and the Department of Transportation have developed tools to educate the transportation sector about cyber risks, and provides tools to guide the development of cybersecurity programs. Trucking, maritime and freight rail elements are all discussed in the *Transportation Systems Sector Specific Plan*,[86] but the integration from vendor through the supply chain is not addressed. Cross-sector dependencies with power and public safety are acknowledged, and the importance of partners and stakeholders is discussed, but there is no discussion of the weak link outside the transportation sector that may expose the supply chain to cyber attack.

In February of 2020, the National Institutes for Standards and Testing (NIST) issued a draft of *Key Practices in Cyber Supply Chain Risk Management (Draft NISTIR 8276)* which "provides a set of strategies to help businesses address the cybersecurity threats posed by modern information and communications technology products."[87] It aims to address the vulnerabilities in the supply chain using lessons from 24 case studies that show "how components and services from third party entities"[88] make securing the supply chain difficult. When the final report is issued, it will provide a valuable tool for securing the surface transportation supply chain's cyber elements.

The US government is aware that transportation security requires attention to numerous other threats besides those posed by technological developments and has developed an overall strategy to combat them. The US Transportation Security Administration's *TSA Strategy 2018-2026* lists its primary goal to "improve security and safeguard the transportation system" and highlights the need to "promote security partnerships across surface transportation systems."[89] The strategy noted six key trends that must be addressed to enhance STSCS over the next eight years: continuous threat, emerging technologies, cyber-physical interdependency, passenger experience, changing workforce and transportation system and the economy. In its report to Congress with a shorter-term view, *2018 Biennial National Strategy for Transportation Security,*[90] the TSA offers some areas for exploration within its modal security and intermodal security plans which are focused on protecting transportation assets "from attack or disruption by terrorist or other hostile forces…."[91] The strategy lays out the primary types of threats to STSCS, and lists the challenges, addressed at the macro level that requires research. It notes, "each area requires thoughtful collaboration to achieve a common understanding of challenges, impacts, and feasible solutions." This research, through the development of the bibliographies and the use of a Delphi workshop, addresses these aspirations.

2.6 COVID-19

In January 2020, a novel coronavirus began to spread from Wuhan, China. The virus, called COVID-19, caused acute respiratory illness for many people who contracted the disease, with a 2.5% fatality rate worldwide by June of 2020, when 7 million people were known to have the disease, and 404,142 had died.[92] Since many people have had the disease but remained asymptomatic,[93] a true count of the number of affected people will be hard to develop. To protect communities from the virulent person-to-person spread, public health leaders in the United States and Europe called for "shelter-in-place" orders from mid-March through June. Social impacts included the closure of schools and workplaces, people working from home, students attending classes through computer-based systems, and a rise in unemployment, as all but "essential" businesses were closed. In the United States, the federal government provided $1,200 per adult and $500 per child in direct financial support to everyone earning less than $90,000 per year, and offered unemployment insurance payments plus $600 per week to enable people to buy food and necessities, and keep the economy going. The G20 nations provided stimulus packages to their

citizens, with the US programs worth about 11% of GDP, Japan at 21%, and most European nations providing about 5%.[94] By May 2020, the US had an unemployment rate of 13.3%.[95]

The economic impacts of COVID-19 have been mixed and have changed over time. While travel restrictions imposed by nations have severely impacted the travel and tourism sector, the online retail segment has actually added jobs as people experiencing shelter-in-place switched purchasing options to e-commerce.[96] Medical research has seen funding infusions as researchers work on developing a vaccine against the disease. Ford Motor Company is making ventilators, while Bacardi and other breweries are making hand sanitizer. *Forbes Magazine* listed dozens of US companies that switched to making products or providing services to support the response to COVID-19.[97] Unlike recessions driven by bad financial management decisions, this recession was driven by government action, causing widespread shutdowns of the economy; it will have a clear end date, driven by the lifting of shelter-in-place orders and the gradual reopening of businesses.[98]

COVID-19 hit China first, causing wholesale closure of factories, thereby slowing the worldwide supply of trade goods. In January and February 2020, China's exports drop by over 17%, and imports also fell 4%. Exports to the US fell 27.7% in January and February, with an increase of 2.5% of imports from the US,[99] driven largely by the import of meat.[100] (The two months are reported together because the Chinese lunar new year shut down for two weeks occurs at different times each year.) While factories reopened in March for many consumer goods, the reestablishment of supply chains delayed some manufacturing.[101] Chinese exports flowing into the United States were slowed by the COVID-19 shutdowns, impacting ports in Los Angeles, Oakland and Seattle. One million jobs in metropolitan Los Angeles are tied directly to the Ports of Los Angeles and Long Beach, where 90% of the Long Beach containers come from Asia. Jobs for longshoremen, truckers, warehouse workers and rail systems were impacted by the factory shutdowns in Asia and the slow reopening.[102]

COVID-19 also demonstrated the insecurity of international medical supply chains. The world had long relied on China for personal protective equipment for medical workers, such as masks and gloves, ventilators and hand sanitizer. The closure of Chinese factories limited the supply of these essential goods, as the available supplies we re-routed to areas within China fighting the coronavirus. Forty-three percent (43%) of the world's medical supplies were made in China,[103] creating a single point of failure when the COVID-19 closed China's factories and led to the creation of more stringent export regulations that further slowed shipments. By March of 2020, medical exports to the US from China were down 24%.[104]

2.7 Policy and Security

Think tanks have undertaken studies on supply chain risk management. The Potomac Institute for Policy Studies hosted the Vital Infrastructure Workshop and created a report, "Security Strategies for Global Supply Chains."[105] However, the work lacks a focus on transportation systems and their effect on the supply chain: differing routes, technologies and carriers, moving goods from

one mode to another. The report summarizes presentations on multiple sectors that would inform the development of a comprehensive blueprint for applied research on supply chain risk and transportation across all modes.

Implementation of new policies in STSCS will require the cooperation of supply chain operators, who must be conscious of stakeholder demands, the technology used by competitors, and stockholders' interest in the "bottom line," which they protect with insurance policies instead of making changes in operations. New technologies are adopted for efficiency, link cyber-based navigation systems on merchant ships, but the investment in security is lacking, leading to malware and ransomware attacks. The current literature has a reactive orientation, addressing problems that have already been demonstrated, while what is needed is forward-thinking about problems that might arise and solutions to prevent them. New regulations and policies should follow the NIST lead in promoting resilience, inter-agency cooperation and integration. CISA's 2018 Transportation Systems Sector Activities Progress Report found that "the security programs had earned an overall score of 3.6 out of 5, the lowest (3.2) was awarded to "enhancing the all-hazards preparedness and resilience of the global transportation system to safeguard US national interests."[106]

To develop proactive policies, more research is needed in specific fields. Government policies related to STSCS need to focus more on interactions among the facets of the supply chain and the vulnerabilities that are created. Implementation of these policies should be encouraged through incentives based on the effectiveness of the strategies that have been adopted. Different types of supply chains should have different levels of expectation for security adoption. Pharmaceutical supply chains should have Food and Drug Administration rules that ensure the safety and quality of the products not only at the point of production but through the whole supply chain. Speed of delivery impacts shelf life, for example.[107] Implementation of blockchain technology might limit tampering and adulteration of products in shipment, but better security for the container through the supply chain might equally rely on RFI tags and high-speed cranes. Government and the private sector both place a high priority on the success of the supply chain, which can be best secured through security plans that are coordinated across all elements of the supply chain. Carl Schroeder said that foresight is about minimizing surprise. STSCS research should aim to create maximum foresight as the transportation elements of the supply chain become more dependent on cyber elements, involve more emerging economies and have to navigate through the challenges of international diplomacy.

III. Methodology

The methodology for this research relies on a mixed methods approach. It began with a comprehensive search for bibliographic material in peer reviewed journals and academic materials. While there is a great deal of literature on the general topic of supply chain security, there is little available on the integrated approach to surface transportation supply chain security as a multi-modal enterprise. The available academic literature was gathered into an Excel-based bibliography that collected the material in numerous searchable frameworks, such as vulnerability, types of risks, modes of transportation, technology's role, and supply chain type and issues. This searchable bibliography is attached to the publication's webpage for easy access, along with a sheet of instructions for using it.

Another area of concern is the adversary aspect of supply chain security. It is critical to understand who is trying to damage supply chain security and what the motives are. A search of adversary literature was conducted, resulting in a companion bibliography in searchable Excel format that is also attached on the webpage. Together, these two bibliographies provide new resources to support deeper research into the security of the integrated surface transportation supply chain.

Delphi Method Workshop

A new approach is needed that looks at the issue of supply chain security and surface transportation's role from multiple perspectives and considers their implications for America's economic future. From the geographical perspective, how do changing transportation routes and the relationship to climate change impact supply chain security, such as the melting of the Arctic ice cap and the development of Russian cargo terminals on the north shore? How do developing technology and cybersecurity issues impact supply chain security and transportation, such as the US Navy being hacked through its ties to university networks.[108] What is the impact of autonomous vehicles, including ships, automated fleet management, and larger containers and longer ships, on surface transportation? How is the US economy impacted by these changes to surface transportation supply chain security?

An expert workshop was convened using the Delphi method in San José, California, on January 9–10, 2020, to examine the future trajectory of surface transportation supply chain security issues and consider where the knowledge gaps are currently. Local, state and federal government agencies were represented, along with perspectives of international organizations and the private sector. Each representative gave a presentation to provide a framework for understanding his or her aspect of the surface transportation supply chain security challenges. The group then evaluated the existing knowledge, the gaps in that knowledge, and created a blueprint for future essential research into enhancing surface transportation supply chain security from unfolding and future perils.

The research areas considered for the blueprint included the following:

- Types of modal relations and their interactions that characterize the transportation systems of US supply chains.
- Types of assets that are secured (cargo, ships, ports and other facilities, routes, intellectual property) and identify the value of each.
- Risk factors that may potentially impact these systems such as terrorism (destruction and havoc creation), criminal activities (theft and substitution), climate, technology (cyber and power) and projection of national power.

Using the Delphi method, the workshop discussions focused on areas needing the greatest research emphasis in the near term, based on the analysis by the experts. They considered the potential impact of each upon contemporary supply chain security issues, including geography (i.e., China's belt and road; Russia's Arctic trade strategy; US land bridge). They considered the impact of the risk factors, singly or in combination, upon the assets, and their relationships (intermodal, multimodal, synchromodal) along dimensions such as the denial of service, disruption, and damage to the system, and assessed the potential costs (monetary, reputation, public confidence). They identified the key actors (private sector, local, state, national and international government agencies, and international organizations) concerned with transportation and the related issues, evaluated the effectiveness of the policies that have been implemented, and obstacles to enhancing security and resilience, such as cyber systems, governmental silos, and emphasis on profitability.

The research blueprint is the outcome of the two days of presentations and discussions. Among primary concerns were providing some guidance on developing policy at the local, state, regional, national and international levels, taking into account constraints and externalities.

The discussion included practical questions about the current surface transportation supply chain security system. What is the system trying to protect? Is it the cargo or the vehicle or the system or the route? Legal/ethical/moral conflicts arise regarding where to place the emphasis. Other elements of the legal environment will impact how the nexus between supply chain security and transportation is understood. Different elements of risk have their own mandates and agendas. Is the emphasis cybersecurity or physical security domains, and which comes first? Is the bigger concern terrorism or criminal enterprise? The mafia was always concerned with providing security to their clientele. Is bribery acceptable? A thorough understanding of supply chain security requires understanding the various nuances across professional boundaries. The workshop offered the opportunity for discussion of these challenges among experts.

IV. Bibliography Development and Literature Review

Although there is widespread acknowledgement that these new challenges are creating a need for new policy responses to deal with these developments that are already creating a new international environment for global business and placing strains and uncertainties on existing US supply chain structures and patterns, the extent to which these—and other themes—have received adequate scholarly attention clearly deserves careful consideration.

Accordingly, the goals of this project may be summarized as follows:

- To develop a bibliography of currently available research in the field that will support future practical research on enhanced supply chain security.
- To develop a blueprint for future research and development for transportation's role in supply chain security from technological and human-caused hazards.
- To create a blueprint for research that will enhance the security of global supply chains by enhancing risk management in its transportation systems.
- To identify practical measures that can be adopted by operators and government agencies in order to enhance the security and resilience of supply chain transportation systems.

From a geographical perspective, for example, how do changing transportation routes and the relationship to climate change impact supply chain security, such as the melting of the Arctic ice cap and the development of Chinese cargo terminals across the globe? From an ethical perspective, what is the relationship between data security and privacy? What challenges do emerging technological and cybersecurity issues pose for supply chain risk management and transportation? What is the impact of autonomous vehicles, including ships, automated fleet management, and longer containers and longer ships, on surface transportation? How is the US economy impacted by these changes to supply chain security? And, how effectively are these new security challenges being met?

When considering the degree to which public and private policymakers are dealing effectively with these challenges, numerous other questions deserve careful consideration. As noted above, the focus of security will differ across modes. Agencies have their own unique views of security, such as the Federal Bureau of Investigation's focus on making a criminal case that stands up in court versus the Drug Enforcement Administration's focus on interdiction and disruption of illicit supply chains. The mafia was always concerned with providing security to their clientele.

Given such a range of issues and questions, the ones that are essential to understanding the topic are as follows:

1. What is the background and current state of the research in supply chain risk management's transportation dimension?
2. What work has been completed by existing transportation and supply chain scholars and organizations, and published in either peer reviewed or professional journals?
3. What are the future research needs, and what is the path forward for the development of practical policies, programs and technologies to enhance supply chain risk management's transportation dimension?

In order to answer such questions, it was essential to maintain a strict focus given the variety of challenges, their increasingly recognized implications for America's strategic future, and the multiple perspectives that can be used to examine issues related to supply chain risk management and transportation's role therein. Accordingly, the following tasks were undertaken. The research began with the creation of a bibliography containing academic and other relevant publications that could be analyzed in order to identify the attention paid to critical issues. The results of this analysis led to the expansion of the research in order to deal with certain issues in more depth and, especially, to assess the state of policy development. Completing these two areas led to the identification of the most important lines of research that can inform the development of future work in the area and contribute to the enhancement of the security of supply chain transportation systems. The attached bibliography is structured so as to reflect these two phases. The first part includes the works that were quantitatively analyzed, the second the other works that were consulted.

Through this work, the research examined the ways in which the literature:

1. Defined the scope and content of such key concepts as risk, security, safety, terrorism, resilience, and emergency management so as to establish a precise focus for the study.
2. Defined the types of modal relations and their interactions that characterize the transportation systems of US supply chains.
3. Defined the assets that are secured (cargo, ships, ports and other facilities, routes, intellectual property) and identified the value of each
4. Identified the risk factors that may potentially impact these systems, such as terrorism (destruction and havoc creation), criminal activities (theft and substitution), climate, and technology, recognizing that geo-political factors exist that are outside of the scope of this research.
5. Classified the potential impact of each risk factor upon contemporary supply chain security, including geography (i.e., China's belt and road; Russia's Arctic trade strategy; China's African food strategy; US land bridge).

6. Identified the impact of the risk factors stated above, singly or in combination, upon the assets and their relationships (modal, multi-modal, intermodal) along dimensions such as a denial of service, disruption, damage to the system and assessment of the potential costs (including monetary, reputation, and public confidence).
7. Identified the key actors (private sector, local and national government agencies, international organizations) concerned with transportation and the related issues, then evaluated the effectiveness of the policies that have been implemented and obstacles to enhancing security and resilience such as an "online society," governmental silos, and emphasis on profitability.
8. Provided some guidance on developing policy at the local, state, regional, national and international levels, taking into account constraints and externalities.

In addition to determining the extent to which the existing literature answers such questions, however, it is important to consider how these can be translated into policies. To that end, a workshop was convened to bring together academics, security officials and supply chain professionals to consider the issue of supply chain risk management and transportation's role from the multiple perspectives cited above, including their implications for America's economic future.

4.1 Supply Chain Risk Management

These surface transportation supply chain security developments have attracted the attention of an increasing number of academics, as well as public and private sector organizations involved with ensuring the efficiency and security of supply chains generally and transportation systems specifically. A large literature has emerged dealing with these topics, although these topics have not received the attention in the enormous supply chain literature that might have been expected.

As mentioned previously, over 40,000 books and articles dealing with various aspects of supply chain management were published between 1982 and 2015. Only one of the popular textbooks dealt with transportation and concluded by identifying such topics as security, sustainability, risk, and disruption are "promising future research areas."[109]

Yet a rich body of work, the Supply Chain Risk Management (SCRM) literature, has developed in recent years as a result of the ever-increasing concern with the risks that supply chain managers confront. This body of works also covers a wide range of topics and perspectives. Scholars have attempted to create models that consider such variables as probability, impact, interactions, frequency, duration and type, and to develop techniques to minimize the impacts and consequences of these different situations.[110] How rapidly this field has grown is evidenced by the great increase in published research—from 8 articles in 2003 to 33 in 2013, for a total of 224.[111] This study too reveals the limited attention paid to transportation—only one article out of 143 that were analyzed dealt with this risk area.[112]

Even in its areas of focus, however, this literature suffers from a number of shortcomings. The first is the conceptual issue that there are "many discussions about risk but few clear and concise definitions."[113] This issue is, of course, not limited to this literature but encompasses all the other terms relevant to any consideration of transportation security issues such as "terrorism," "security," "resilience," "safety," "inter-modalism" and the like.[114]

Another important area that has been largely neglected in the SCRM literature is the role of macro challenges, although the "risks" are commonly divided between the "micro" and the "macro," with the former receiving an overwhelming degree of attention. One study found that almost half (70) of the 143 articles that were analyzed focused on supply risks, another 27% dealt with demand issues. Only six articles dealt with macro challenges, even though an understanding of such issues would seem of great importance if supply chain managers and decision makers are to successfully manage a supply chain or develop policies that enhance the security of all its elements, including transportation.[115]

The studies that have attempted to deal with these issues often use the Delphi method to identify and aggregate expert opinion. One that focused on the "new field" of "Security Supply Chain Management" sought to determine how a variety of stakeholders viewed various elements in the macro and the micro-environments and assessed their impact on the logistics industry by 2025.[116]

Its respondents held the highest anticipations regarding the following areas: economically, the energy supply; politically, the advancement of least developed countries (LDCs) and a global water crisis; socio-culturally, the continuing importance of human capital and the ability to respond rapidly to natural disasters; and technologically, major advances in transport systems.[117]

A limited body of literature focuses explicitly on the future of logistics. A German study has analyzed this topic in-depth, using the Delphi approach that included detailed interviews with the top 50 logistics providers and other major practitioners. It found that the major themes that would characterize the industry in 2025 were: (1) a concern with social responsibility, (2) increased global business interactions through political and legal issues, (3) a shortage of qualified personnel, (4) changing customer expectations, and (5) digitization. These results demonstrate the limited attention that supply chain officials paid to security issues as late as 2013.[118]

Clearly, the academic literature dealing with the potential impact of global developments upon the supply chains' security issues generally, and their transportation systems specifically, is quite limited. As one recent study of these topics noted, "there is clearly a research gap in the domain of infrastructural risks such as transportation, information and financial risks as well as macro risks."[119]

This finding is largely consonant with the substantial literature that has been produced by supply chain organizations. As might be expected, given the changes that have been taking place globally, it seeks to help ensure that global supply chains continue to function effectively in an environment that poses new and complex challenges. Thus, its primary focus is upon how the risks that

managers and operators of supply chains confront—such as enhanced technological competition, sub-contractor failure, inadequate information and the like—can best be assessed and mitigated so as to achieve enhanced efficiency and thus, profitability. Macro factors and transportation security receive only limited attention.

Business for Social Responsibility (BSR), for example, has identified the following as the major change agents through 2025—the adoption of new technologies, climate change and resource scarcity, human migration, changing markets, and "mixed signals on trade and transparency." It then makes recommendations on how firms should prepare themselves to function effectively in this new environment, especially in terms of its procurement policies.[120]

Similarly, the Chartered Institute of Procurement and Supply, which recognizes "that businesses are trading in unprecedented economic and political times," emphasizes economic and financial factors. Its recent report, published in December 2017, concluded that its risk index (which stood at 79.8) though high, because of political and economic tensions, had improved because of increased global growth and reduced risks in the major economies.

Business organizations, however, are not the only ones concerned with the future of supply chains. Many "think tanks" have also expressed their concern, and these do tend to focus on geo-political factors and their national security implications. Thus, when the Council on Foreign Relations held a workshop in May 2016 to discuss the future of global supply chains, its participants shared BSR's concern with growing protectionism and climate change, but it also noted the prevalence of cyberattacks and human rights abuses, as well as the rise of China and the implications of these developments for national security.[121]

Since the beginning of the twenty-first century, studies dealing with transportation security issues have also proliferated greatly. The Transportation Research Board published an early relevant work, "Deterrence, protection, and preparation: the new transportation security imperative" in 2002, and some scattered studies can be traced back to the mid-2000s with discussions of terrorist and criminal activities aggravating the dangers inherent in hazardous shipments.[122]

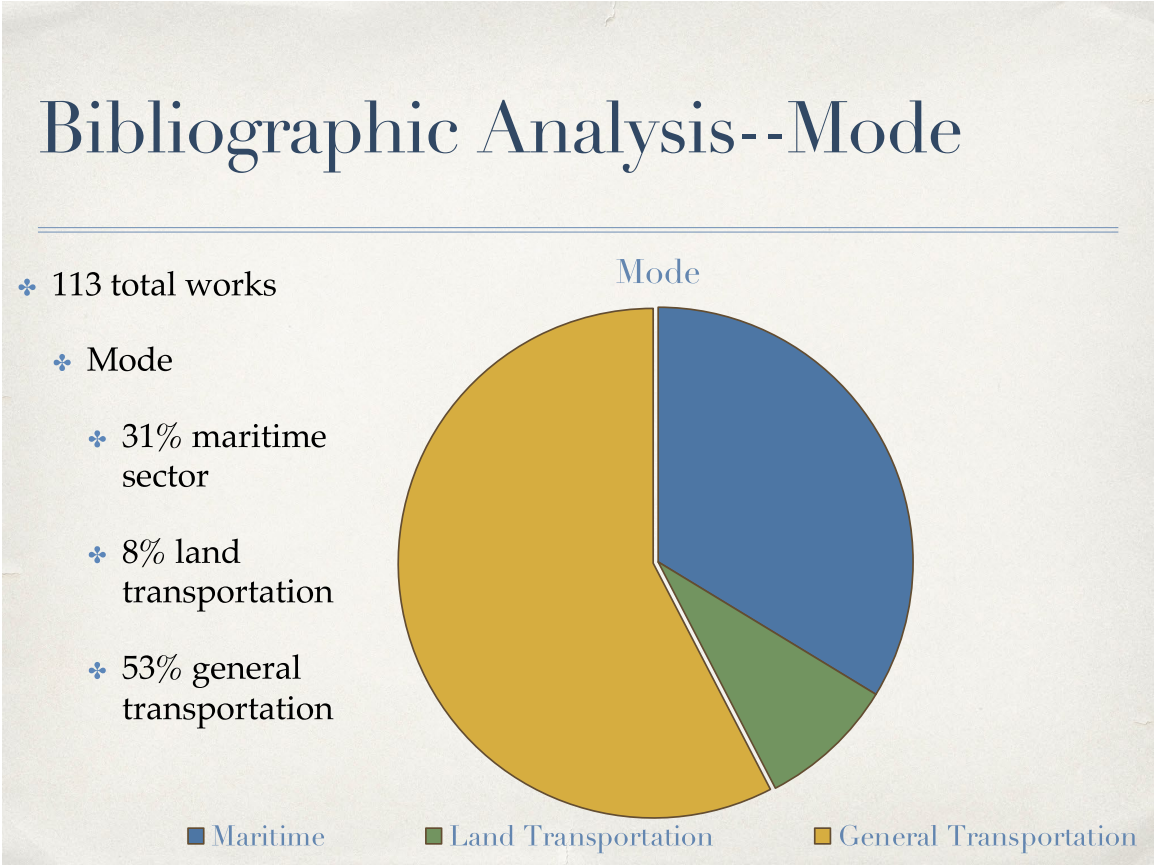
4.2 The Literature: Issues and Coverage

What is not clear, however, is how the transportation security literature is dealing with the macro risk factors in terms not only of identification but also as regards the development and implementation of effective policies to mitigate these risks. Accordingly, the research identified and analyzed 113 articles dealing with transportation security issues, 81 of which (72%) were academic, many of which were themselves reviews of bodies of literature, eight (7%) were by private sector organizations and companies, ten (9%) by US governmental agencies, and 14 (12%) by independent and international agencies.

Surface supply chain transportation systems encompass a variety of modes that operate on sea and land. Yet, surprisingly, very limited attention has been paid to the security of the land

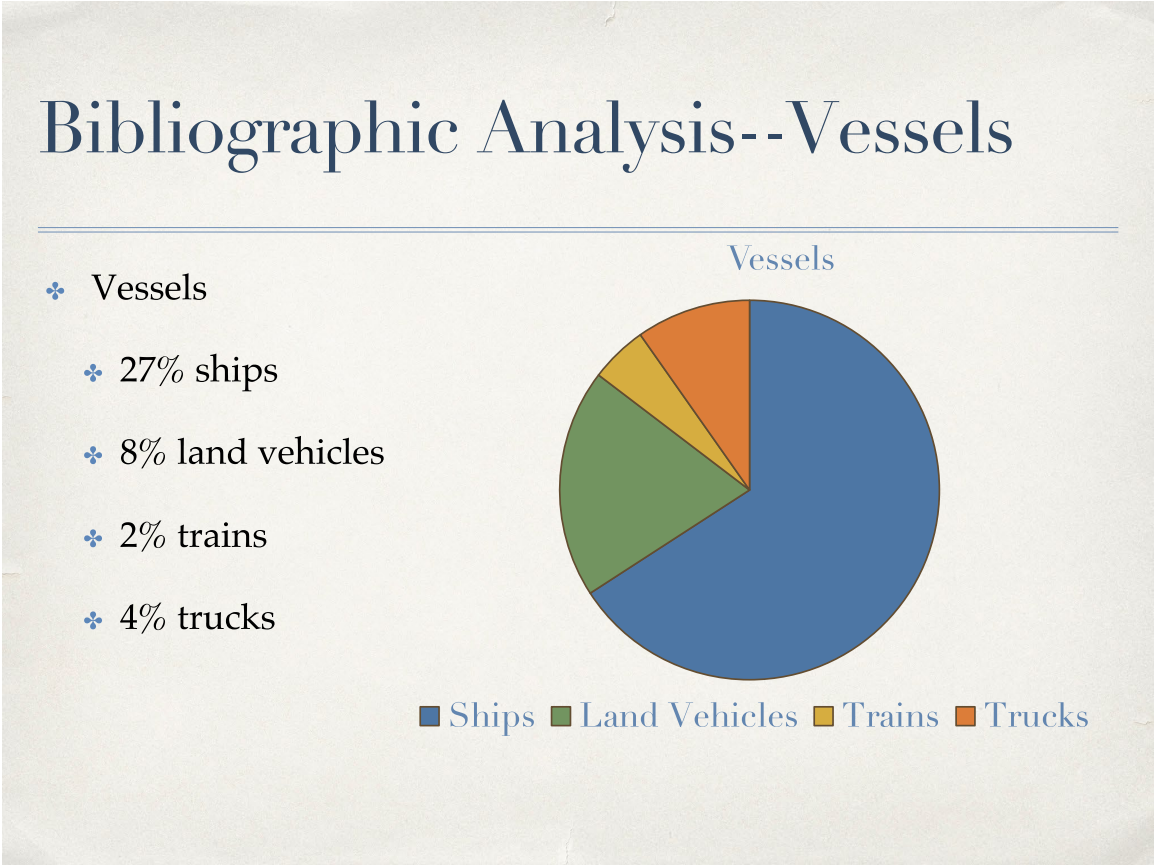
transportation systems' components—rail, road, and pipelines. Of the works that were analyzed, 35 (31%) dealt with the maritime sector, whereas only ten (8%) focused on land transportation. By far the largest number, however, 60 (53%) involved transportation generally.

Figure 1. Bibliographic Analysis: Mode



The emphasis on maritime was repeated when the research considered the specific vehicles that were discussed: 31 works (27%) involved ships compared to only nine (8%) with land vehicles, three (2%) with trains, and six (4%) with trucks). The majority 55 (49%) dealt with all modes, while the remainder focused on general administrative and policy issues.

Figure 2. Bibliographic Analysis: Vessels



Though it can be argued that the focus on the security of maritime supply chains is justified, given that the vast majority of international trade is sea-based, and that most of the literature examines global supply chains, not specific products or regions, such a proposition ignores the critical role played by the risks to the cargoes after they have been offloaded and shipped by truck and/or rail to warehouses and customers.

Clearly, the land modes require greater attention. Though very limited literature deals with truck freight issues, that mode certainly deserves greater notice. Rail freight transportation, which has been neglected even more, and which is known to present security issues, remains a topic that is certainly worthy of more research. Equally striking is the total absence of another mode of land transportation, pipelines.

Pipelines play a critical role in the economy, and ensuring their security is clearly a matter of national importance, one that has been officially recognized by the US government. Administratively, they have been officially defined as a transportation mode by the Department of Homeland Security (DHS),[123] and numerous efforts have been made to ensure its security, given its vulnerabilities to physical attacks and cyber threats.[124] Clearly this is yet another sector that deserves more academic consideration.

Furthermore, the relationship between inter-modalism and security also seems to have been totally ignored. The need to coordinate freight movements as they travel through various modes became evermore obvious, and technological developments made it increasingly possible to create an integrated system. By the end of the 20th century, the need to move policies away from individual modes was widely recognized, and in 1991 the US Congress enacted the landmark Intermodal Surface Transportation Efficiency Act (ISTEA). Concomitantly, the number of studies dealing with inter-modalism has increased greatly. However, scholars have focused on such topics as conceptualization, quality and efficiency, and modelling.[125] Thus, it is not surprising that another recent study of how risk issues were handled in intermodal supply chains found "very few papers on the topic of intermodal supply chain risks."[126] None of the works in the current literature review dealt explicitly with this important topic. This is clearly another important area that deserves greater attention.

Not surprisingly, the bibliography of literature that was analyzed revealed a great concern with risk; 43% of the sources ranked it a high concern, 8% considered it a moderate issue, 18% classified it a matter of low concern, and 38% regarded it as a matter that varied over time. When viewed in terms of the major issues confronting supply chains and their transportation systems, similar results prevailed. Security ranked as the major topic (48), and when combined with risk assessment (27), accounted for 65% of the total. Surprisingly, management issues accounted for 35% of the total.

When the data is analyzed over time, there is a marked degree of fluctuation over the last 17 years, but certain trends emerge clearly. First, while risk assessment has consistently been a common topic of discussion for some time, supply chain security specifically has been discussed with increasing frequency in the past decade. And, as might be expected, while attention paid to internal issues has remained fairly constant, albeit at a higher level in the years following 2010, interest in external threats and vulnerabilities has increased markedly in recent years. Surprisingly, however, the rise did not begin until 2012 and accelerated markedly only after 2017.

Figure 3. Mentions of Vulnerability Type by Year

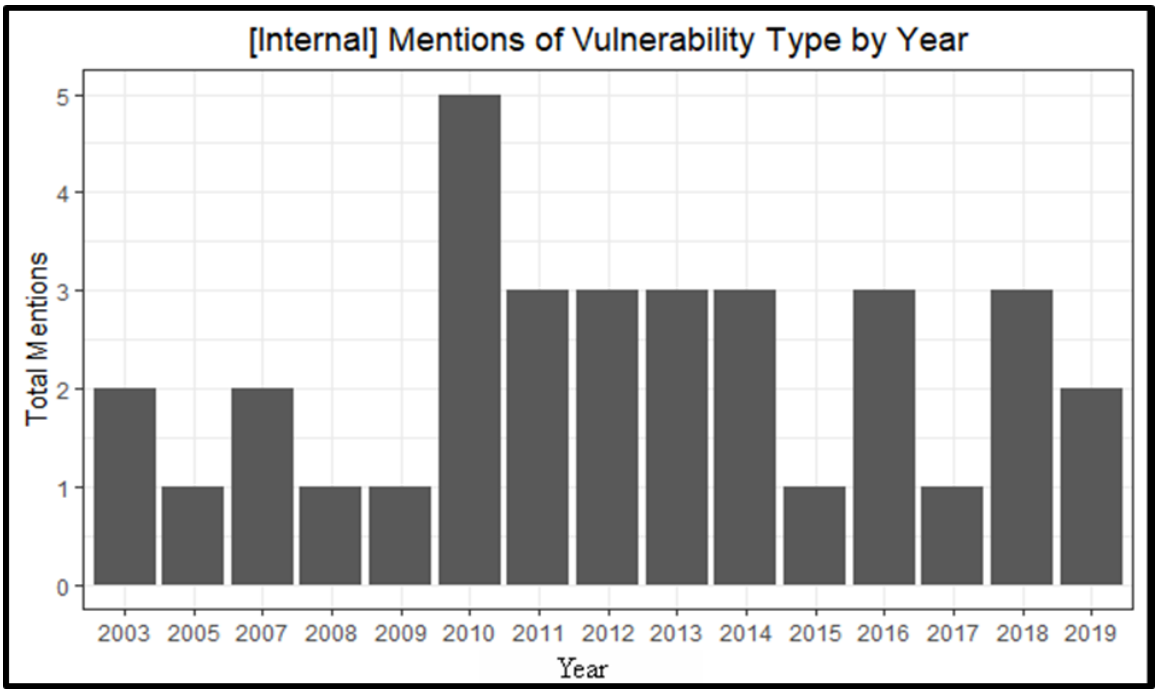
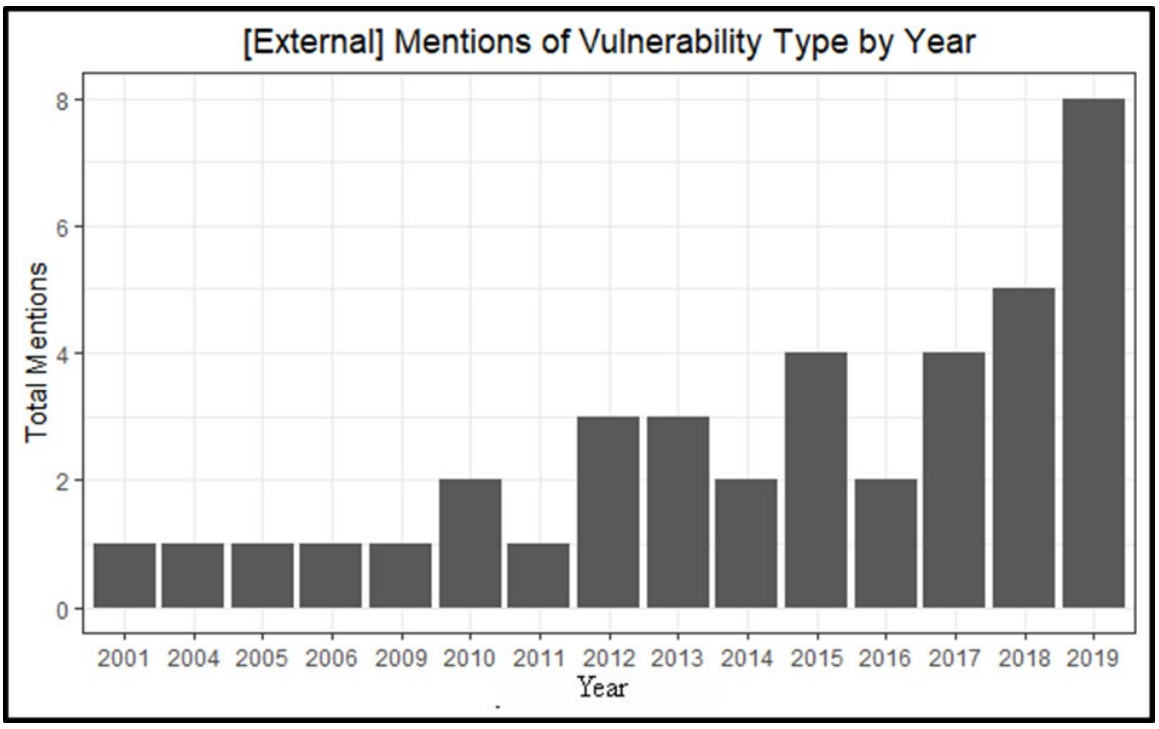
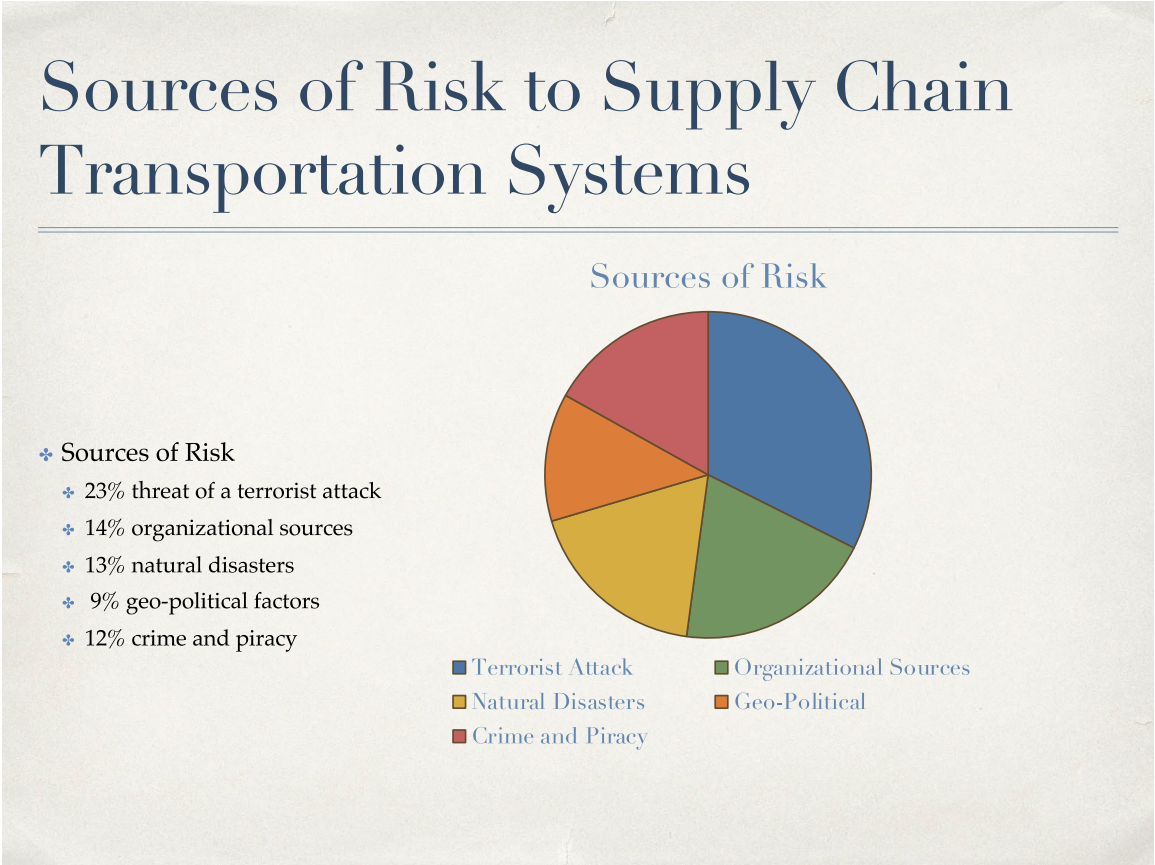


Figure 4. External Mentions of Vulnerability Type by Year



The literature also recognizes that supply chain transportation systems are potentially subject to many sources of risk, and it is clear that it has focused on these to varying degrees. The most cited source was the threat of a terrorist attack (23%), followed by organizational sources (14%) and natural disasters (13%), geo-political factors (9%) and crime and piracy (12%). That criminal activity received so little attention is rather surprising, given its widespread prevalence.

Figure 5. Sources of Risk to Supply Chain Transportation Systems



The changing geo-political global landscape, as noted above, was mentioned in only 9% of the literature that was analyzed, as compared to 13% that were concerned with the impact of natural disasters.

Yet the roles that such factors are playing and will play in the coming decades suggests that they deserve far more attention. They have already aroused increasing concern in government circles. The Transportation Security Administration (TSA), for example, has issued a report dealing with such issues. The *TSA Strategy 2018-2026* identifies the six key trends that it believes will impact its activities in the years to come. These are: (1) Continuous Threat, (2) Emerging Technologies, (3) Cyber Physical Interdependency, (4) Passenger Experience, (5) Changing Workforce, and (6) Transportation System and the Economy. It is in the process of developing specific goals, priorities and plans in these areas.[127]

Although this document reflects an awareness of the importance of a long-term perspective, it must be noted that half of these trends relate specifically to the internal workings of an organization. Only three identify external forces that will have a major impact on the functioning of transportation systems: (1) terrorism, (3) cyber threats, and (6) changing geo-economic patterns.

However, not only do these dimensions deserve elaboration, but it is also necessary to consider other macro factors whose impacts upon the security of the transport systems that integrate the

global network of supply chains are already discernible. Specifically, geo-political issues such as growing trade tensions received little attention, as did the geo-economic changes that are already impacting the global trading system. Yet such factors as the emergence of new economic powers will clearly impact existing supply chain transportation systems directly by creating new logistics networks that will render established ones obsolete.

China's "new silk road," which consists of both land and sea projects, is by far the largest and most grandiose program of this sort. Designed to establish new trade corridors that will link China to Central Asia, the Middle East and Europe, it is costing over $900 billion and involves over 60 countries. China has also invested heavily in ports and other transport facilities in Africa, where many states are exploring ways to expand and integrate their railroad systems. Whether it will succeed in achieving its ambitious goals, however, is a subject of much debate.[128]

There is, however, little doubt that all these developments represent a major challenge to existing trade patterns that have been traditionally centered around the US, the EU and Japan. The Organization for Economic Cooperation and Development (OECD)'s Economic Department has carried out a detailed study that concluded that Asia will continue to expand its role in the manufacturing sectors for decades, so that "the share of global trade within the present OECD will decline from 50% in 2012 to 25% by 2060, while trade among non-OECD economies will account for approximately one-third of global trade."[129] Moreover, these developments will shape the shipping sector, including the size and type of ships and their technologies.[130] Its strategic and security implications have also received attention. The Subcommittee on Coast Guard and Maritime Transportation of the US Congress, for example, recently held a hearing on "China's Maritime Silk Road Initiative: Implications for the Global Maritime Supply Chain."[131]

Trade routes are also being shaped by environmental factors. Climate change is already affecting the production of various agricultural products throughout the world and making possible the development of new routes such as the Northwest Passage. This will have serious implications for existing routes and facilities, since it will cut the distance from Asia to Europe and the US by 30% and 20%, respectively, and thus negatively impact Panama and Egypt since the number of ships using the Panama Canal and the Suez Canal will greatly decrease. On the other hand, the Baltic and the North Sea countries, especially Russia, will benefit greatly. President Putin officially announced in 2018 that Russia was adopting a maritime policy to increase its traffic through the Arctic. As part of that effort, Russia is actively pursuing various projects to enable it to optimize its ability to use the new routes, including building a new port on its Arctic shore.[132]

Nor can one ignore the environmental impacts of maritime transportation. Numerous efforts are already underway to deal with this problem. The International Maritime Organization (IMO), for example, has adopted a program designed to reduce greenhouse gas emissions from ships by at least 50% from the 2008 base by 2050. Many believe, however, that additional policies and regulations are required. As a United Nations (UN) representative recently stated: "we are headed for an environmental disaster" unless the maritime industry drastically cuts its emissions.[133] Such

measures will obviously change maritime technology and create new possibilities for attacks and exploitation.

These issues are also linked to the growing concern with sustainable development. Sustainability incorporates many other dimensions besides pollution, such as human rights, gender equity and fair trade. All these topics have obvious implications for patterns of national and international growth, as well as for the operations of supply chains in various sectors. Each dimension has received increasing attention by corporations that have reacted to governmental concerns and the efforts by private organizations to bring about change in corporate policies. As a result, public concern has risen to such a degree that in a 2016 report, Ernst and Young, a major accounting and professional services firm, noted that "supply chain sustainability can no longer be ignored."[134]

Such issues can be traced back to the container revolution that began a few decades ago and rapidly transformed transportation, thus contributing greatly to the emergence of today's system of globalized supply chains. Now, new technologies are again disrupting existing patterns and are likely to so ever more intensely in coming decades. Numerous organizations are exploring and developing a variety of technologies ranging from blockchain to 3D printing to drones to the Internet of Things (IOT) platforms. According to one expert, the key trends in 2017 involved autonomous road transport, crowdsourcing freight, apps that permitted a shipper to obtain instant freight services and digital freight matching.[135] Indeed, there is widespread agreement on such developments. Another professional agreed that autonomous trucking will be commonplace, that trucking will be "Uberized," that blockchains will create immense visibility along the supply chain, that such changes are already underway, as evidenced by reports that Rolls Royce plans to launch autonomous cargo ships by 2030, and that Amazon will use drones for last- mile deliveries.[136] Numerous other examples of companies moving rapidly ahead can be cited, including the development of a blockchain application for tracking cargo operations by Maersk and IBM that is being tested by a number of ports and Dutch and US customs.[137]

Technology, however, is a mixed blessing, for each innovation can be and has been used for nefarious purposes, which range from theft to product substitution and from falsification to ransom demands. Ongoing conflicts in the Middle East and elsewhere enhance the threat from terrorism and pose obvious security challenges, as does piracy. Though pirate attacks have decreased since 2019, the problem remains acute, especially around West Africa.

As might be expected, the literature that was analyzed for the bibliography reflected these concerns. Terrorism was considered the major threat (23%), criminal activities (including piracy), rather surprisingly, were cited only 7% of the time. As was mentioned above, this is a surprisingly low figure given the degree of criminal activity and the recognized need by the US government to deal with this problem.[138] Furthermore, while discussions of terrorism in relation to supply chain security seriously increased in the 2000s; after 2010, it has largely plateaued. Though it continues to be a common theme, it has not increased in importance much since then.

Again, as might be expected, the literature recognizes the critical role being played by new technologies and their vulnerabilities, especially in information and communications. There has been a sharp increase in attention paid to cyber/information topics in recent years, both as technology and risk. Between 2003 and 2012, cybersecurity was cited 13 times, and in the years that followed until 2019, almost tripled to 35, as shown in Figures 6 and 7.

Figure 6. Cyber/Information Mentions of Tech Type by Year

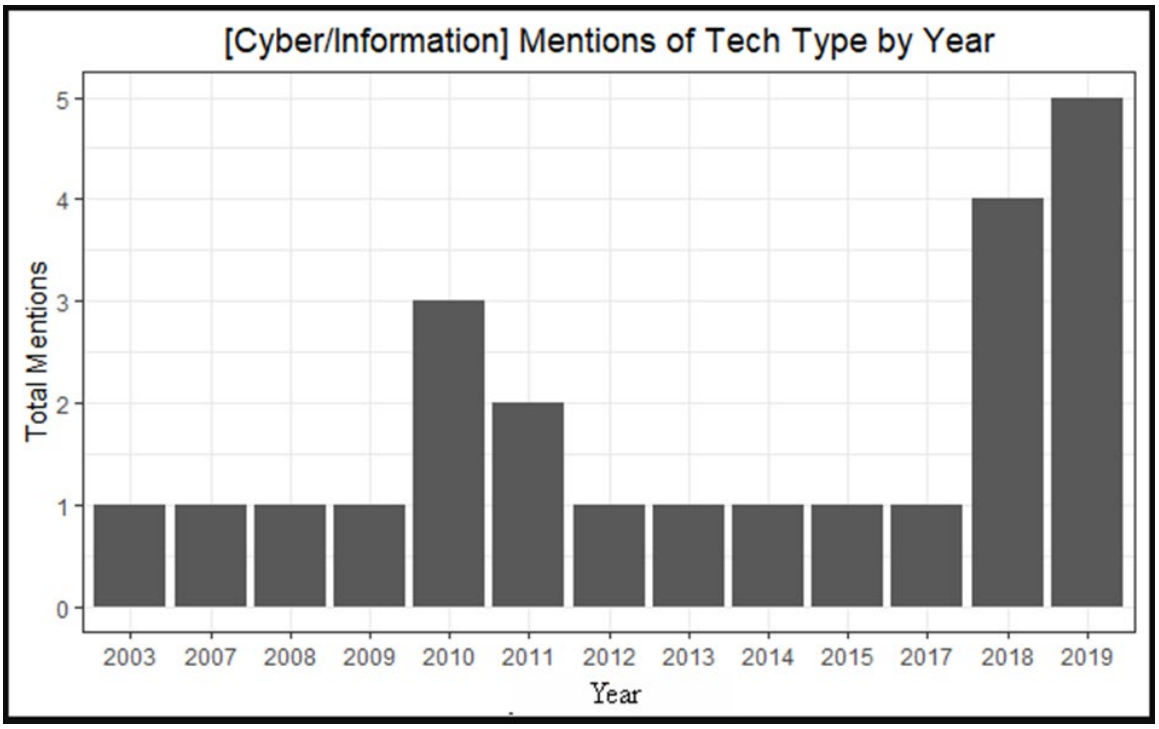
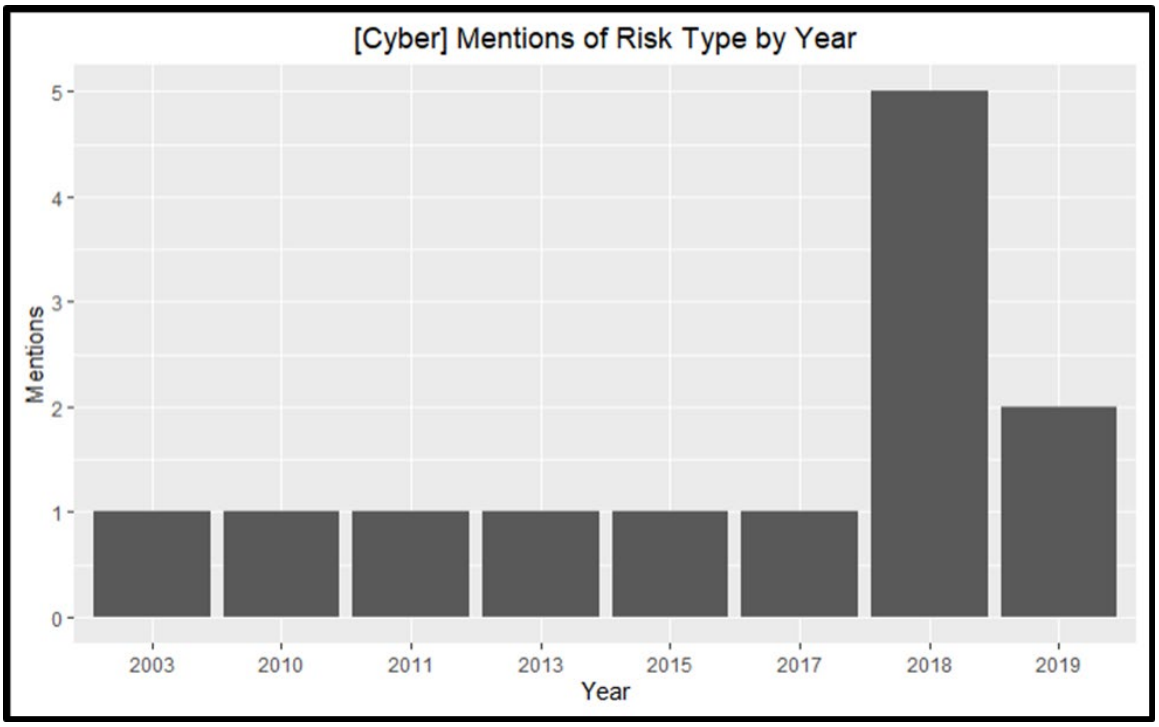


Figure 7. Cyber Mentions of Risk Type by Year



The area of greatest national concern is the increasing reliance on artificial intelligence (AI), which has created new vulnerabilities that are recognized as a major security issue for all transportation modes, as well as many other sectors. Not only is it listed by the TSA as one of the major trends, but Daniel Coates, Director of National Intelligence, ranked it first in a list of global threats. He noted its use against global shipping and pointed out that it is a continuing and increasing problem.[139]

Despite the great emphasis on this issue by the US government and other agencies, including the IMO, which issued specific guidelines in 2017, it is widely acknowledged that this vital sector has failed to adopt adequate measures to deal with the cyber threat so that it has to play "catchup."[140] According to another expert: "it's no secret the maritime industry is behind the time when it comes to cybersecurity, but there are encouraging signs."[141] Soon after this comment, on July 18, 2019, the US Coast Guard issued a warning following a cyber incident that impacted a ship bound for the port of New York. Noting that "cyber security awareness is low to non-existent," it urged "ship owners to conduct robust cyber security assessments of the vessels." Doing so, it must be noted, is no simple matter given the nature of the crews who are usually on temporary contracts and the need to safeguard onshore facilities, including company headquarters.[142] Several articles in the literature considered such issues, namely the need to control vessels and facilities, as well as the importance of ensuring cargo security. Yet, if the maritime sector is to attain a significant level of security, a new orientation by the managers and operators is required, for its high degree of vulnerability has been attributed to "its lack of encryption, increased use of computer services, a lack of standardized training in and awareness of cybersecurity among crew, the sheer cost…and industry-wide complacence…"[143]

That technologies pose a threat to maritime security is recognized in the literature. When technology was analyzed by type, cargo control technologies (24%) ranked second to cybersecurity (59%). In addition, one might reasonably conclude that many of the authors who discussed the impact of technology on vessels and vehicles, which ranked third with 7%, were also concerned with ship security.

Criminal actors have also recognized the ways in which technology can enhance the effectiveness of their activities, though as has been noted, the literature has not accorded it the degree of attention that it deserves. Businesses and governments have long regarded such acts as issues of great concern, for they threaten the integrity of supply chains which are subject to widespread theft, product substitution and falsification. Already commonplace in many countries and for numerous supply chains, they represent major security issues, especially given their often-deadly consequences. Many countries are struggling to deal with this problem by adopting policies to ensure the integrity of their supply chains. In the US, for example, The Food and Drug Administration issued a draft guidance on June 30, 2017, regarding product identification under the Drug Supply Chain Security Act in an attempt to safeguard the security of that critical supply chain. The rapid development of blockchain technology is widely expected to minimize such threats and is being increasingly adopted by many businesses.[144]

This is another area that deserves more attention, for it is necessary to differentiate among types of supply chains and their different transportation systems. Yet the literature that we analyzed focused primarily on the generic supply chains; none dealt with drugs or food, for example, though hazardous materials and energy were mentioned.

Other technological developments, notably the adoption of containers to move goods, have created new security challenges. How to ensure their security has been an area of major concern, and the US and the IMO have adopted a number of relevant policy measures, such as Customs–Trade Partnership Against Terrorism (CTPAT) and Maritime Transportation Security Act 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) Code. Not surprisingly, given the overwhelming attention paid to the maritime sector, container security received considerable attention.

Containers are not only an important security issue in their own right, but they have also contributed greatly to the emergence and implementation of a new vision of transportation, inter-modalism, which presents its own security issues. It became increasingly obvious that the advantages of moving containers by land as well as by sea necessitated a new approach, that the traditional approach to transportation that treated each mode separately no longer sufficed, and that it had, in fact, contributed to many problems, ranging from pollution to the inefficient movement of goods and people. Accordingly, in 1991 the US Congress enacted the landmark Intermodal Surface Transportation Efficiency Act (ISTEA). Over time, this new approach has led to the emergence of a more efficient and cost-effective system that also possesses new vulnerabilities. Even if the impact of the future trends discussed above on the security of

transportation systems is carefully analyzed, it is essential to recognize that the breakdown of any component of the intermodal system can have devastating repercussions for the entire supply chain. Ensuring the security of this system is also more challenging because of its size and complexity. Not only are intermodal terminals, a critical node in the system, attractive targets, but traditional security challenges are complicated by problems of coordination and integration of the many different categories of workers who flow in and out. And, though the terminals are critical, an attack on the trucks that carry raw materials, or to the maritime transport to and from port, can also lead to major disruptions.[145] Yet, the bibliography that was analyzed revealed a very limited amount of relevant works, though a few viewed existing infrastructural patterns and practices such as transfer points as areas of risk. In this field, too, the issue of conceptual clarity complicates analyses, for such terms as multi-modal and synchromodal are also commonly used.

4.3 Policy and Security

Although this literature possesses rich discussions of how to enhance the security of the various transport modes, albeit primarily the maritime, the degree to which these have been adopted and implemented by key actors remains unclear and deserves further attention.

Furthermore, supply chain operators generally continue to place business considerations ahead of security. They seek to protect their interests by eliminating internal risks and redundancy so as to improve the efficiency of their operations. By doing so, they hope to remain competitive and to grow their customer base. Hence, they are generally interested in using emerging technologies, such as automated vehicles, drones, and improved tracking and GPS software to improve their ability to track goods and transfer them as quickly as possible. However, doing so may contribute little to enhanced security.

Even when there is a recognition of the need to adopt technological innovations for security reasons, other factors can make such innovations difficult. Each supply chain has its own organizational structure and administrative decision-making processes, and such factors as how these processes function, including the role and power of various administrators, can all determine whether security enhancing measures will be adopted. It has been noted, for example, that if cybersecurity is to be enhanced, "digital supply chain officers need to be seen and heard."[146]

Clearly, management is a key factor and, as noted above, has received considerable attention in the literature that was analyzed. When the major supply chain issues were being discussed, three emerged: risks, security and management. Management received 36 mentions, placing it second to security, which received 48 mentions. Risk assessment also received 36 mentions, and it should be noted that how effectively these elements are conducted is also a function of management. The extent to which management is a critical issue emerges even more clearly when the policies that have been implemented are analyzed.

Essentially supply chain managers have two options when seeking to enhance security in their transportation systems—to act proactively by adopting policies designed to minimize perceived

risk(s) or reactively after some incident; the latter is the common pattern. As in the maritime case, supply chain security measures tend to be adopted reactively, sometimes in response to unforeseen developments. The former is primarily the result of regulations imposed by local, national, regional and global governmental organizations. These have obviously increased significantly in recent years as governments reacting to the disruptions and ever-changing threats have adopted numerous policies to safeguard supply chains generally, and transportation systems specifically. These policies, however, have proven to be of varying effectiveness, and how to improve them poses ongoing challenges, not least of which is how to enhance the willingness of supply chain stakeholders, with their different perspectives and interests, to act proactively.

The importance of acting in this manner to enhance supply chain security is widely recognized by business organizations and academics.[147] Not only does it minimize the impact of a negative event, but it has proven to be a cost-effective approach to doing so. As Deloitte concluded after an analysis of the impact of the disruptions, 85% of the companies that it surveyed agreed that "proactive risk management in the supply chain has shown to be a cost-effective approach. Companies that indicated that they proactively manage supply chain risk spend 50 percent less to manage supplier disruptions than companies that stated that they aren't proactive."[148]

Acting proactively can contribute to another important element to supply chains generally and transportation systems specifically—resilience. This too, has become a theme that has been widely promoted by business organizations and has attracted growing attention in academic circles. Only two articles were published between 2006 and 2008, but in 2017 the number had climbed to 25, for a total of 95, almost half of which were published in transportation journals.[149]

The importance of this topic was recently underlined by the recent National Academies Press publication *Freight Transportation Resilience in Response to Supply Chain Disruptions,* which contains a detailed analysis of the topic. Its stated goal is to provide information that will help stakeholders implement policies that will enhance system resiliency. As part of this effort, it identified the major factors within a supply chain that could impact transport resiliency—the physical infrastructure, logistical, financial, communications, regulatory and institutional elements. Of these elements, one emerged as the key—"effective interagency and intergroup communication was identified by many in the literature as being the most important input into effective resiliency strategies."[150]

Each of these elements is a critical one. Effective security policies require cooperation and integration across numerous national agencies, and between local, national, and international organizations, and the private sector. The challenge of interagency cooperation at the national level is reflected by how the 2018 Transportation Sector Activities Program,[151] which evaluated the state of transportation security, was prepared. Jointly issued by the US Department of Transportation (DOT), the TSA and the US Coast Guard, the specific relationships and responsibilities were as follows: "the U.S. Department of Homeland Security (DHS) and the U.S. Department of Transportation (DOT) as Co-Sector Specific Agencies (Co-SSAs) for the Transportation

Systems Sector. DHS delegates its Co-SSA responsibilities to the Transportation Security Administration (TSA) and the United States Coast Guard (USCG). DOT, TSA, and the USCG jointly perform the Co-SSA functions through a steering group and co-leadership of Government Coordinating Councils (GCCs)."[152]

It found that the security programs had earned an overall score of 3.6 out of 5, the lowest (3.2) was awarded to "enhancing the all-hazards preparedness and resilience of the global transportation system to safeguard US national interests."[153] It also made various recommendations to improve security levels. Its second-lowest stated, "increase sector engagement across the following five proposed focus areas: private sector engagements, modal dependencies and interdependencies, supply chain resilience, exercise integration, and intersections with international programs."[154]

Various government agencies and related organizations have, for years, attempted to engage with the private sector. Their efforts have included numerous publications designed to provide guidance to supply chain operators so as to enhance the security of their transportation systems.[155] However, as the report acknowledges, serious gaps remain between the desire of governments to enact policies that enhance security and the willingness of supply chain and transport companies to adopt various measures that will enhance security and resiliency, and apply them rigorously. The recommendations identify areas that clearly need attention. However, their successful execution will be no simple matter.

Surprisingly, one organization that could be very helpful has played a minor role, the General Accounting Office (GAO), which is responsible for evaluating and monitoring federal programs.

A sophisticated European study of its activities between 2005 and 20015 drew conclusions that were not only aligned with the findings of the literature review but also pointed out the same weaknesses and issues that were enumerated above.[156]

First, it found that the major concerns, as reflected in the number of reports, were supply chain security (38%) and maritime security (33%). It explicitly noted the lack of attention to road and rail transport and noted, "it would be reasonable if future GAO research or studies by other organizations also addressed these currently neglected modes of transport…Also the existing GAO reports largely overlook important supply chain security themes such as cyber security and supply chain resilience."[157] Furthermore, it pointed out that the reports' "recommendations on information management also urge the agencies to collaborate more actively with one another and with their fellow foreign organizations."[158] Finally, it should be noted that little seems to have changed in recent years. A search of the GAO website listed only three reports dealing with transportation—air quality, funding, and US interests in the Arctic.[159]

V. Findings from the Workshop

On January 9–10, 2020, Mineta Transportation Institute researchers convened a workshop on "Surface Transportation Supply Chain Security," bringing together subject matter experts from international, federal and state governments, the private sector, and academic researchers. The goal of the conference was to understand and evaluate the current state of the practice in surface transportation supply chain security and to consider areas of needed research to address existing as well as new and developing challenges. Areas of focus included risk estimation, geopolitical aspects, modal relations and cybersecurity.

The keynote speaker was Professor Joseph Szyliowicz of the University of Denver, with presentations on geopolitical challenges by CAPT Manual Raras, USCG (Ret.); security planning by CDR Romulus Matthews, USCG; and maritime management cybersecurity by LCDR Robert Cole, USCG. The impact of power outages on supply chains was presented by COL Mitch Medigovich, CANG (Ret.), deputy director of the California Office of Emergency Services. Challenges of cargo security and port management was presented by Kevin Krick of Matson Lines. Ash Padwal of Allied Telesis discussed cybersecurity and related future challenges. Gzim Ocakoglu, European Union representative to the United States, reviewed the strategies employed by European nations to achieve supply chain security. Jan Benini, retired from the US Department of Transportation, provided the dinner speech on the work of regional organizations such as the Asia Pacific Economic Cooperation (APEC) group, the Transported Asset Protection Association (TAPA) and the North Atlantic Treaty Organization (NATO) in supply chain security. Discussants for the workshop included Daniel Goodrich, Senior Transportation Security Scientist and adjunct professor at MTI; Herby Lissade, Deputy Director, Caltrans; and CDR Greg Callaghan, USCG. Professor Frances Edwards, deputy director of the Allied Telesis National Transportation Security Center, MTI, was the facilitator for the event.

The outcome of the workshop was the creation of the following products: a blueprint for future research in surface transportation supply chain security, supported by bibliographies developed by Professor Szyliowicz and two graduate students, Liz Lange and Autumn Anderton, and by Professor Goodrich.

5.1 Supply Chain Security Resilience

Achieving resilience in global supply chains—a widely accepted necessity—requires dealing with the vulnerabilities of complex modal and intermodal systems.[160] In the sections that follow, the workshop's findings regarding the vulnerabilities inherent in sea and land-based supply chain transportation systems, the policies that have been implemented by the US and other actors to deal with existing and potential threats and the challenges that remain are presented.

In the critical maritime sector, minimizing vulnerabilities and enhancing resilience is complicated by the fact that ports are optimized by cargo type. For example, Los Angeles and Long Beach are

built around container shipping of goods imported from Asia, while Oakland is a container port with a focus on food exports. For the surface transportation supply chain to be fully resilient, the US Coast Guard (USCG) needs to be able to reroute ships for security reasons, but what is the ability to shift cargo to another port? Between the port organization around cargo type and the manufacturing sector's focus on just-in-time supply chains, shifting a ship's port calls to another location is problematic. It might be possible to make changes over a short term, such as for immediate response to a natural hazard event, but over the long term there would be unwanted impacts on the larger delivery system and supply chain.[161]

Hurricane Sandy had just such an impact on the Port of New York and New Jersey, the third-largest port in the US and the largest on the east coast. Although several plans were in place to manage weather notifications, port operations planning and maritime security, due to the size of the storm and the storm surge that was generated, these were inadequate. The port was closed on October 28, 2012, due to the storm predictions, and for an additional ten days afterwards owing to the severity of the flooding. Even after the port reopened, damage and loss of power kept other container facilities idle. Moreover, the USCG's resources at Sandy Hook, Staten Island and Bayonne were not fully operational for weeks due to facility and infrastructure damage.[162]

Loss of power and the resulting loss of fuel were early challenges that required the cooperation of the private sector. A private terminal operator gave gasoline to National Oceanic and Atmospheric Administration (NOAA) staff so that their boat could continue recovery operations. Restarting port services was facilitated by a public-private partnership between the private port pilot service and NOAA and the USCG's Sector New York personnel. The private pilots stayed in the harbor during the storm, quickly began operations and carried their federal partners through the port to conduct the harbor surveys, which in turn facilitated the reopening of less damaged areas.

Ports cannot operate without surface transportation to move the cargo once it is off-loaded, so that, although the pier was clear, the storm surge, flooding and loss of power made the surface movement of goods difficult, as roadways were clogged with debris. Cargo containers were picked up by the flooding and floated around the harbor creating navigation hazards and damaging the contents. Cargo ships bound for the Port of New York and New Jersey were redirected to the large container port complex at Norfolk that had suffered less storm damage. Ships stranded at sea by the storm were redirected to berths at Baltimore and the Port of Virginia.[163]

Even lesser storms can cause major disruptions, as shown by the even more complex impact of Hurricane Harvey in 2017 on the Port of Houston. The second biggest port by tonnage (after Port of Louisiana on the Mississippi), it is the largest petro-chemical complex, shipping 38% of US gasoline exports and serves a petroleum and chemical industry economy. Though less damaged than the Port of New York and New Jersey had been by Hurricane Sandy, with no visible damage to containers or cranes, the port was closed for seven days while the ship channel was dredged. Ships awaiting berths had nowhere to be diverted. Thus, its closure impacted national and

international oil supplies[164] and created significant resilience challenges along all the supply chains and their transportation systems.

Since surface transportation is a 24-hour operation with no surge capacity, all its elements must be working for the surface transportation supply chain to function.[165] In the Bay Area, the Association of Bay Area Governments has estimated that 1,700 road segments would be damaged by a regional earthquake, disrupting the movement of vehicles throughout the Bay Area,[166] including trucks to and from the Port of Oakland, which is a major food exporter. Some of the food is fresh and delivery-time sensitive. Refrigerated containers have to be powered to preserve the contents, but natural disasters often disrupt local power supplies. Refrigerated containers on ships waiting to be off-loaded have to be monitored to ensure that the power continues to be provided, but if the container is on the third tier or above, it cannot be monitored. Shippers are seeking a technology-based monitoring system, but then it would be vulnerable to cyber-attack. The loss of power to refrigerated containers would mean more than the loss of luxury food. For example, all the milk distributed in Hawaii arrives from refrigerated cargo containers that would be vulnerable to loss of power.[167]

Interstate 10 (I-10) serves the Port of Los Angeles and Long Beach and ends at Jacksonville, Florida. Eighty miles east of the California port, the interstate highway goes through the Cajon Pass, which lies between the San Gabriel Mountains and the San Bernardino Mountains. This rift created by the movement of the San Andreas Fault is the US "land bridge," I-10, carrying the rail and truck supply chain from the port to inland distribution centers, all the way to the east coast connections to Europe. It is a point of vulnerability for the supply chain, especially if the San Andreas Fault were to rupture there again, or if terrorists undertook sabotage. Blocking I-10 could have major consequences, for it would create a denial of service for the ports and the stoppage of the supply chain. Nor is there any easy workaround since the closest transcontinental route is I-80, 380 miles to the north, which connects San Francisco to New York City.[168]

Another threat to surface transportation supply chain resiliency is the cargo itself. Dangerous goods are moved in containers, raising issues related to their regulation and stowage. Fireworks, cigarette lighters and lithium batteries all present a potential threat to the goods sharing the container and even to the adjacent containers. E-commerce has no supply chain integrity, with shippers and consolidators often unsure of the dangerous goods regulations governing their cargo. In addition, to avoid extra costs and hazardous materials licenses, shippers may intentionally mislabel or mis-declare dangerous goods.[169]

Personnel can also pose a threat to the resilience of the surface transportation supply chain. In the maritime segment of the supply chain, crew members come from many nations, predominantly from India, Indonesia and the Philippines. Large container ships have relatively small crews because of the automation of many of the ship's operations. The New York Times notes that the mega cargo ships are "the pack horses of globalization, carrying $13 trillion in goods, representing 70% of total freight worldwide."[170] The cargo containers are stacked ten layers below deck and ten

levels above deck. The crew numbers only 20 to 30 personnel, about half officers and half crewmen. At any time, there are about 1.2 million mariners at sea.[171]

Under normal circumstances, crew members are at sea for about four months at a time. Ship management firms arrange for a crew member to join the ship, work the contract, and be flown home from the next possible port at the contract's end. During the long cruises, morale is important, so the shipping line is expected to provide games, entertainment and communications capabilities for the crew. This is in conformance with both union contracts and international conventions on mariners' comfort. However, mariner interactions with the technology systems can easily lead to a loss of ship security, as when a crew member charging a cell phone introduced a virus into the ship's systems, causing the loss of the navigation charts. Thus, it is widely acknowledged that cyber systems pose a unique security challenge.[172]

To meet all the challenges enumerated above, the primary actors in the maritime enterprise—USCG, port facility managers, cargo forwarders, ship owners, utility providers and cyber systems users—need to develop vulnerability and resilience metrics for the complex systems involved in Surface Transportation Supply Chain Security (STSCS). The interrelated systems rely on each element operating successfully to achieve the safe and secure delivery of goods in the surface supply chain.[173] One strategy might be the application of the National Academy of Sciences' measures of resilience to the STSCS sector. Their report, Disaster Resilience, suggests that four functions define resilience: (i) planning and preparation, (ii) absorption, (iii) recovery, and (iv) adaptation.[174] These closely match the Federal Emergency Management Agency's four phases of emergency management: planning, response, recovery and mitigation.[175] The various USCG initiatives use these elements for maritime security, but other transportation modes in the supply chain may need a more intentional approach to developing policies that support resilience.

5.2 State of the Practice in Maritime Transportation Supply Chain Security

The US Department of Transportation's national maritime strategy, "Goals and Objectives for a Stronger Maritime Nation: A Report to Congress," issued in February 2020, included four new goals, focused on the role of the maritime sector in national security and the economy:

- "Goal 1: Strengthen U.S. Maritime Capabilities Essential to National Security and Economic Prosperity
- Goal 2: Ensure the Availability of a U.S. Maritime Workforce that Will Support the Sealift Resource Needs of the National Security Strategy
- Goal 3: Support Enhancement of U.S. Port Infrastructure and Performance
- Goal 4: Enable Maritime Industry Innovation in Information, Automation, Safety, Environmental Impact and Other Areas."[176]

In placing resiliency ahead of efficiency, the strategy reinforced the Jones Act's importance in maintaining domestic sea routes in American hands, encouraging the development of a more robust maritime capability for Sealift Command, development of private sector infrastructure, and the key security role of US flagged vessels.[177] These factors are critical as the US is faced with a growing set of geopolitical challenges to its surface transportation security, notably from China.

Geopolitical Challenges

International Ship and Port Facility Security Code (ISPS)

Following the 9/11 terrorist attacks on the World Trade Center and Pentagon, using airplanes as missiles, the US Congress passed the Maritime Transportation Security Act (MTSA) in November of 2002. It lists security standards for US ports and for all vessels that use them. The USCG was given the responsibility to monitor anti-terrorism measures in foreign ports and to provide training for foreign port leaders who want to improve their security. In July, 2004, the regulations to implement the MTSA were approved. The goals are to prevent loss of life, damage to the environment, economic disruption and transportation system disruption.[178] The Coast Guard and Transportation Security Administration jointly manage the Transportation Worker Identification Card (TWIC) program that uses background checks and security threat assessments to evaluate the potential for threats and issue cards for mariners and transportation workers with access to MTSA vessels and port facilities.[179]

In response to the potential for ships being used for terrorism, the United Nations' International Maritime Organization (IMO) created the ISPS to minimize the likelihood of ships being used as weapons in terrorist attacks. For example, "gas ships might be hijacked and blown up in busy ports."[180] The code was implemented "through the International Convention for the Safety of Life at Sea (SOLAS), 1974 chapter XI-2 to enhance maritime security,"[181] and came into force on July 1, 2004.[182] The IMO made these actions international requirements for security programs in shipping companies, in ports and on the ships to protect against terrorism and piracy. The cost of implementation of the security planning and equipping by the ship owners and port operators is borne by freight shippers through an ISPS fee.[183]

A port has to meet ISPS requirements for international shipping to call. Once a ship calls at a non-ISPS port, it may be denied access to ISPS ports. The ISPS requires trained security leaders for every vessel, port and maritime company, with the goal to deter piracy, terrorism, stowaways and any tampering with the safety of the ship or crew.[184]

The way that the US works with foreign countries on port security depends on local agreements. Counter-terrorism work is uniformly supported in the world's major ports, but countering drug trafficking is harder because of government corruption, enabling drug cartels to buy influence in some host nations. Criminal enterprises may also be influential in the port through bribery of officials or influence in the labor unions. There also has to be an agreement between the US and the port's government regarding the level of threat from different vessels that is acceptable. For

example, a Russian flag ship may be viewed as a threat in the US and Canada, but not in another country. Sometimes there is a reason to withhold enforcement and see the criminal network in action to allow for arrests rather than to initiate deterrent action.[185]

Domestic and foreign politics and regimes, trade agreements and escalation of violence quickly change the security landscape in maritime transportation. TWIC provide some ability to identify who is authorized to enter a port, but enforcement is a shared responsibility between the port and the national government of the port. Often nations were built around their ports, and even today, in some places, residents are integrated into ports, and cargo is stored in neighborhoods in Africa and southwest Asia. Since such arrangements do not comply with the security elements of the ISPS, these ports cannot be used for international trade until ISPS compliance is achieved. Port security improvements since the 9/11 attacks on the US are notable, and the US has tried to extend its port security regimes to other nations through diplomacy. However, other nations remain focused on issues of concern within their societies. For example, Indonesia and Malaysia have cards that say, "Drug trafficking is punishable by death." Still, despite all such efforts, crime is still a vulnerability throughout the maritime supply chain, especially the human elements.[186]

Deterring human trafficking is particularly challenging in foreign ports. Security monitors tend to trust the manifest for the container. Some containers get X-rayed by US Customs and Border Patrol (CBP) officers, but only those being imported into the US All containers get scanned for radiation. Most ships have a foreign flag, foreign operator, and foreign crew, so port security has to rely on worldwide intelligence gathering about criminal enterprises to disrupt human trafficking using cargo containers. If there is nothing intelligence-driven, the container is put on a truck to its destination.[187]

As has been noted, container ships are growing in size. In May of 2020, the largest container ship was the HMM Algeciras, at 1,312 feet long and 200 feet wide, own by Hyundai Merchant Marine. The ship was built in South Korea and flagged in Panama. On its maiden voyage, it stopped at the Port of Rotterdam on June 3 with a record load of 19,621 TEUs, but it is capable of carrying 23,964. Unloading the mega-ships requires carefully choreographed coordination of port, crane and trucks, creating severe limitations on container scanning time frames. Container security inspections are run by CBP, while port security compliance with ISPS is overseen by the USCG.

Chinese Maritime Silk Road and Ports

Within the framework of these regimes, international trade involves a variety of vessels calling at multiple ports around the world. The management of ports has become highly sophisticated, with the need to enforce the international laws, and with the use of high-speed cranes that are cyber enabled to connect the ship manifest to the truck or train that will move the goods from the port.[188] Ports must provide not only berthing for ships and unloading capacity, but also cyber systems and connectivity.

China has undertaken the ownership or management of ports around the world. In some cases, the mainland Chinese maritime giant COSCO has bought out port contracts of Hong Kong-based entities. This raised security concerns within the US, and Chinese ownership ended in many cases. A good example is the Port of Long Beach, which gets 90% of its containerized cargo from Asia.[189] For thirty years, the Port of Long Beach, the second largest containerized port in the U.S, was owned by Hong Kong-based Orient Overseas International (OOI). The COSCO shipping empire acquired majority shareholder status in OOI in 2017, causing the Department of Homeland Security (DHS)—of which the Coast Guard is a part—to raise concerns. In 2019 the port was bought by a North American private equity fund called Macquarie Infrastructure Partners under an agreement between COSCO, DHS and the US Department of Justice, which included a commitment from OOI and COSCO to use Long Beach for port and rail services for the next 20 years.[190] This ended a 40-year lease on the Long Beach Container Terminal that was signed with OOI in 2012, before the COSCO buy-in.[191]

China aspires to build a Maritime Silk Road to support its global trade. The warm water route will travel from Fuzhou, China to Vietnam, and along the coast of the Indian Ocean to Iran, and Kenya on the south, to the Suez Canal, to Mediterranean ports, ending in Italy. China is planning to add a polar extension to its Maritime Silk Road projects, connecting its port at Dailan on the Pacific directly to Rotterdam.[192]

In a 2019 Congressional hearing, Carolyn Bartholomew, chair of the US-China Economic and Security Review Commission, noted that control of ports in Africa, Europe and Asia gives China an advantage in logistics supply chains, especially the import of raw materials for its manufacturing economy and its export of finished products. China's Maritime Silk Road initiative extends existing commercial contracts through loans to domestic entities and purchases of port facilities.[193] China has a controlling interest in two-thirds of the 50 largest container ports in the world, including investments in Los Angele and Seattle. Through its acquisition of a 49% stake in French Terminal Link, it also controls the US ports of Miami and Houston.[194]

Additional vulnerabilities noted in the 2019 hearing included that the gantry cranes needed to unload the large container ships in US ports are made in China. Further, the US does not own or control ships needed to refuel US Navy vessels. California Congressman John Garamendi sponsored a bill requiring the construction of 50 US constructed and flagged refueling vessels.[195] To counter the Maritime Silk Road, the US military needs to complete a National Maritime Strategy that examines all aspects of maritime supply chain security. Lt. Gen. Giovanni Tuck, responsible for the movement of US troops abroad, noted that while the USCG maintains physical security for ports, "we're talking about the resiliency of a port and the cyber threat that can go with that, including with these mega cranes."[196] Chinese programming of the gantry cranes' operating systems leaves room for bots and malicious code to be introduced into their cyber-based operating systems.[197]

Port management companies from Dubai and China dominate the container shipping industry.[198] Modern ports have highly complex infrastructures, including reliance on cyber systems. For example, Busan, South Korea, relies on a GPS-dependent surface transportation system. Threats such as GPS spoofing exist when ships are navigating in the harbor. China had a spoofing incident in Shanghai, although it may have been due to a bandwidth problem rather than intentional hacking. Nevertheless, the challenge for maritime security remains.

China uses 5G broadband (a more robust network for moving data) widely in its ports. Of more concern, they have also developed their own GPS system called Beidou. After two decades of development, the final satellite was placed in orbit in June of 2020.[199] Mariners might be required to use the Chinese system in Chinese waters. Receiving information from the Chinese system would be acceptable, but transmitting could be an intelligence concern.[200]

The Maritime Silk Road initiative goes beyond simple port access. Chinese investment in Africa and Central America includes building soccer stadiums, hospitals and roads. Chinese workers and companies install everything; then, the debt has to be repaid by the host nation. Ports in Eastern Africa provide the Chinese military with the ability to land blue water navy vessels. These new commercial ports around the world offer Chinese military units global reach for logistical support. The projects can also generate new relationships with small nations that can later be used for Chinese benefit. For example, the Chinese build a fish processing plant as an economic development project, lending the money for the construction. The debt is slowly repaid to China, and the country now has a debt diplomacy relationship to China, a situation which is most notable in Oceania. Cruise ship terminals built to enhance the influx of foreign currency and grow the local economy can also accommodate a naval destroyer for port calls and resupply.[201]

The Chinese are developing similar relationships in Europe, owning large terminals in Brussels, for example. The new port serving Athens is an example of Mediterranean debt diplomacy. They go to a nation when it has financial vulnerabilities and build-zones of influence. Thus, the Chinese bought Piraeus, a small port outside of Athens, during the Greek debt crisis, made it a modern container port, and undercut the Greek shipping magnates, cutting out the main Port of Athens. In 2019 China agreed to a further 660 million Euro investment in Piraeus by COSCO to create a hub for Asia-to-Europe shipping, with the goal to make it the largest container port in Europe.[202] Ports and roads in the western Balkans were built using Chinese labor to undercut local bidders. The cost-saving and new infrastructure initially make the local leaders happy, but the outstanding debt creates political influence for China.[203]

The Melting Arctic

Another pressing geopolitical issue is the development of new trade routes through the melting Arctic Ocean. The summer retreat of the ice for up to 75 days has permitted the development of the northern coast of Russia, including the exploitation of mineral resources. Trade routes linking Vladivostok on the Pacific coast with the Yamal Liquid Natural Gas Project on the north coast can operate through the summer, shortening the trip to Asian customers. The Russian icebreaker

fleet has developed with both nuclear powered and diesel-powered vessels. Russia has created floating nuclear power plants to support the commercialization of the northern coast, with plans for additional installations.[204]

Russia is exploiting the Arctic for military purposes. New deployments of naval and air forces menace Alaska and raise concerns about the passage through the Bering Sea. Guided missile patrol ships have been added to the Russian Arctic fleet. Land-based exercises have included the deployment of troops who walked across the peninsula from Cape Vankarem to Egvekinot as part of the Vostok 2018 event.[205]

The Russian telecommunications company Mega-fon is a partner with Cinia, a Finnish firm, in developing a new submarine fiber optic cable that will run along Russia's northern coast, not in territorial waters, but along its continental shelf. The Arctic Connect Project will add an 18,000 km cable to connect Europe, Asia and the US. The Chinese have expressed an interest in this project as part of their One Belt, One Road system.[206] The planned cable will run to Hokkaido, Beijing, Vladivostok, Kamchatka, through the Being Strait into the Arctic Ocean and along Russia's northern shore.[207]

The melting Arctic ice is also opening the fabled Northwest Passage, from the Atlantic to Hudson's Bay and across the northern coast of Canada to Alaska's North Slope oil fields. Passage through the Bering Strait connects the Arctic Ocean to the northern Pacific Ocean. These new trade routes are leading to sovereignty disputes among the nations with Arctic Ocean frontage, the "coastal states." The US and Canada have issues with boundaries in the Beaufort Sea. A much bigger concern is Russia's claims to the major European trade route where the Baltic states also lay claims.[208] Under international law, all coastal states have a three-mile limit that is national territory, which is measured from the low tide mark, or the farthest point of the harbor infrastructure, out to sea. Under the United Nation's Convention on the Law of the Sea, nations have another 12 nautical miles of territorial sea where they control the air space, seabed and subsoil. Ships may engage in innocent passage, but not in any commercial, fishing or landing activities without the permission of the state.[209] An exclusive economic zone then extends for another 200 nautical miles where the coastal state has control of fishing and extraction industries.[210] It is this zone that causes the most overlap of national sovereignty as the lines of longitude converge.

On the Pacific side of the Arctic Ocean, there is only the Bering Strait to provide access between the two oceans. With a frozen Arctic, there was little need for vessels to move into the Arctic Ocean through the strait. Now that Russia's northern shore is developing extraction industries, the demand for seasonal passage by tankers and supply ships is increasing. Since the navigable passageway is relatively narrow, it is possible to imagine a time when the strait will be as crowded as the Strait of Malacca, with ships lining up for days to await their turn to pass through. Clearly, the melting Arctic poses a variety of geopolitical challenges for the twenty-first century.[211]

Maritime Management Security Challenges

Maritime management poses a variety of security challenges. Experts have described its ecosystem as a trade-driven challenge. Fixed assets such as ports, cranes and warehouses are working with mobile assets such as ships, trucks and rail cars to move goods across the supply chain. The economic impact of this ecosystem is significant, with the western US ports managing $1 trillion a year in import and export goods.[212] These goods are used in the US manufacturing sectors, as well as exported again from east coast ports to Europe.

Components of Port Security

The USCG's 11th District covers all of California. Sector Los Angeles/Long Beach combined is the largest container port in the US, and ninth largest in the world. It received 16 million containers in 2018; 43% of western US refined oil products come from this port, as do 75% of California's. Three cruise lines operate out of the port. It has an automated terminal that can handle mega-ships with high-speed cranes. Sector San Francisco includes the largest passenger ferry fleet in California, carrying 10,000 people per day, and has the largest military outload port in the state. The Port of Oakland is the fifth largest container port in the US, with 2 million containers handled in 2018, and ships 25% of California's refined gas products.[213] The Chinese mega container ship, Benjamin Franklin, carrying 16,000 containers, visited the Port of Oakland on New Year's Eve, 2015, on its maiden voyage.[214] Sector San Diego is home to the US Navy's Pacific fleet and is the second-largest surface ship US Navy base in the world, with 54 ships. The port generated $9.4 billion in economic impact to the region.[215]

A 2015 west coast port strike by the Longshoremen's Union demonstrated the impact on the economy of the loss of port capacity. Six days into the strike, manufacturers ran out of supplies due to just-in-time management, which eschews stockpiling of components. The 30 striking west coast ports cost the US economy $2 billion per day. "Longshoremen play an indispensable role [216]in getting 90 percent of consumer goods into the country—and they know how to use that to their advantage."[217]

Providing security to such important facilities is a challenge because of the large attack surface provided by the enormous amount of maritime trade. The elements include ports, terminals, vessels, cargo, supply chain, people, and communications. It is a transaction-rich environment, which attracts criminal elements. Security requires that maritime partners improve information sharing related to threats and vulnerabilities and reduce known vulnerabilities through regular reviews and improvements. A layered defense against security breaches includes continuous monitoring and development of a resilient operational program.[218]

As with all industries, maritime shipping focuses on efficiency to enhance return on investment. These improvements include automation of processes, the introduction of cyber capabilities that enhance the ability to have remote access, monitoring and reporting, and the convergence of activities and dependencies inherent in the internet of things (IOT). It is a difficult management

decision over whether to prioritize efficiency by using outside contractors for these automated activities, or to hire a more expensive in-house information technology staff to manage the cyber-based activities. The choice is between the superior capability and lower cost of contractors who focus on one aspect of cyber and are specialists—but also could be the source of hostile cyber incursions, versus the higher security of an in-house cyber management approach, but with employees who must work across multiple cyber platforms. "Every additional layer introduces risks that need to be managed."[219]

Security Laws and Regulations

Recognizing the security vulnerability of shipping, a variety of new laws and regulations were introduced after the terrorist attacks of 9/11 that used airplanes as bombs.[220] The opportunity to use ships similarly to damage ports or disrupt the supply chain was recognized, and the US created the US CBP program called Customs–Trade Partnership Against Terrorism (C-TPAT) that was begun in 2001. Its goal was building partnerships with other nations for inspections of goods in the country of origin before they are shipped. Partnerships include importers and exporters, customs brokers, freight consolidators, as well as trucking companies and shipping companies. In 2006 the program became law and now has 11,400 partners.[221] The MTSA, passed in 2002, established maritime security levels.[222] The MTSA regulations are published in 33 Code of Federal Regulations 103, 104, 105, and 106, which lays out the security requirements for domestic port facilities and US-flagged ships and certain offshore oil rigs. Naval Vessel Inspection Circulars (NVIC) published periodically provide guidance to the industry. The Public Health Security and Bioterrorism Preparedness and Response Act of 2002 requires that the US Food and Drug Administration (FDA) must be notified in advance of all food imports to facilitate inspections.[223]

The ISPS was adopted by the IMO in 2004. The USCG's port security program was started in 2002–2003. The USCG accesses intelligence and analyzes world events to ascertain possible threats to the supply chain. Program partners include 150 nations with coastal access, of whom 70 are active trade partners with the US. Countries are divided into three risk levels, with strict enforcement for Tier 1 nations.[224]

The ISPS regulates the ship-to-port interface. It relies on CBP to regulate the cargo through its C-TPAT program. Within 96 hours in advance of arrival, a ship must notify the receiving port of its cargo, passengers, crew, and other ports it has visited. CBP looks at people and cargo, while USCG looks at ship history. Conditions of entry into the port for the ship are based on the USCG's evaluation of whether the ship is a risk to the port, including the security posture of the ship's previous ports of call. Being prevented from a timely entrance into the port costs money and causes delays to market for the goods. A port security advisory may be issued, which may be due to failure of the port of origin or last port of call to follow port security rules. If the port of origin or last port of call does not comply with ISPS, shippers will not serve that port because of the disruption to their later port calls.[225]

The USCG can revisit the problematic port and provide capacity building guidance to clear it for secure international trade. The USCG's goal is compliance with the ISPS regulations, which it enforces in foreign ports, using the "carrot" of trade with the US to encourage the development of appropriate security standards. A port that cannot export may damage the local economy and even impact national stability. US Agency for International Development and the Millennium Corporation may help to fund compliance with ISPS Code, but it is left to ports to implement the regulations by installing cameras, fences, and other security devices, with the goal to prevent a breach. The USCG enforces the MTSA once the ship is in US waters.[226]

Global peer pressure through allies helps to get ports in other nations to enhance their threat tier. Tier 3 areas include all the nations of the European Union, Australia, Japan, and other trading partners that are evaluated by intelligence estimates as low risk and whose ports have a low rate of non-compliance with ISPS security requirements. Tier 2 includes most of the rest of the US's trading partner nations. Tier 1 is high risk areas, including Iran, North Korea, Cuba, Myanmar, and any state sponsors of terrorism. The USCG tries to visit nations on the Tier 3 or 2 list to create the conditions to enhance diplomacy through maritime trade. However, Eritrea, for example, would not accept the invitation, so no ships from that country may enter US waters. The Arab spring of 2010 took nations of North Africa from Tier 2 to Tier 1 until violence subsided. The USCG was able to access Myanmar and explained how they could get their port to become part of international trade, and they are working on meeting the requirements. When Cuba opened to the west, the USCG worked with them to develop compliance with the ISPF for their ports.[227]

US government classifies terrorist groups and nations tied to them, while the Drug Enforcement Administration (DEA) monitors the "narco" side. Ships coming from such ports are subject to scrutiny under the ISPS. The USCG works to get cooperation on ship tracking. They use time and distance to screen information provided under the ISPS as the ship transits to the US port. USCG's role at the intelligence table is to use the Maritime Operational Threat Response to evaluate risk; and either formulate a plan to intercept the ship at the 200-mile limit or allow it to make port and respond. The local Fusion Center evaluates the Advance Notice of Arrival provided under the regulatory side; then, criminal evaluation may determine that a ship is a "vessel of interest." The threat type determines the response.[228]

Policy Development

After the 9/11 attacks on the US World Trade Center and Pentagon, new security regulations were developed for many elements of transportation. For example, C-TPAT was expanded into the supply chain, and new security criteria now include cyber and bioterrorism rules for food imports. To qualify for C-TPAT designation, a shipper must demonstrate the documentation of a power outage plan that enables the continuation of operations. The plan must encompass power losses from system failures and weather impacts. All computer operations must use two-factor authentication.[229] All ships using US ports are required to have an automated tracking system (AIS) that allows the ship to be tracked using GPS. Each ship has a unique signal that broadcasts the

ship's name, course, speed and other details. It broadcasts 4,500 messages per minute, with a range of 40 miles. This allows the USCG to monitor incoming vessel traffic for safety and security purposes.[230] Maritime shipping companies are responsible for tracking their own communications and having a process for dealing with reports of AIS and GPS spoofing incidents.[231]

Cyber is another support system that must be included in security planning. Cyber monitoring is conducted in McLean, Virginia, but defining maritime messages is a challenge. There are now self-driving vehicles in maritime terminals that use cyber systems, a new cyber layer. There are few American domestic shipping companies, and many US ports are run by foreign companies, which compounds issues of control. Foreign entities are less likely to share information on cyber events with USCG than American owners. The Jones Act states that all goods moved between two US ports have to use US-built and owned ships. This provides layers of cybersecurity and integrity. Servers, however, may be located away from the port, even in another country, creating an MTSA enforcement problem. Shipping companies argue that moving computer servers out of the US is often justified on the basis of cost and efficiency, but often it is to evade US regulations. Malaysia and Indonesia port headquarters planned to carry out a cybersecurity demonstration in 2020 for the USCG to prove that their locations are both secure and efficient. US domestic operators are struggling to remain competitive with foreign shippers while also ensuring the security of their systems. For example, Matson has to carry out their own inspections in China through C-TPAT for customs. The process to approve foreign ownership of ports, ships, and logistics components as part of a supply chain is complex and requires writing security requirements into contracts for logistics support services.[232]

The US Coast Guard uses a variety of methods to ensure the security of US ports. The National Targeting Center (NTC) is part of the Department of Homeland Security and run by US Customs and Border Protection (CBP). It uses several software packages to track goods in the supply chain for security. The US partners with many other nations to ensure the integrity of the maritime cargo systems.[233] For example, Columbia coordinates with the CBP on cargo monitoring. It puts GPS trackers on its goods in transit from the factory forward, connects to NTC and tracks the goods in the cargo container to the final destination, such as a Walmart distribution center.

Drug and drug component transporting and smuggling are also concerns for the international supply chain system. Columbia, which was previously known as a major source of drugs smuggled into the US, is now the most advanced national port system in Central America, with MTSA and ISPS compliance. US diplomatic influence was used to develop alternate trade in legal goods, but the national government now requires security regulations for all goods in commerce. Guatemala and El Salvador are now the focus of concern as precursor drug providers.

While CBP monitors the movement of the containers, the USCG monitors the movement of ships[234] of 300 gross tons or greater headed for a US port or traveling within 1,000 nautical miles of the US coast, using the International Maritime Organization's (IMO) Long Range Identification and Tracking system (LRIT). The LRIT reports the ship's location at least every

six hours,[235] and maintains a log of the ship's voyage up to that time, allowing the USCG to evaluate ships for threats. If a ship turns off the LRIT its voyage history is lost. Doing so is suspicious, suggesting that it made unauthorized stops or used unauthorized routes. Other approaches to ensure port security are used in other nations. For example, Israel takes fingerprints and photographs every mariner arriving at an Israeli port. In California, the ports are linked to local intelligence sharing groups (fusion centers) and share information about risks from international flag port arrivals.[236]

The ISPS/MTSA Security Compliance Targeting Matrix provides an analysis of ships' voyage histories. Ports of call history is a major concern for container ships since cargo containers could have been tampered with. Ships that have made port calls at suspicious or poorly secured ports may require extra scrutiny before being permitted to off-load goods or personnel at US ports. For example, ports in the Philippines are not considered secure, so if a ship has gone to a port there within the last five port calls, the USCG will place conditions of entry for the ship to enter any American port.[237]

The USCG works with US ports to evaluate security concerns, find deficiencies and create solutions. A variety of plans are required for port facilities to minimize risk. Vessel Security Plans, Facility Security Plans, and Area Maritime Security Plans each play a role in developing a more secure port. The USCG Captain of the Port is in overall charge of all security operations of the port and holds quarterly meetings of federal, state and local entities with an interest in port security to assess the plans and strategies currently in place. The group uses scenarios such as a terrorism event to evaluate the capabilities of that port to respond successfully to identified threats. The exercise helps to disclose existing security deficiencies. Funding is available to ports to harden systems and facilities against terrorist attacks, based on the Maritime Security Analysis model, which offers methods for mitigating against those identified vulnerabilities.[238]

Other policies and plans are required to reduce the risk of smuggling, human trafficking, cargo theft and terrorist acts. American and foreign flag ships must take steps to prevent their vessels from becoming the source of criminal or terrorist actions. Navigation and Vessel Inspection Circulars (NVICs) provide guidance to the maritime industry to comply with the Maritime Transportation Security Act (MTSA). The Code of Federal Regulations (33 CFR 103, 104, 105) requires the creation of security plans, implementation of security measures, and specific activities for cargo handling. The High Interest Vessel Boarding Matrix helps USCG leadership to identify target vessels based on intelligence. The USCG, Federal Marshals' Service, Federal Bureau of Investigation (FBI) and CBP respond together to investigate possible criminal activity or other threats involving a suspect ship.[239]

5.3 Cybersecurity Challenges

The vision of mariners at sea finding their way around the globe with the stars and a sextant is now out of date. Today's mega-ships navigate using GPS-enabled charts that require cyber

technology to work. Electronic Chart Display and Information System (ECDIS) is a digital version, multi-layer database that is now replacing the paper navigation chart. Ships use USB-enabled data as back-ups, but in one instance, someone introduced a virus through cell phone charging, which meant that the ship now had no chart.[240] ECDIS & GPS are not only essential for navigating at sea, but they are also critical in the navigational channel area where a large vessel is very vulnerable to navigation hazards. Other critical operating systems such as AIS, NAVTEX, the ship's speed log and fathometer are all tied to the ECDIS.[241]

The maritime industry is deeply embedded with developing information technologies that create efficiencies and safety in the management of maritime resources. Cyber-enabled operations, automation of scheduling and crane operations, remote access to facilities, monitoring and reporting are all part of the new maritime operations. New dependencies have been created by the IOT, which makes every device a window into a ship's operating system. For example, at the port in Busan, South Korea, there is one operator for eight cranes, all controlled through computer-based systems, and autonomous vehicles are used on the port facility. Each poses a possible risk of cyber-attack.[242] Ships are not the only maritime facilities vulnerable to cyber system failure. In 2010 an oil rig lost stability when it lost its cyber navigation systems. Since floating platforms require navigation to stay in position, the oil rig suffered the loss of electric supply, loss of station and had to make an emergency disconnect.[243] There were 14 computer viruses that corrupted the primary navigational computer.[244]

The challenge for management is to determine whether efficiency or security is the dominant factor in IT system design. The increasing outsourcing of information technology (IT) systems designs to specialized third parties is one option that gains efficiencies, while doing everything with in-house staff may lose the benefits of specialization but provide a higher level of system security.[245] For example, the APM Terminals in Rotterdam, a Maersk enterprise, suffered a Petya ransomware attack on June 27, 2017, which may have been made possible by "loopholes" in the cybersecurity systems.

The Maersk attack is believed to have started as a virus in a Ukrainian accounting software update, which exploited a flaw in the Windows operating system. The company removed computers tied to the regular network, but this action failed to prevent the stoppage of automated cargo operations at numerous terminals. The security system at the marine terminal was also affected but able to remain in compliance.[246] Worldwide, 17 terminals were impacted, and the only cure was to erase the hard drive completely and restore the system with an uninfected back-up. Maersk found a server in West Africa that had been off-line for service during the attack and used it to restore services. This solution demonstrates the importance of maintaining some back-up capability off-line since the malware can spread across the entire network.[247]

During the attack, the IT systems used to schedule ship arrivals and cargo handling had to be replaced with "paper and pencil systems."[248] When Maersk Shipping suffered its cyber-attack, Matson Lines resorted to these old-fashioned systems at the port in Tacoma to manage their

operations. They have one ship two days a week at the port, so they were able to maintain operations with manual work. Verizon experienced a loss of service in Oakland, a major port for Matson, where they had an effective cyber-contingency plan. Their systems were segregated from the main systems and included a cloud back-up on the east and west coasts.

Restoration requires knowing what normal looks like. What are the assets and how are they connected? What are the latest configurations? Which users have to be brought back on-line? Are there back-ups? For example, new chips in a ship's engine operation system use cyber monitoring to improve efficiency. Systems such as ballast can be impacted to manage the engine's load for the best operation. If the chip were hacked, the ballast water could rush to one side of the ship and cause it to list, perhaps dangerously.[249]

Cyber systems are also used to ensure that paperwork gets transmitted to support trade. The value of data sharing is recognized along the supply chain, although shippers and operators want to retain some power to decide who gets the data. Big corporations have software for data management, but small vendors and suppliers have to manage the data exchange on their own. To do this, they have to build the rules of the game—who is allowed to participate, contribute data, or get data?[250] Vessel connections are a critical aspect of cybersecurity. Modern cargo vessels are largely operated by computer-enabled systems that the crew interfaces with but does not directly control. Networks on ships control navigation, propulsions, power, and communication. The whole of business connections integrates the vessel with the marine terminal operations and landside facilities. International headquarters' IT systems are tied to the ship's operating systems, which created efficiency but also vulnerability.[251]

On September 27, 2018, the Port of San Diego was subjected to a ransomware attack,[252] suspected to have been introduced to the network through a networked security camera system. Based on their cybersecurity protocol, other systems voluntarily shut down to stop the spread of the ransomware. No commercial impacts were felt at the port because there was little automation on the cargo side. The attack affected San Diego Harbor Police operations, but the port was able to remain in compliance with Facility Security Plans.[253]

These events point out the need for data governance in the supply chain. How much is invested in the pursuit of data security is determined by the evaluation of the risk to the systems. Doing so requires attention to the three components of risk—threat, vulnerability, and consequences. Data governance is intended to create information assurance via cybersecurity. Data governance is the foundation of managing the supply chain and protecting its physical and intellectual property.[254]

Data hygiene is essential to protect the systems from incursions, but the social norms of password security and safe computer operation are not yet fully embedded in business culture. While double passwords and frequent changes of passwords can be built into the computer access systems, there is only so much that management can mandate. Information security has to become automatic for users, both "right and left of boom," before and after an attack, because, for the supply chain industry, it is not a question of if, but when, an attack will occur. Cybersecurity market segments

are becoming ever more important to the operation of modern vessels, ports and supply systems. Devices, applications and networked data are all part of the supply chain ecology. All users have a degree of dependency on cyber-moderated data. The role of the cybersecurity sector must be to identify potential vulnerabilities, and when intrusions begin, protect, detect, respond, and rapidly recover the systems.[255]

Cybersecurity is a means to an end for safer transactions. Supply chains are increasingly dependent on data flows, such as the logistics systems of users, Supervisory Control and Data Acquisition (SCADA) systems, and regulatory systems. In the supply chain, the physical space and cyber space have to interact together. Compromised elements can seep through the network routers. The challenge is that the infrastructure depends on multiple data types, multiple data clouds, so the question is, "what do you want to secure?" Is protecting everything sustainable? What are the impacts of loss to the supply chain partners: suppliers, vendors, stakeholders, along the chain?[256] The answers dictate the type and level of the investments in cybersecurity.

The USCG has established the Office of Cyberspace Forces (CG-791) to oversee the safety and security aspects of cyber systems in the maritime industry.[257] The USCG provides guidance on how to protect cyber systems through NVICs, thus enhancing the ability of the field personnel in carrying out inspections and other regulatory actions.[258] One such effort is the Draft Facilities Cyber NVIC issued by the Office of Port and Facility Compliance (CG-FAC),[259] which the Office of Management and Budget (OMB) characterizes as major rulemaking since this regulation when published, will give the USCG oversight of computers in maritime-related facilities.[260] This new NVIC is intended as an awareness tool to make the maritime industry partners aware of the requirement to include "radio and telecommunication systems, including computer systems and networks, in facility security assessments."[261] The USCG has also developed a draft of an NVIC on cyber systems on vessels. The IMO already requires ships to address computers in their security plans, and cyber systems are supposed to be covered in safety management systems for cargo movement, maintenance, and safety processes.[262]

The introduction of computer-operated cranes and self-driving vehicles has added to the complexity of cyber issues at port facilities. Accordingly, CG-FAC hired Miter Corporation to analyze its Cyber Risk Assessment Models to better understand the cyber risks to a port. The USCG continues to explore information sharing across the maritime enterprise, with a view to mitigating cyber events. The National Institutes for Standards and Testing (NIST) Cybersecurity Framework provides guidance on managing cyber threats and risks using a framework of activities, outcomes and references. It sets the priorities in identifying potential risks, detecting imminent threats, and protecting critical infrastructure in the cyber realm.[263]

5.4 Inter-Sector Security Challenges

The surface transportation supply chain involves multiple economic sectors, from raw materials through the retail outlet. Multiple transactions are required to bring a product to the consumer.

The goal of transportation supply chain security is to reduce the known vulnerabilities, so as to have the capacity to deal with unexpected events. Greater security integration with partners and third parties is required all along the supply chain. This is based not just on technology but also on people and processes. When an incident occurs, how well does the security system respond? Internal security is fine, but there must also be an external data security component.[264] One goal of the transportation supply chain security system is to protect the victims' rights, to protect the facility, and the entity that suffers the security breach. One challenge is to find a security officer with knowledge of the multi-faceted supply chain systems. Large transportation supply chain enterprises may form a multi-agency cybersecurity committee that includes the multiple stakeholders because facilities operators may not be knowledgeable about cybersecurity, while IT specialists may be unaware of the vulnerabilities in the physical spaces. Indicators of compromise may be hard to get defined, and experts want to follow the trail of the crime and investigate and prosecute, not give out information. The result of this failure to communicate is that investigators often cannot tell what to look for because the victims prize their intellectual property.[265]

Stakeholders along the supply chain need to develop interagency "indicators of comprise" agreements to allow for warnings of future attacks to be shared across the transportation sector. The USCG has a cyber-response team to assist local commanders in each port. There is also the regulatory problem of rulemaking about information sharing versus creating guidance. One good example of cross-sector cooperation is the State of California's cyber center that has information sharing protocols with its ports.[266]

To what extent can federal or state agencies regulate information sharing about compromises, breeches and cyber-attacks on the private sector supply chain partners? Should companies train their staff to audit their company's internal systems? Is it better to use external third party experts? What is the trust level between the company staff and the outside auditors? Governments and small companies may be challenged to keep good cyber auditors at reasonable salaries. Because of the high cost of cyber expertise, only the oil industry has in-house experts.[267] Shipping companies use both in-house and third party experts for cybersecurity work. Within the US, the USCG is a trusted partner, but shipping is international, and other nations may not have a similar trustworthy agency. How do foreign-owned vessels fit into the information exchange?[268]

Power Sector

The power sector is another crucial partner in the transportation supply chain security effort. California has recently experienced several severe wildland-urban interface fire seasons, with loss of life and property at record levels. The power utility was at fault for several of the fires that were caused by power line sparking during wind events. To prevent such future events, they have developed a Public Safety Power Shutoff (PSPS) plan that deprives thousands of California residents and transportation supply chain partners of all power for hours to days.[269]

Many elements of the transportation supply chain security enterprise are directly impacted by a loss of power. Examples include rail crossings warning indicators, railroad signal systems, radio

systems, including positive train control systems that are essential to prevent accidents on shared tracks, traffic signals, streetlights and freeway signage. PSPS created generator requirements for sensitive facilities, has direct impacts on hazardous materials pipelines that carry fuel to airports and distribution points, including point of sale for trucking, as well as passenger cars. Cell phones and telecommunication systems rely on electricity to function. Many aspects of land transportation share the same cyber management approaches that have been described above for maritime transportation.[270]

Each electric utility in California approaches PSPS differently. Pacific Gas and Electric provides services in the northern half of the state. On October 9, 2019, 750,000 people lost power. Business impacts, including loss of refrigeration, ATMs, check clearing machines and electronic cash registers, as well as security systems, were mostly addressed through assistance at the county level. Between October 23–25, 2019, 500,000 customers were impacted. From October 26 through November 1, 2019, there was another PSPS. Southern California Edison had 181,000 customers without power, and San Diego Gas and Electric had 54,000 customers without power. Shared infrastructure was shut down, and Monterey County lost internet for a week, causing crucial delays to food shipments, just at the harvest. Altogether, 30 counties were impacted by PSPS in 2019. including 564 schools that closed, impacting 171,000 students.[271]

The Federal Emergency Management Agency (FEMA) activated Emergency Support Functions (ESF) 6 (mass care) and ESF 8 (public health and medical) to provide shelters and food because the PSPS created cascading impacts of food shortages. Stores without power did not have the connections to the distribution centers to notify the shipping department of their deficiencies. The Bay Area's Caldecott Tunnel ventilation system shut down because of PSPS, and CO2 accumulated, causing the California Department of Transportation (Caltrans) to shut down this major transportation route until new generator-powered fans could be obtained. Private water wells did not work unless the owner had a diesel generator, so many people suffered water shortages, both in the household and for livestock and irrigation.[272]

California's rail system also suffered impacts from the PSPS. The safety signals at rail grade crossings have battery back-ups, but they only have a few days' life expectancy. When the signals' back-up power failed, trains had to slow at every crossing. After the first event, the rail operators often installed generators. While the rail impact is not known to have had direct impacts on the supply chain, the generators required a coordinated fueling and maintenance system that impacted rail operations.[273] Power losses have historically lasted for only a few hours, but the 2019 fire-related PSPS events lasted as long as five days,[274] causing the grade crossing safety system failures. As the PSPS continued through fire season, there were not enough generator mechanics for the 30 counties that were impacted. There was no street lighting, so traveling to fix the generators was a challenge.[275]

Motor fuel is a key part of the supply chain system. Trucks move more than 70% of all goods in the United States or 10.8 billion tons of freight per year.[276] Fuel is generally moved from refineries

by pipelines to major distribution centers, from which trucks deliver supplies to local point of sale outlets. Power for the Kinder Morgan pipeline that transports fuel from Rocklin, California to Reno, Nevada was also shut down by the PSPS,[277] so fuel had to be moved to Nevada by truck to ensure supplies for the trucking industry. Moving fuel by truck is not a long-term solution for fuel supplies, but generators to power the pipeline would be the size of a semi-tractor trailer truck and would itself require fuel and maintenance. In the future it would be important to know the inventory level for point-of-sale access, and to have a plan in place for fuel rationing when pipelines have to be shut down.

During the 2019 PSPS, generators were used as a temporary measure, but a more sustainable future solution must be put in place. Refineries developed a fuel backlog because of the PSPS-caused fuel delivery disruptions and were going to cut production, which would have had impacts across the supply chain.[278] The port at Humboldt, California, normally receives fuel by barge to the Chevron distribution point, but it was closed by the PSPS. Trucks from Chico were the only choice to move fuel into the area. Because motor fuel is a hazardous material, and because the trucks are heavy, Caltrans had to develop routing on roads and bridges capable of bearing the weight, and the California Highway Patrol had to escort the trucks for security.[279]

When PSPS cuts normal sources of power, the generators that are substituted exacerbate the fuel distribution problems by creating a new demand on the limited supply. Point of sale issues make the distribution of available fuel a challenge, as the local gas stations and truck stops may have no battery back-up for pumping gas, and no working cash registers, ATMs, credit card machines, or check cashing systems to facilitate purchases. While the grocery stores association could say which stores were open, the fuel outlets were not organized to report functionality. While grocery stores often have a system in place for cash-only purchases, and many have generators for freezers that also power cash registers, there are no standards for fuel stations for life safety or community recovery functions. Communities often do not know which fuel outlets have back-up power and which outlets need functionality.[280]

Critical telecommunications systems were also impacted by the lengthy PSPS events during the fall of 2019. Alerting and warning systems failed in many areas, so community emergency notifications did not get delivered. When there is no power, there also is no ground-based internet service. Likewise, cellular phone systems, which also depend on power for the repeaters, did not function as soon as the emergency power supplies failed. Fewer people have landline service available since many providers have switched to voice-over-internet-protocol (VOIP) services only. Since these "landline" services also depend on power to the internet, over 500,000 people in California lost all communication systems due to loss of power. It took six days to get wireless information disseminated and systems operating. Communications providers were worried about their public image, so the loss of communication was not reported. The greatest public safety concern was the inability to notify people who needed to evacuate ahead of the fires, forcing first responders to revert to door-to-door notifications, which are time and resource consuming. For example, all of Marin County had no power; 57% of cell towers were not working. The loss of the

internet and cable meant that data and text services were also not working. Land mobile radio systems used by the public safety professionals worked, but no one else had reliable communications.[281]

While the state might have called on neighboring states for mutual aid to supplement the available emergency power systems, the generators from out of state do not meet the California Air Resources Board's (CARB) standards, so the Office of Emergency Services could not bring them into the PSPS area. Fortunately, critical government functions had emergency power systems, so county emergency operations centers had communications capability outward to unaffected areas, using amateur (HAM) radio, satellite, and microwave systems.[282]

The impact on marine transportation security from the 2019 California PSPS surprised the USCG. The California command quickly passed the word to the maritime community that alternative sources of power would be crucial to continued operations. The Port of Oakland used locomotives as a supplemental power source, for example.[283] There was no direct PSPS impact on the Port of Oakland, which does not use PG&E and provides most of its own power, but the Port of Los Angeles/Long Beach did lose power due to the PSPS. Matson has PG&E services, but the Port of Oakland provides the rest of the power. All container vessels plug into shore power when they are in port, so it was critical to ensure that alternate sources of power were provided during the PSPS to preserve the cargoes.[284] The USCG admiral ordered the staff to create an emergency plan for PSPS. The biggest challenge was determining what critical systems had back-up generators and a fuel supply chain to continue to support them. They are now looking for a fuel vendor and supply chain for fuel for critical command functions. The plan has also extended to contingencies for security when power is lost to the surveillance systems.[285]

Although not all ports are faced with the likelihood of such widespread commercial power losses, natural hazards, solar weather impacts[286] in the GPS systems and security threats to the power grid all generate a need for emergency power planning.[287] Some areas with a high level of lifeline dependence on the ports have more robust contingency plans. For example, because the port in Honolulu is a critical asset since most essential goods have to be imported by sea, the Department of Homeland Security (DHS) provides backup power for the cranes to ensure that the port can keep moving. When Hurricane Katrina impacted the New Orleans area in 2005, the US DOT sent out the ready reserve force vessels to provide support. Two vessels were kept in the Port of New Orleans and pushed against the dock to provide lighting to support relief operations because they were the only facilities with lights in the area. The New Orleans Naval Reserve Base kept the ships refueled. During the early days of limited community public safety control, the ships' crews had to break open the small arms lockers to defend the ships against looters.[288]

These inter-sector impacts on the surface transportation supply chain have important effects on security and resilience. NATO has recognized the importance of preventing disasters from cascading from one critical infrastructure to another. It has established seven principles of

resilience, which acknowledge the interconnectedness of power, communications, transportation, and most recently (June 2020), supply chains, which will be discussed in more detail below.[289]

5.5 Responses to Transportation Supply Chain Security Challenges

The EU STSCS Responses

The European Union (EU) is an economic and political union of 27 member states, shown in Table 3.

Table 3. European Union Member States

Austria	Italy
Belgium	Latvia
Bulgaria	Lithuania
Croatia	Luxembourg
Cyprus	Malta
Czechia	Netherlands
Denmark	Poland
Estonia	Portugal
Finland	Romania
France	Slovakia
Germany	Slovenia
Greece	Spain
Hungary	Sweden

Source: European Union, 2021.

The Euro is the common currency for 19 of the 27 members. People and goods are able to move freely within the EU's Schengen Area, which includes all EU nations and some neighboring nations and is free of all internal borders. The external borders of the Schengen Area have been strengthened to ensure the security of the travelers and goods within the open travel area.[290]

The 27 nations have a combined population of 447 million people, and 11.7 million people (5.3% of the total workforce) are involved with trade. Each year the EU moves 3,731 billion metric tons of goods, 50% by road, 31% through ports, and 11% by rail. External trade from outside of the EU nations uses 73% maritime resources, representing 50% of the value in goods. Only .8% of the trade goods move by air, but these are high-value items.[291]

The EU has a robust policy on surface transportation supply chain security. Its Transportation Security Framework covers all threats from terrorism to graffiti. There is no detailed EU framework for land transportation—roads, trucks and rail—because there are diverse risks and threats that have to be managed by the nation in which the goods are located. Crime, valued at a

loss of 8 billion Euro per year, happens on the premises of transport, such as the use of trucks for smuggling, human trafficking, theft of cargo and theft of the trucks themselves. When the crime is within one nation, it is the purview of that nation's police forces. However, the larger EU "secure supply chain" initiative includes maritime piracy, international criminal acts and cybercrime. The initiative covers the roles and responsibilities for operators and third-country partners. The EU's maritime transport security plan is based on the ISPS framework, which includes "computer systems and networks," and is understood to encompass cybersecurity. The controlling regulation is the European Union Customs Code, which details the management of cargo at the external border.[292]

The EU has also adopted measures to strengthen the security of its rail systems, especially the passenger mode, after its vulnerabilities were vividly exposed.

On August 21, 2015, a heavily armed Moroccan national carried out an attack on the high-speed rail Thalys train traveling from Belgium through northern France. Two American military personnel and a third colleague who were on vacation overpowered the shooter before he could kill anyone. Ayoub el Khazzani was convicted of attempted murder and terrorism.[293] This attack demonstrated the existence of a security gap for passenger rail. In response, a Rail Security Action Plan was adopted by the European Commission in June 2018, focusing on rail passengers and staff. They now have metal detectors for rail passengers in larger countries, and smaller countries use random checks of passengers and baggage to detect weapons. The 2018 Rail Security Action Plan has seven elements:

1. EU Passenger Rail Security Platform, which is focused on "collecting information on rail security, on optimizing (sic) the security of cross-border rail services and defining a coordination mechanism to avoid unilateral decisions at the national level."[294]
2. Common methodology for the assessment of rail security risks.
3. Technical guidance on information to passengers involved in an incident, security technology and design solutions for enhanced security, staff security procedures and security training.
4. National contact points on rail security.
5. Implementation of a mechanism at the national level for sharing information on rail security.
6. National level rail security management.
7. Rail security management plan.

This risk-based approach encourages a proportionate response to emerging threats, keeps passenger rail services accessible, creates coordination among member states, yet has no binding requirements.[295] Moreover, even though some of these recommendations are also relevant for

freight security, this sector continues to possess widely recognized weaknesses. The European Agency for Railways, for example, recently declared, "European Rail Freight is facing multiple challenges." These range from consignment tracing and tracking to the harmonization of national rules.[296]

Road security is based in national responsibility, but there is cross border cooperation on developing common strategies, such as safe and secure parking for trucks, designed to prevent security threats to drivers at rest stops. The EU nations have collaborated on dangerous goods rules and on minimum security and service levels for rest stops. The common standards across all EU nations address sanitation, restaurants and comfort facilities. The EU planning started with a shortage of 100,000 parking spaces for trucks, which led to unsafe parking habits. The result was 8 billion Euro in theft related to road transport each year. Under the new plan, rest stops were classified as bronze, silver, gold and platinum levels, allowing truckers to select an appropriate facility for the value and sensitivity of their cargo. There is still a shortage of 17,000 secure parking spaces.[297]

Another effort to enhance cross border security is the 2019 commercial road security toolkit called *EC Security Guidance for the European Commercial Road Freight Transport Sector*. In addition to the freight theft problem, the trucking sector faces challenges ranging from irregular migrants hiding in cargo containers to terrorists using trucks as weapons,[298] as happened in Nice, France. [299] The toolkit was developed by the Directorate General for Mobility and Transport of the European Union (DG MOVE). The comprehensive guide contains a section for truck drivers, warning against unscheduled stops and how to manage the stages of the journey, such as pick-up, stopovers and deliveries. The section for "logistics managers and key stakeholders" describes risk management and decision making when planning cargo truck journeys. Annexes provide detailed guidance for specific elements of trucking security, including a checklist for drivers and for inspecting trucks.[300]

Germany, one EU member state, has developed its own Security Strategy for the Freight Transport and Logistics Industry. The strategy has seven elements, depicted in Table 4.

Table 4. Strategic Elements

Assign roles and responsibilities
Enhance resilience of logistics (resilience = protection, reliability, redundancy, reaction)
Targeted and efficient government actions through risk-based approaches
Promotion of cross-sectoral comprehension of security
Cooperation in spirit of trust and structured dialogue
Improved awareness and knowledge of stakeholders
Continue and extend international cooperation

Source: Benini, 2020.

While fitting well with the NATO initiatives, these internal guides help the German government and its critical economic sectors to plan and prepare for disruptions as a way to minimize impacts on their internal economy and the supply chains in which they participate.[301]

Asia Pacific STSCS Responses

The US is a partner in the Asia Pacific Economic Cooperation (APEC) organization, which also focuses on supply chain resilience. It has 21 members, shown in Table 5.

Table 5. APEC Members

Australia	New Zealand
Brunei Darussalam	Papua New Guinea
Canada	Peru
Chile	The Philippines
People's Republic of China	Russia
Hong Kong, China	Singapore
Indonesia	Chinese Taipei
Japan	Thailand
Republic of Korea	The United States
Malaysia	Viet Nam
Mexico	New Zealand

Source: APEC, 2020.

The organization was formed in 1989 in recognition of the shared economy of the nations around the Pacific Rim, with a goal of secure growth and regional economic integration. APEC's focus is on trade, so they refer to members as "economies" rather than countries. One goal is the coordination of regulations and standards to facilitate cross border trade among the member economies to improve "logistics and transport networks to enhance supply chain connectivity." They also have a focus on "disaster resilience, planning for pandemics and addressing terrorism."[302]

One focus of their work is on the mitigation of the worldwide economic impacts of disasters. Researchers have noted that in the US, 43% of businesses impacted by disasters never reopen, and 29% of those that do reopen fail within two years. They also recognize the far-reaching impacts of disasters. The volcanic eruption in Iceland in 2010, for example, impacted the nearby ponies, European air passengers, auto assembly plants in the US, Germany and Japan, rose growers in Kenya and manufacturers worldwide, as supply chains were disrupted by the interruption in air cargo.[303]

There are many examples of the integrated economy that has developed around the Pacific Rim. Ten nations supply parts for the hard drives that are assembled in Thailand, creating multiple

vulnerabilities in this worldwide supply chain. Thailand is the #2 producer of hard drives in the world. Floods there in 2017 resulted in a 30% drop in global hard-drive production. Company losses included $162 million for Sony, $603 million for Canon, and $199 million for Western Digital.

Recognizing these impacts, APEC has developed Seven Principles of Supply Chain Resilience, depicted in Table 6.

Table 6. APEC Seven Principles of Supply Chain Resilience

Share information and knowledge to promote supply chain resilience.
Promote disaster risk management and hazard mapping to better understand potential risks to supply chain resilience.
Support planning and business continuity management to improve global supply chain resilience.
Promote best practice policy, regulations, and flexibility to enable global supply chain resilience.
Leverage regional cooperation to support the supply chain, including coordination with other multinational organizations working on supply chain resilience inside and outside the APEC region.
Promote critical infrastructure protection and inter-modalism as a key component of supply chain resilience.
Recognize and promote best practices in human resource and capacity management in the context of supply chain resilience.

Source: Benini, 2020.

These principles help the countries that partner through APEC to develop systems that create a more resilient internal economy and make them more reliable partners in international supply chains.[304]

5.6 Private Sector Supply Chain Responses: TAPA

Logistics is becoming an ever-larger part of the world economy as supply chains lengthen and become more complex. In 2000 logistics was 5% of the US economy, but is 8% in 2019. Table 7 shows the value of US logistics operations.

Table 7. Value of US Logistics

Mode	**Value**
Motor carrier	$668 billion
Parcel	$104.9 billion
Rail	$88.4 billion
Air freight	$76.5 billion
Water & ports	$457 billion
Pipelines	$53 billion

Source: Council of Supply Chain Management Professionals, 2019.

The logistics sector is evolving in a number of ways that impact supply chain security. Amazon is one example of a logistics company that uses a business plan with small warehouses across the nation. As an online retailer, Amazon must deal with goods moving in both directions, with up to 40% of products returned by the consumer. Its main warehouse is staffed using a mix of humans and robots. The robots cost $1 million each, but each replaces 1,300 human employees. The robots have a two-year return on investment.[305] Amazon uses third party delivery companies for the last mile delivery service and plans to deliver some last mile packages using drones in its own Prime Air fleet. The drones can deliver package under 5 pounds to customers up to 15 miles from the drone's base.[306]

Goods in the worldwide supply chain are the property of a range of private businesses. The goods move through several modes of surface transportation: rail, maritime and principally trucks. The Transported Asset Protection Association (TAPA) is an organization of global manufacturers, logistics providers, freight carriers, law enforcement agencies, and other stakeholders with the common aim of reducing losses from international supply chains. In 2014 supply chain crimes involving luxury goods exceeded 43 million Euro.[307] The association's goal is to protect members' assets, recognizing that theft of high value, high risk cargo is the biggest supply chain challenge.[308]

TAPA sets minimum security standards for various transportation modes, such as its Trucking Security Requirements (TSR), which include policies and procedures involving certifications from TAPA or C-TPAT, and practice, which is the physical aspect of the trucks. Facility Security Requirements (FSR) cover secure warehousing and in-transit storage of goods. Requirements cover issues such as security systems that integrate X-ray, weight scales, scanners and CCTV. Environmental considerations include high-value cages and facility access controls. Audits confirm compliance, and certification for Level A (highest security), B or C will be awarded following each audit. Producers can then determine the security level needed for the goods and hire shippers based on their certification level. Law enforcement and regulatory partnerships collaborate to limit cargo-related crime.[309]

NATO's Seven Elements of Resilience Strategy

The North Atlantic Treaty Organization (NATO) was formed at the end of World War II on April 4, 1949, through the Treaty of Washington.[310] It is a consortium of nations that is designed to provide collective security for its members. The current member states are listed in Table 8.

Table 8. 2020 Membership of NATO

Albania	Belgium	Bulgaria	Canada
Croatia	Czech Republic	Denmark	Estonia
France	Germany	Greece	Hungary
Iceland	Italy	Latvia	Lithuania
Luxemburg	Montenegro	Netherlands	North Macedonia
Norway	Poland	Portugal	Romania
Slovakia	Slovenia	Spain	Turkey
United Kingdom	United States		

Source: NATO, Member states, August 31, 2020.

Originally formed to combat the potential for aggression against European nations by the former Soviet Union, today the Alliance provides broad-ranging crisis support to its member states. Guidance is provided for members states across a variety of threats, including cybersecurity, energy security, counter-terrorism, and most recently, the COVID-19 pandemic.[311] Article 3 of the founding treaty required every member to engage in preparedness to resist armed attack. Today this concept recognizes that civil systems such as utilities, transportation, cyber systems and support of the population are critical to responding to any threat, whether from a natural hazard, technological failure or intentional attack.[312]

Article 5 of NATO's founding treaty is the commitment to collective defense. Although designed to bring the Allies together to defend a member state that was being invaded or attacked by the former Soviet Union, Article 5 was actually invoked for the first time after the United States was attacked by terrorists on September 11, 2001. Resilience is a cornerstone of the collective defense concept, ensuring that each member state is able to recover from any event quickly to maintain its role in the Alliance.[313]

Recognizing that a collective defense military action requires the ongoing support of civilian assets, NATO has developed a resilience strategy to ensure that "basic government functions can continue during emergencies or disasters, in peacetime or in periods of crisis."[314] At its 2016 meeting, NATO issued the Warsaw communique, which stated that NATO had developed the Baseline Requirements for National Resilience, which included "continuity of government, continuity of essential services, the security of critical civilian infrastructure, and support to military forces with civilian means."[315] To achieve these goals, NATO has created seven elements of resilience, as shown in Table 9.

Table 9. NATO Resilience Requirements

Requirement 1: Assured Continuity of Government and Critical Government Services	Requirement 2: Resilient Energy Supply	Requirement 3: Ability to Deal Effectively with Uncontrolled Movement of People	Requirement 4: Resilient Food and Water Resources
Requirement 5: Ability to Deal with Mass Casualties	Requirement 6: Resilient Civil Communication Systems	Requirement 7: Resilient Civil Transport Systems	

Source: Benini, 2020.

NATO took a three-step process approach to achieving the resilience requirements among all member states. While nations such as the US and the United Kingdom (UK) have long-standing systems for managing civil defense and disaster response, not all member states had well understood government-based systems in place when the process started. Nations each conducted a self-assessment process that was completed by 2017. In 2018 experts from the Alliance met to discuss the key role of critical infrastructure elements and their interdependencies in the achievement of resilience. Transportation resilience was a key issue in the discussions. [316] Based on the gaps discovered by the self-assessments, NATO provided technical assistance to the Allies between 2018 and 2019. The member states then reassessed their capabilities after receiving the technical assistance, and their updated capabilities were reviewed by experts between 2019 and 2020. Status reports were then to be issued to national leaders in 2020,[317] but COVID-19 challenges intervened. At the Defense Ministers' meeting on June 18, 2020, resilience baseline Requirement 7 had the element of security of supply chains added, recognizing the demands of the COVID-19 response.[318]

The NATO framework offers a multi-national view on how global surface transportation systems should be secured. Coordinating across sectors in a public-private partnership offers the best hope for the security of the transportation of critical goods needed for national security and economic progress. The framework might provide guidance for the surface transportation supply chain security enterprise.

VI. Analysis of the Workshop Findings

The discussion of the workshop presentations presented above allows us to highlight the following issues that public and private decision-makers must grapple with in their ongoing efforts to enhance the security and resilience of global supply chain surface transportation systems.

6.1 Complex Relationships

The modern surface transportation supply chain involves a complex web of relationships involving private enterprise and a variety of government entities in multiple nations. While the transportation modes are mostly privately owned, and the goods in the supply chain are also mostly privately owned, the security regulations are developed and enforced by either private entities such as APEC and TAPA or by numerous governmental entities from the USCG, USCBP, and the EU to the customs agents in small nations. Managing supply chain transportation systems is further complicated by the multi-national ownership of many facilities. To cite but two examples, some of Rotterdam's terminals are owned by the Danish company, Maersk Shipping, while some US ports are owned by Chinese or Dubai-based entities.

6.2 Diverse Supply Chains

Management of the supply chain requires different levels of support for different products and services. Supply chains include a rich variety of products ranging from critical medicines to Christmas lights, often in the same cargo container. Some hazardous materials are labeled and provided with special handling, while lithium batteries and butane lighters may be shipped in a mixed goods load in a container with flammable items such as clothing or books. Containers are stacked above and below the deck level, making it difficult or impossible to check the condition of the containers in transit. Refrigerated containers require shore power when in port, but it may not be possible to check the individual connections for all containers. The US FDA requires advanced notice of the arrival of goods under its purview to permit scheduling of inspections, while other containers from the same ship may include high tech components or children's toys and move through the port based on C-TPAT inspections in the country of origin.

The foreign origin of materials further complicates the required actions in the port. Cargo containers of essential goods such as medical masks, gowns and gloves may need to be expedited through inspections and ground-based shipping during a pandemic. Pharmaceuticals may require expedited FDA inspections to reach critical points of distribution.

Adulteration of products made outside of the US is another security concern that may go far back in the supply chain. While the US FDA inspects food and drug products coming into the country, they do not test the contents of each box. In 2008 more than 20 people died and over 400 were sickened by tainted heparin, which is made from pig intestines. The US FDA inspects the foreign plants in which the dried heparin is made, but in 2008 a pig disease in China forced heparin plants

to buy pig parts from smaller, uninspected workshops where the pig intestines were harvested. Once the material was created in the pharmaceutical plants, it was inspected, but the tainting was a result of the use of improperly obtained raw material. How far back in the supply chain should security go?

6.3 Crime and the Need for STSCS

Goods in the supply chain require different types of security. Inexpensive goods may be tagged under C-TPAT in a foreign port, and not be opened again until they reach their destinations. High value goods may travel under bond, or be diverted in the shipping process by criminal enterprises. Theft of cargo was identified as an 8 billion Euro business in the European Union. APEC recognizes that criminal enterprise is a constant threat to the supply chain, since 1 pallet of Xbox machines buys the thief a BMW X5. Substitution of counterfeit products at the point of origin or at the point that the cargo container is opened also generate illegal income.[319]

Modern piracy was brought to the world's attention with the 2009 boarding of the Maersk Alabama by Somali pirates. Since then, armed security guards have been added to merchant ships, and the navies of the world have created patrols in the Indian Ocean and Persian Gulf to deter further attacks. Ships now sail further from the coast to make the trip too far for local pirates in small boats. But security experts have noted that while piracy off the Somali coast has diminished in the past ten years, piracy still persists in places such as Nigeria. The Straits of Malacca and parts of Indonesia are especially attractive areas for pirates since the shipping lanes are too narrow to permit ships to avoid them.[320]

6.4 Availability of Goods

Supply chain security may also be impacted by the availability of goods. Scarce goods, such as protective equipment and ventilators in a pandemic, may demand a higher level of access control and supply chain management quality control. Before the pandemic, the loss of a few boxes of medical gloves would represent a small dollar-value loss, but in the winter of 2020, the scarcity of such medical supplies was a life safety issue around the world, greatly raising their value. Thus, since consumers were willing to pay more for medical personal protective equipment (PPE), suppliers were able to spend more on their security and still make a profit.

Labor actions can also impact the availability of goods and surface transportation supply chain security. In 2015, 27 US west coast ports closed for four days in a labor dispute. Even such a short stoppage created supply chain havoc. During the strike, US buyers and port facility managers ramped up security provisions to ensure that the labor dispute did not impact the security of the goods in transit. The strike was estimated to cost $1.9 billion per day and to require up to eight weeks for deliveries to return to normal at the ports of Long Beach and Los Angeles, the primary container port for Asian goods. Even before the strike, ships had to anchor out for up to ten days awaiting berths and logistics support.[321]

6.5 Cyber Issues in STSCS

The US Department of Defense (DOD) is the world's largest logistics organization. Threats to the DOD supply chain include cyber threats, counterfeit goods, and the shrinking American industrial base that pushes purchasing offshore. The Defense Logistics Agency (DLA) serves both military units and the Federal Emergency Management Agency (FEMA). The DLA obtains materials from a prime contractor, but the components may come from various sources in different nations, "so it is difficult to certify the security of second and third-tier suppliers."[322] Cyber processes are a critical part of managing the logistics enterprise. Protection includes placing all processes behind the DOD firewall, understand the role of cyber in the supply chain, and training employees to recognize and avoid phishing attacks. Yet, such measures need constant vulnerability assessments, for even the most highly classified systems can be breached, as indicated by the successful introduction of the Sunburst malware into the cyber systems of numerous private organizations (including technology companies) and government agencies (including DHS, State, the military and the NSA) sometime in late 2019 or early 2020.[323]

Cybersecurity is especially critical at sea. Modern ships are largely computer-controlled. Malware introduced into the navigation system could leave a ship blind and subject to navigation hazards, getting lost at sea, or colliding with another vessel. Systems that manage ballast could be spoofed to cause listing or even capsizing.

Ports rely on cyber systems to schedule ship arrivals to coincide with the availability of cranes and land side transportation. Cranes may be computer operated, along with self-driving vehicles serving port operations. VOIP and wireless systems are critical communications assets. All of these systems are subject to tampering through a variety of cyber-attacks. Preventing interference with critical cyber systems is a constant challenge for surface supply chain security management.

6.6 Natural World Changes

After centuries of being frozen, the fabled northwest passage sought by Henry Hudson is opening as the Arctic Sea experiences 75 ice-free days each year. Russia has developed its northern slope as a natural resources center, creating a demand for supply chains to connect these new resources to ports such as Rotterdam and Yokohama. Cruise ships and military vessels transit the Bering Strait's narrow passage, raising the specter of maritime traffic jams in summer.

The melting Arctic poses numerous supply chain security challenges. The primary concern is the management of the overlapping areas of national interest created by the UN Treaty on the Law of the Sea. While China, Russia and Canada are signatories, the US is not. What will this mean for enforcement of mineral rights, rights of innocent passage, or use of natural resources such as fish? Concerns have also been raised about the safety of the pristine environment from ship accidents and potential oil spills.

Norway, Sweden, the United Kingdom, and Germany face overlapping economic zones with each other, and with Russia on the Eurasian side of the ocean. How will the opening of this northern access point impact historic European trade ports such as Rotterdam and Kiel? What changes will it make to trade routes as Russian North Slope ports become available to serve inland areas of Russia and Eastern Europe?

6.7 The Blueprint: Research into STSCS

The factors discussed above reflect the complex security challenges that the evolving surface transportation supply chains, which are global in reach, diverse in goods, and threatened by natural, human-caused and technological events, must confront. Suppliers, consumers, logistics companies and governments all have a stake in developing systems and technologies to ensure that STSCS is maintained to guarantee the integrity of products that move across the world. Geopolitical challenges from the melting Arctic and the Chinese Belt and Road initiative join and enhance transitional concerns such as theft prevention as focus areas for research.

Identifying these challenges provided the information necessary to achieve the primary goal of the workshop—the creation of a blueprint to be used by researchers wanting to enlarge knowledge of STSCS and to create systems and technologies to enhance supply chain transportation security. It can benefit researchers and funders by providing some guidance for focused research with immediately applicable benefits. This blueprint is the work of every member of the workshop and is published as Appendix A of this report.

VII. Conclusion

Though numerous practical obstacles have been identified in any effort to enhance the security of supply chain transportation systems, the above analysis clearly indicates the need for more research in numerous areas. In addition to new research on numerous security aspects of various transportation sectors, the policy area deserves special attention. Essentially, research is needed to enhance the understanding of (1) the degree to which relevant government organizations interact in developing and implementing policies nationally, sub-nationally and internationally and their effectiveness, and (2) the degree to which supply chains have adopted and implemented relevant and effective security measures.

These topics have emerged because the literature has demonstrated that little is known about the degree to which the US government has developed an integrated and effective policy approach to such critical areas as cybersecurity. Furthermore, it has reflected the fundamental difference in the concerns of the private sector that operates the transportation systems and the supply chains generally and those of the government. Articles written with a private sector focus generally reflect a desire to protect business interests by eliminating internal risks and redundancy. Yet, it must be recognized that there is also a growing recognition of the importance of such issues as pollution, sustainability and resilience.

Accordingly, although supply chain operators are interested in using emerging technologies, such as automated vehicles, drones, and improved tracking and GPS software, their concern is on how to improve their ability to track goods and transfer them as quickly and efficiently as possible. Security-related issues are narrowly defined and include integrating emerging technology effectively, managing and integrating supply chain transportation with other supply chain nodes, achieving rapid freight flows and minimizing theft, and risk to their customers and/or investors. The ways these priorities impact security is evidenced by the maritime industry's cyber situation.

The difference with the government's security priorities is obvious. It is focused broadly on the external risks to all aspects of supply chain transportation systems, and emphasizes security measures that will protect them against the ability of terrorist and criminal organizations to exploit legitimate supply chains for illegal operations or to sabotage them in ways, which would endanger societal functioning and national security. Yet though the US government has successfully developed and implemented effective policies in some areas, the extent to which it has done so and its ability to do so in others remains unclear.

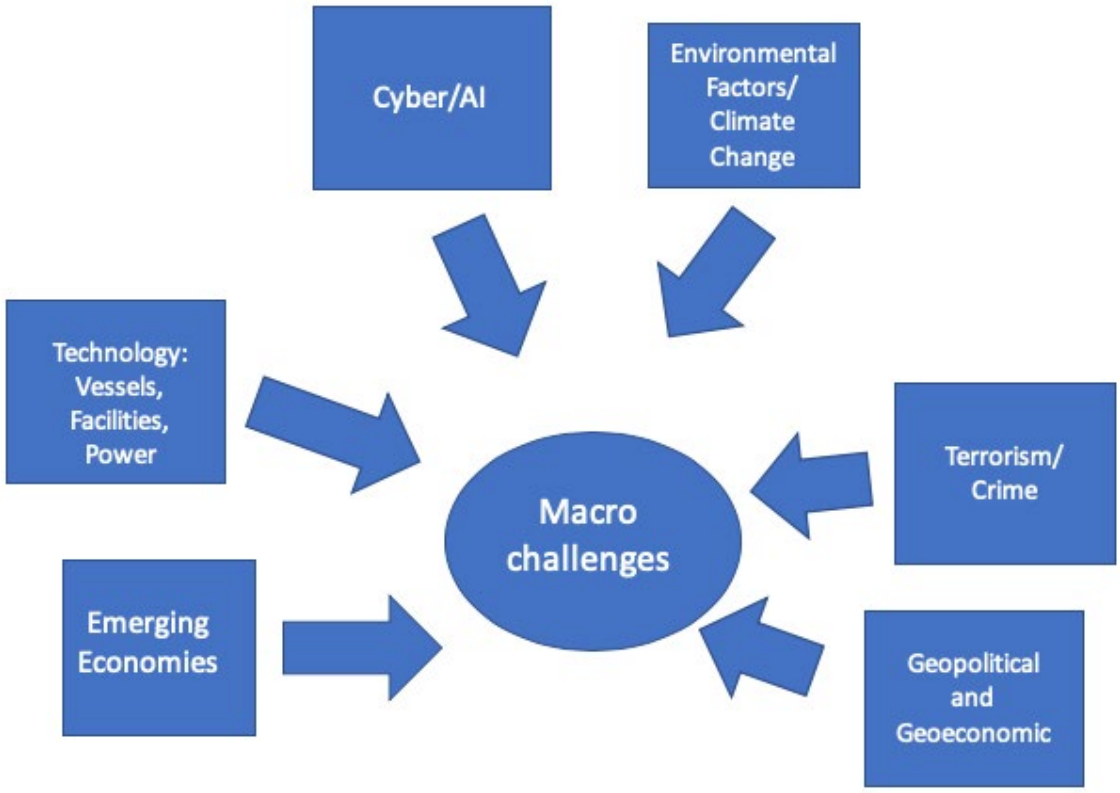
It has issued numerous publications that relate to mitigating general and specific supply chain risks. However, it is not at all clear to what extent these have been implemented, and it is difficult to measure their success. However, it is safe to say that a major obstacle to achieving higher levels of transport security is the inherent difficulty in overcoming the differing goals of the private and public sectors.

The result of such differences is particularly evident in the cybersecurity realm. Although supply chain companies have been integrating emerging cyber and related information technologies into their transportation systems, few, especially (as we have emphasized) in the maritime sector, have been eager to pay for recommended security measures.

Enhancing the knowledge of these issues, including the functioning of the government and its relationship with the supply chain organizations and their transportation systems, will facilitate the creation of a proactive environment that will facilitate the emergence of the necessary cooperative action among all the governmental and intergovernmental organizations and with the private sector. As we have seen, this will be no simple matter, yet the literature survey that was have carried out reveals that there is widespread agreement on the need for action and numerous suggestions regarding policies that should be implemented. The next step is clearly to build on existing knowledge and to fill the critical gaps identified above.

However, even this will not suffice, for this is a rapidly changing world. Accordingly, it is also essential to develop a deeper understanding of the nature of the global environment and the ways in which the six macro challenges identified above will influence supply chain transportation systems in the years to come.

Figure 8. Supply Chain Macro Challenges



If global economic networks are to function securely and effectively for future generations, the implications of these factors for transportation systems must be understood, and appropriate policies developed and implemented.

Appendix A: Blueprint for Future Research

As a result of the STSCS Workshop presentations and discussions, the participants in the Delphi process jointly developed a blueprint for future research in the field. There is a great deal of literature on many aspects of the supply chain, but very little on the role of transportation security in the supply chain or on how transportation security's performance is critical to supply chain security overall. As the bibliographies demonstrate, research on the security of individual modal elements of the supply chain is well-developed, but there is little on the intersection of transportation security with the supply chain's operations. While the workshop was focused on surface transportation modes of maritime, road and rail, the areas identified as needing further research may equally apply to aviation transportation supply chain security.

The blueprint provides an outline of issues and topics that would benefit from further research. Some of them have not been investigated at all from a transportation security perspective. Others have been studied at an earlier time but are newly influenced by changing technology, geo-political activities or management strategy changes.

OVERARCHING ISSUES

1. Supply chain itself, or environments in which supply chains operate
    a. Mechanics of the supply chain's transportation security, from origin to destination
    b. Arctic Ocean's evolving trade routes
    c. China's Belt and Road initiatives in the Eastern Hemisphere and South Pacific
    d. Maritime management.
    e. Road and rail innovations and security
2. Ranking of supply chains in national security? Or what are the most important US supply chains?
    a. Economically?
    b. Strategically—criteria?
    c. National defense (Jones Act), to ensure that the "Fourth Arm of Defense" of the merchant marine extends to both sides of the waterborne transit
    d. Resiliency—criteria? Hazards that must be addressed to ensure resiliency
    e. Redundancy as a solution
    f. Rapidly employable alternatives

g. Distributed sources for critical goods

3. Who is responsible for transportation supply chain security?
    a. Range of responsibilities
    b. Degree of cooperation and collaboration within the transportation elements of the supply chain
    c. Criteria for transportation supply chain security? Use adoption of ISO 28000:2007 as an indicator? (see https://www.iso.org/obp/ui/#is o:std:iso:28000:ed-1:v1:en)
4. Organizational learning capacity
    a. Conflict between minimal staff, standardized systems and economic environment.
    b. How to cope with the conflicts?

TOPICAL AREAS

1. Define supply chains, including the transportation assets
    a. Military
    b. Commercial
    c. Sector: Essential Commodities – National Security/Emergency Management/ Public Health
        i. Water
        ii. Fuel
        iii. Medical
        iv. Food
        v. Energy: pipelines and electricity
        vi. Communications
2. Defining supply chain security-position in the supply chain (prime, support, subcontractor)
    a. Where resilience fits in security
    b. Role of JIT in resilience—having things there when you need them
    c. Development of resilience metrics for complex systems in STSCS

d. Application of National Academy of Sciences measures of resilience in engineering to resilience in the STSCS sector

e. Difference among/interaction of safety, security and emergency management

3. Threats and risks to material and information supply chain

   a. Analytical frameworks for supply chain managers?

   b. How to quantify risks?

   c. Internal threats, single point failure, layered defense

   d. Comparing the impact (cost) of disruption of supply chains versus the cost of restoration of those supply chains (i.e., balancing preventive measures and reactive measures)

4. Supply chain governance- what are the laws, regulations, standards?

   a. International

   b. National

   c. State

   d. Local governments

   e. Supply chain manager, e.g., Amazon

   f. Trade associations, e.g., Asian Pacific Economic Cooperation (APEC)

5. Supply chain governance – what are the strengths and weaknesses: from the perspective of government/ supply chain manager/ trade association?

   a. International

   b. National

   c. State

   d. Local governments

   e. Supply chain manager, e.g., Amazon

   f. Trade association., e.g., Association for Supply Chain Management (ASCM)

   g. Inter-agency, inter-governmental, international

6. National Highway System (NHS), Strategic Highway Network (STRAHNET) and Strategic Rail Corridor Network (STRACNET)

   a. Evaluating the criteria for construction and route selection for current relevance

b. Military bases—locations have changed

c. Military support to civil authority

d. Civil support to military

7. Use NATO standards of quantification and accountability to evaluate specific surface transportation supply chain resiliency as an element of security

   https://www.nato.int/cps/en/natohq/topics_49158.htm

8. All hazards supply chain resilience development

   a. Impact of ESF 14: Cross Sector Business and Infrastructure, 2019

   b. Use of pass down log to capture lessons and best practices [military turn-over file model]

   c. Use of temporary but redundant supply routes and hubs to make the system more resilient during crisis

   d. Impact of disease on supply chains—loss of workers, changing demands, impact on transportation modes

9. What areas and to what degree do you need international cooperation and agreements for transportation supply chain security?

   a. European Union

   b. International Maritime Organization, International Ship and Port Code

   c. United Nations' Conventions

   d. International regulations for the carriage of dangerous goods for the security of the cargo

10. Growing dependence on information flows within supply chains [physical and cybersecurity]

    a. Physical security of undersea cables and landing stations

    b. E-commerce

    c. Blockchain, Tradelens (IBM/Maersk)

    d. Autonomous vehicles

    e. SCADA

    f. Logistics

    g. Data governance for enhanced trust in supply chain information exchanges, the benefits of mainstreaming cyber-hygiene in transportation

11. Periods of transition and the vulnerabilities that they create for surface transportation supply chains and security challenges
    a. Physical supply chains
    b. Information supply chains
    c. Ports, stations as points of access and vulnerability
    d. Vessels in operation
12. Leveraging emerging technologies for multiple applications
    a. Using GPS for goods tracking and security oversight
    b. Using various streams of information for validation to support decision making
13. Better communication linkages to create resilient supply chain transportation security
    a. Cross-industry/supplier
    b. Language issues—among crew members

Appendix B: Workshop Participant Biographies

Janet Benini's career began with the California Office of Emergency Services, where she led program development for the California Specialized Training Institute and was a responder during major disasters such as the Loma Prieta and Northridge earthquakes. She transitioned to the US Department of Transportation emergency management office in 1998 and was its Deputy Director during the 9/11 attacks. She led development of the National Response Plan at the White House, and developed the "Principles of Supply Chain Resilience" for the Asia-Pacific Economic Cooperation group (APEC), the topic of her dinner speech.

Jan is an adjunct professor at George Washington University, and she continues to work as a Civil Transportation Expert for NATO. She is co-Principal Investigator for the Transportation Research Board's (TRB) NCHRP project that caps a 20-year effort to improve transportation resilience and will develop a playbook and training program for all State DOTs.

Commander Greg Callaghan is currently the Chief of Prevention for the Eleventh Coast Guard District, covering California, Nevada, Utah, and Arizona. His previous assignments include Commanding Officer and Executive Officer of Marine Safety Unit Texas City, the Office of Port and Facility Compliance at Coast Guard Headquarters. There, he was also the Coast Guard representative to the US and Canada Bi-National Maritime Security Working Group. Commander Callaghan was also assigned to Sector Boston, MA and Marine Safety Office Miami, FL.

Commander Callaghan's education includes a Bachelor of Science degree from the State University of New York Maritime College, a Master's in Public Administration and Certification in Port and Maritime Administration from Old Dominion University, and a Master's in National Security and Resource Strategy from the National Defense University's Eisenhower School.

LCDR Robert Cole serves as the Port and Facilities Activities Section Chief at Coast Guard Pacific Area. His prior assignments include Sector San Diego as the Waterways Management Division Chief, Sector Mobile in the Inspections Division, and Sector Houston-Galveston in the Vessel Traffic Service. Prior to joining the Coast Guard, LCDR Cole served in the US Navy for nearly seven years.

LCDR Cole's assignments have been in support of the Coast Guard's Prevention mission, which provides port and waterway management oversight and coordination, and ensures that vessels and facilities comply with applicable regulatory requirements, all in support of the safety and security of the nation's ports and waterways. In regard to cybersecurity, as a result of the June 2017 APM-Maersk ransomware event, his office was tasked to prepare guidance detailing how subordinate units should manage and respond to cybersecurity events in the Marine Transportation System.

Frances Edwards, M.U.P., Ph.D., CEM, is a professor and director of the Master of Public Administration program at San José State University. She is also Deputy Director of the National

Transportation Security Center at the Mineta Transportation Institute (MTI). She is a Certified Emergency Manager with over 20 years' experience in California. She is editor of *Housing Recovery After Disasters*, co-author with Dan Goodrich of *Introduction to Transportation Security,* and two books on terrorism with Fritz Steinhausler of the University of Salzberg, twelve major publications for MTI, and more than 40 articles and book chapters. She provides emergency management planning and training for Caltrans and Santa Clara Valley Transportation Authority and gives frequent media talks, conference presentations and public education seminars in Silicon Valley. She has provided leadership for two NATO Advanced Research Workshops and consulted with the European Union.

Frances has a master's degree in political science (international relations) from Drew University, a Master of Urban Planning and a PhD in public administration from New York University, and a certificate in hazardous materials management from the University of California, Irvine. She is a FEMA-certified instructor for the ICS course suite and a California Specialized Training Institute outreach instructor.

Dan Goodrich, MPA, CEM, MEP, is the Senior Transportation Security Scientist with the Mineta Transportation Institute (MTI) at San José State University and the instructor for "Security Issues for Transportation Professionals" in the College of Businesses' Master of Science in Transportation Management program. He is a Certified Emergency Manager, a Master Exercise Practitioner, a Professional Continuity Practitioner and a Certified Security Specialist. He is co-author with Frances Edwards of *Introduction to Transportation Security*, nine major research publications for MTI, as well as a variety of professional articles and book chapters. He provides emergency management planning and training support to Caltrans and Santa Clara Valley Transportation Authority. He has participated in two NATO Advanced Research Workshops and consulted with the European Union.

Dan has a master's degree in public administration from San José State University. He is a FEMA-certified instructor for the ICS course suite and a California Specialized Training Institute outreach instructor. He has worked at county government and in the private sector, and has sixteen years' military service, including US Marine Corps Security Forces and US Army Reserve Military Police.

Kevin Krick serves as Matson's Senior Director, Safety, Quality, Environment, & Security (SQES). As a department head reporting directly to the president, Kevin is responsible for all initiatives and aspects of SQES compliance programs for the Matson companies. Overseeing a geographically diverse department that serves vessels, terminals, and supply chain operations throughout the Pacific, SQES oversees physical security and supports cybersecurity initiatives as well as the monitoring of the carriage of dangerous goods.

In addition, Kevin serves as the Designated Person Ashore and is a board member of both the Chamber of Shipping of America and the Smithsonian Environmental Research Center advisory board. Previously, he served as a Presidential appointee to the US Maritime Administration and

is currently a Captain in the United States Navy Reserve in the Strategic Sealift Program. Early in his career, as a dual license graduate of the US Merchant Marine Academy, Kevin sailed aboard tankers for most of the 1990s. He has an M.S., Marine Policy from the University of Delaware College of Marine Studies.

Liz Lange, MPA, is a graduate of the San José State University Master of Public Administration program and was Vice President of the MPA Student Association. Liz's final project for the degree is a comparative benchmark analysis of Façade Improvement Programs (FIP) in the Bay Area. She hopes that this inventory and analysis of programs will allow other cities a set of common practices and trends and encourage them to start their own FIP. As a research assistant for this project, Liz assisted with developing a bibliography of relevant work on surface transportation supply chain security that will be used to support future practical research in the field. She provided logistics support to the workshop and assistance with the workshop report preparation.

Herby Lissade, P.E., is the Principal Transportation Engineer at the California Department of Transportation, serving as Assistant Division Chief overseeing the Offices of Maintenance, Technical and Field Support, Storm Water and Environmental Compliance, Emergency Management and Technical Field Support, ITS and Roadway Maintenance, Radio Communications, and Roadside Management. Previously Herby was Chief, Office of Emergency Management for ten years. He also worked in District 7 (Los Angeles) as a Senior Engineer. He started his career with the New York State Department of Transportation's construction division in New York City. He is a licensed Professional Civil Engineer in California and graduated from The Pratt Institute.

Herby is the Chair of three National Cooperative Highway Research Program Project Panels and an international expert on emergency management and transportation, speaking at conferences in China and Japan. Following the devastating Haiti earthquake of 2010, Mr. Lissade formed the non-profit Haiti Engineering and is the President. Haiti Engineering is supported by Caltrans professionals of all classifications, brought together to provide technical assistance to the people and government of Haiti.

Commander Rom Matthews currently serves at the US Coast Guard Eleventh District in Alameda, California, as the Chief of Contingency Planning. Under the direction of the Eleventh District Commander, his duties include oversight of the Eleventh District and four major field commands' contingency plans, including the Area Maritime Security Plan, Maritime Transportation System Recovery Plan and multiple field unit all-hazard contingency plans.

Commander Matthews is in his 25th year of service. He has served in a variety of domestic and overseas assignments, including high seas maritime law enforcement, foreign and domestic port operations and security and maritime search and rescue. He supported the global war on terror as a Foreign Port Security Advisor deployed to over 50 foreign countries assisting foreign governments in securing the global supply chain against acts of terrorism.

Colonel Mitch Medigovich (CANG, Ret.) has 37 years in public service. Currently, he serves as Deputy Director for California Office of Emergency Services (Cal OES), overseeing Public Safety Communications, Information Technology Operations, and Disaster Logistical Operations. He was appointed by Governor Brown to Cal OES in December 2012 and reappointed by Governor Newsom. Col. Medigovich is a decorated combat veteran with numerous medals and citations. His final assignment was as Chief of Staff to the California Military Department. He has directly led and supported response efforts for the state in sixteen Presidential Disaster Declarations since 2013, including historic wildfires, major earthquakes, and devastating floods across 55 counties.

Col. Medigovich earned his Bachelor of Science from CSU Sacramento, a Master of Business Administration from Embry Riddle Aeronautical University, and a Master of Arts in Strategic Studies from the United States Army War College.

Gzim Ocakoglu is, since mid-August 2019, First Counsellor on Mobility and Transport at the Delegation of the European Union to the United States of America. His role is to support and promote EU-US transport cooperation and dialogue and facilitate the exchange of information on transport issues between the European Commission and the US authorities, as well as with the relevant international organizations, private sector representatives and professional organizations. In the European Commission for more than 16 years, Gzim has extensive experience in transport policymaking, developing and implementing rules and legislation in maritime transport and logistics (from 2017 to 2019), in aviation and air traffic management (from 2013 to 2017), and in Intelligent Transport Systems (from 2008 to 2013). In his most recent position in DG MOVE (Deputy Head of Unit "Maritime Transport and Logistics"), Gzim was also Chairman of the Digital Transport & Logistics Forum (http://www.dtlf.eu), a Commission expert group addressing the challenges of the digitalization in logistics chains.

Before joining the Commission in 2003, for ten years, Gzim held various research and management positions in the telecom industry, working for both equipment manufacturers and telecom operators. He holds a MS degree in Electro-Mechanical Engineering from the Université Libre de Bruxelles and a MS in Electrical Engineering from the University of Minnesota.

Ash Padwal, PE, JD is the Chief Risk Officer for Allied Telesis, Inc. (ATI). ATI designs, manufactures, sells and supports high performance information technology infrastructures for healthcare, aerospace, defense and transportation companies around the world, including US, Canada, Mexico, Europe and South America.. In this capacity, Ash is responsible for oversight of the legal, regulatory affairs, corporate governance and risk management activities of the company. He is also a founding Trustee of the University of California, Merced Foundation. Ash holds a JD from Santa Clara University and a BE in Telecom Engineering from University of Poona in India, and completed graduate work in Industrial and Systems Engineering at San José State University.

Manny Raras has worked for the US Coast Guard for the past thirty-five years, both as an active-duty officer and a civilian employee. He has served in a wide variety of professional fields, including naval engineering, training, operations, international affairs, and intelligence. He currently

manages the Geopolitical Section of the U.S. Coast Guard's Maritime Intelligence Fusion Center Pacific. He is responsible for providing information and analysis to Coast Guard executives regarding issues and events that impact Coast Guard Operations throughout the Pacific and Polar regions. As the Director of International Relations in the Pacific, he planned and coordinated engagement activities with foreign agencies to promote cooperation on strategic maritime issues. He negotiated a historic agreement between Coast Guards from Japan, China, Russia, South Korea, Canada and the United States that established areas of cooperation and guidelines on information sharing between them.

As the Director of Contingency Exercises, he managed the Coast Guard's conting ency exercise program throughout the Pacific, including all major Homeland Security and Homeland Defense exercises. As the Deputy Chief of Detection and Monitoring Operations for Joint Interagency Task Force West, he managed all Department of Defense counter drug operations throughout the Pacific. As a result of his efforts, Task Force West seized 40 metric tons of cocaine worth $700 million.

Manny graduated from the United States Coast Guard Academy, earning a Bachelor of Science in Naval Architecture and Marine Engineering.

Joseph Szyliowicz, PhD, is Professor Emeritus at the Josef Korbel School of International Studies, Denver University and the Founder of its Intermodal Transportation Institute. He has received numerous awards for his research activities and been a visiting fellow at St Antony's College, Oxford University, and the Institute for Advanced Studies and the Harry Truman Institute at Hebrew University, Jerusalem, among others. He has served as the International Co-Chair of the Sustainable Transportation Task Force of the China Council for International Cooperation and Environmental Development (2003–2008), has been a member of the US delegation to the Asia Pacific Economic Cooperation's Intermodal Transportation Working Group (2001–2007) and has participated in several NATO Advanced Research Workshops.

Professor Szyliowicz has published extensively on transportation security issues, most recently co-editing and co-authoring a series of comparative analyses of maritime, intermodal and aviation security. He is currently co-editing a special issue on freight transport security for Transportation Reviews. His PhD is in Political Science and Government from Columbia University in New York City.

Abbreviations and Acronyms

9/11	September 11, 2001 terrorist attacks on the United States
AI	Artificial Intelligence
AIS	Automatic Identification System (USCG)
APEC	Asia Pacific Economic Cooperation
ATM	Automated Teller Machine (banking)
BRI	People's Republic of China One Belt, One Road Initiative
BSR	Business Social Responsibility
Cal OES	California Office of Emergency Services
Caltrans	California Department of Transportation
CANG	California National Guard
CAPT	Captain
CBP	US Customs and Border Patrol
CCTV	Closed Circuit Television (security cameras)
CDR	Commander
CFR	Code of Federal Regulations
CG-791	USCG Office of Cyberspace Forces
CG FAC	USCG Office of Port and Facility Compliance
CISA	Cybersecurity and Infrastructure Security Agency
COL	Colonel
COSCO	Chinese Overseas Shipping Company (People's Republic-based shipping and port owner)
COVID-19	Corona Virus Disease, 2019, the cause of a worldwide pandemic
CSSA	Co-Sector Specific Agencies
C-TPAT	Customs Trade Partnership Against Terrorism
DHS	Department of Homeland Security

DEA	US Drug Enforcement Administration
DG MOVE	Directorate General for Mobility and Transport of the European Union
DLA	Defense Logistics Agency (DOD)
DOD	US Department of Defense
EC	European Commission
ECDIS	Electronic Chart Display and Information System
ESF	Emergency Support Function (FEMA), part of the National Response Framework
EU	European Union
FBI	Federal Bureau of Investigation
FDA	US Food and Drug Administration
FEMA	Federal Emergency Management Agency
FSR	Facility Security Requirements (TAPA)
GAO	Government Accountability Office
GCC	Government Coordinating Councils
GDP	Gross Domestic Product
GHG	Greenhouse Gasses
GPS	Global Positioning System
HMM	Hyundai Merchant Marine
IMO	United Nations' International Maritime Organization
IOT	Internet of Things, refers to connected appliances, electronics and motor vehicles
ISPS	International Ship and Port Facility Security Code
ISTEA	Intermodal Surface Transportation Efficiency Act
I-STEP	Intermodal Security Training and Exercise Program
IT	Information Technology
LCD	Least Developed Countries
LCDR	Lieutenant Commander

LNG	Liquefied Natural Gas
LRIT	Long Range Identification and Tracking system (IMO)
MTSA	Maritime Transportation Security Act
MTI	Mineta Transportation Institute
NATO	North American Treaty Organization
NAVTEX	NAVigational TEleX, a direct printing warning system for ships
NIST	National Institutes for Standards and Testing
NOAA	National Oceanic and Atmospheric Administration
NTC	National Targeting Center (CBP)
NVIC	Naval Vessel Inspection Circular (USCG)
OECD	Organization for Economic Cooperation and Development
OOI	Orient Overseas International (Hong Kong-based port owner)
PSPS	Public Safety Power Shutoff (California)
Ret.	Retired
RFID	Radio Frequency Identification
SCADA	Supervisory Control and Data Acquisition, a combination of hardware and software that uses computers to control processes
SCRM	Supply Chain Risk Management
SOLAS	International Convention for the Safety of Life at Sea
STSCS	Surface Transportation Supply Chain Security
TAPA	Transportation Asset Protection Association
TEU	Twenty-foot equivalent unit, a measure of cargo container capacity of a cargo container ship
TSA	Transportation Security Administration (DHS))
TSR	Trucking Security Requirements (TAPA)
TWIC	Transportation Workers Identification Card
UN	United Nations
US	United States

USB	Universal Serial Bus, a type of computer connection
USCG	Unites States Coast Guard
US DOT	United States Department of Transportation
VOIP	Voice Over Internet Protocol (computer-based phone system)
WTO	World Trade Organization

Endnotes

[1] Gregory J. Skulmoski, Francis T. Hartman and Jennifer Krahn, "The Delphi Method for Graduate Research." *Journal of Information Technology Education,* vol. 6, 2007, p. 1–21.

[2] United Nations Conference on Trade and Development. *Review of Maritime Transport, 2019*. https://unctad.org/en/PublicationsLibrary/rmt2019_en.pdf

[3] FEMA. *Supply Chain Resilience Guide*. (April 2019). p. 2. https://www.fema.gov/media-library-data/1555328671083-d9422177bd55d9c6fafc327a6b239290/SupplyChainResilienceGuide-April2019.pdf

[4] Department of Homeland Security, *National Strategy for Global Supply Chain Security* (Washington, DC: DHS, 2012, p. 1).

[5] Rhonda R. Lummus and Robert J. Vokurka, "Defining supply chain management: a historical perspective and practical guidelines," *Industrial Management & Data Systems*, 1999, vol. 99 No. 1, p. 11. https://doi.org/10.1108/02635579910243851

[6] John T. Mentzer, William DeWitt, James S. Keebler, Soonhong Min, Nancy W. Nix, Carlo D. Smith, Zach G. Zacharia. "Defining Supply Chain Management," *Journal of Business Logistics*, 22, 2011, p. 3.

[7] Frances L. Edwards, Daniel C. Goodrich, Margaret Hellweg and Jennifer Strauss, "Earthquake Early Warning Systems: International Experience," in Bandana Kar and David Cochran, eds., *Risk Communication in Community Resilience,* (London: Taylor & Francis, 2019).

[8] Guna Selvaduray, "Effect of Kobe Earthquake on Small Businesses," (paper presented at the Business Continuity Planning III Conference, Santa Clara, California, (November 20, 2022).

[9] Frances L. Edwards, Daniel C. Goodrich, Margaret Hellweg, Jennifer Strauss, Martin Eskijian and Omar Jaradat, *Great East Japan Earthquake, JR East Mitigation Successes, and Lessons for California High Speed Rail.* Report 12–37. San Jose, CA: Mineta Transportation Institute, 2015.

[10] Kelly L. Bennett, et al., "High infestation of invasive Aedes mosquitoes in used tires along the local transport network of Panama." *Parasites Vectors* 12, 264 (2019). https://doi.org/10.1186/s13071-019-3522-8

[11] Larry Kramer, "Use of Landbridge Cuts Containerized Cargo Travel Time." *The Washington Post*. (August 20, 1978). https://www.washingtonpost.com/archive/business/1978/08/20/use-of-landbridge-cuts-containerized-cargo-travel-time/ff1bc2de-c2ad-489a-bba9-c66e7e5cad69/

[12] Chamber of Commerce of the United States. "Land Transport Option Between Europe and Asia," (report presented at 18th Osce Economic and Environmental Forum, Vienna, 1–2 February 2010).

[13] Frances L. Edwards and Daniel C. Goodrich, *Introduction to Transportation Security.* Boca Raton, FL: CRC Press. 2012.

[14] Margot Roosevelt, "Truckers, dockworkers suffer as coronavirus chokes L.A., Long Beach ports cargo." *LA Times,* March 7, 2020. https://www.latimes.com/business/story/2020-03-07/la-fi-coronavirus-ports-california-economy

[15] John S. Pistole, "TSA's Ongoing Efforts to Expand and Improve Risk-Based Security," testimony before the House Committee on Appropriations, Subcommittee on Homeland Security (February 27, 2013). https://www.tsa.gov/news/press/testimony/2013/02/27/tsas-ongoing-efforts-expand-and-improve-risk-based-security

[16] Martijin Mes and Maria-Eugenia Iacob, "Synchromodal Transport Planning at a Logistics Service Provider," in: H. Zijm, M. Klumpp, U. Clausen, M. Hompel (eds) *Logistics and Supply Chain Innovation. Lecture Notes in Logistics*. Springer, Cham (2016).

[17] Project Management Institute, "Belt and Road Initiative," accessed July 7, 2020, https://mip.pmi.org/belt-and-road

[18] *The Economist,* "Special report: China's belt and road - Return to centre." (February 6, 2020).

[19] The Arctic Journal, "A year after its historic voyage, the Crystal Serenity is preparing to sail the Northwest Passage again." (May 24, 2017). https://www.arctictoday.com/a-year-after-its-historic-voyage-the-crystal-serenity-is-preparing-to-sail-the-northwest-passage-again/#:~:text=The%20Crystal%20Serenity%2C%20which%20has,passing%20through%20Canadian%20Arctic%20territory.

[20] Ocean Conservancy. "Protecting the Arctic- Bering Sea: Gateway to the Arctic." (2020). https://oceanconservancy.org/protecting-the-arctic/take-deep-dive/bering-strait-gateway-arctic/

[21] Richard A. Clarke and Robert Knake, *Cyber War.* New York: Ecco, 2010.

[22] Lori Musser, "Not your father's cranes and equipment." American Association of Port Administrators. *Seaport.* November 25, 2019. https://www.aapaseaports.com/index.php/2019/11/05/not-your-fathers-cranes-and-equipment/

[23] Richard A. Clarke and Robert Knake, Cyber War. New York: Ecco, 2010.

[24] Margot Roosevelt, "Truckers, dockworkers suffer as coronavirus chokes L.A., Long Beach ports cargo." *LA Times,* March 7, 2020. https://www.latimes.com/business/story/2020-03-07/la-fi-coronavirus-ports-california-economy

[25] Kelly L. Bennett, et al., "High infestation of invasive Aedes mosquitoes in used tires along the local transport network of Panama." *Parasites Vectors* 12, 264 (2019). https://doi.org/10.1186/s13071-019-3522-8

[26] Margot Roosevelt, "Truckers, dockworkers suffer as coronavirus chokes L.A., Long Beach ports cargo." *LA Times,* March 7, 2020. https://www.latimes.com/business/story/2020-03-07/la-fi-coronavirus-ports-california-economy

[27] See, for example, George A. Zsidisin and Bob Ritchie, eds., *Supply Chain Risk: A Handbook of Assessment, Management and Performance* (Springer Science Media, 2009).

[28] M. Asgari et al., "Supply Chain Management 1982-2015: A Review," *IMA Journal of Management Mathematics*, pp. 6, 12.

[29] Kahlid Bichou, Joseph S. Szyliowicz, and Luca Zamparini (Editors). *Maritime Transport Security: Issues, Challenges and National Policies*. (Northampton, MA: Edward Elgar Publishers, 2014); Joseph S. Szyliowicz, and Luca Zamparini (Editors). *Air Transport Security: Issues, Challenges and National Policies*. (Northampton, MA: Edward Elgar Publishers, 2018); Joeph S. Szyliowicz, Luca Zamparini, Genserik L.L. Reniers, and Dawna L. Rhoades (Editors). *Multimodal Transport Security: Frameworks and Policy Applications in Freight and Passenger Transport*. (Northampton, MA: Edward Elgar Publishers, 2016).

[30] Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute and Allied Telesis, San Jose, California, January 9–10, 2020.

[31] The papers will be published next year in a special issue of *Transport Reviews* co-edited by Joseph Szyliowicz and Luca Zamparini, the organizers of the workshop. Reported by Szyliowicz at the MTI Workshop, January 9, 2020.

[32] *The Economist*, "Over the white cliffs of Dover," (July 18, 2020), p. 6.

[33] Douglas Irwin, "Understanding Trump's Trade War," *Foreign Policy*, (Winter 2019).

[34] Jean Paul Rodrigue, "How Serious Are the Alternatives to the Panama Canal," Inter American Development Bank, accessed July 7, 2020 http://logisticsportal.iadb.org/node/4212?language=en; Muller, Nicholas, "The Chinese Railways Remolding East Africa," *The Diplomat*, January 25, 2019. Accessed July 7, 2020, https://thediplomat.com/2019/01/the-chinese-railways-remolding-east-africa/

[35] Craig McClory. De-Risking The Supply Chain. *Spend Matters.* (June 19, 2012). https://spendmatters.com/2012/06/19/derisking-the-supply-chain/

[36] Ibid.

[37] World Bank, "Gross Domestic Product 2018." https://databank.worldbank.org/data/download/gdp.pdf

[38] Ibid.

[39] US Census Bureau, "Foreign Trade," (2018.) https://www.census.gov/foreign-trade/balance/index.html

[40] Chamber of Commerce of the United States. "Land Transport Option Between Europe and Asia," report presented at 18th OSCE Economic and Environmental Forum, Vienna, 1–2 February 2010.

[41] When first used, the standard cargo container was 20 feet long. Today many cargo containers are 40 feet long. To be able to describe the capacity of a cargo container ship, the standard of a TEU has been set so that a 40-foot container is 2 TEUs, and a 20-foot container is 20 TEUs.

[42] ArcBeat. "10 Busiest Seaports in the World." (September 5, 2017). https://arcb.com/blog/10-busiest-seaports-in-the-world

[43] *The Economist*, "Biting the bullet." September 23, 2017, p. 65–66.

[44] Lori Musser, "Not your father's cranes and equipment." American Association of Port Administrators. *Seaport. (*November 25, 2019). https://www.aapaseaports.com/index.php/2019/11/05/not-your-fathers-cranes-and-equipment/

[45] Evert A. Bouman, Elizabeth Lindstad, Agathe I. Rialland, and Anders H. Strømman, "State-of-the-art technologies, measures, and potential for reducing GHG emissions from shipping – A review," *Transportation Research Part D: Transport and Environment*, 52, Part A (May 2017): 408–421.

[46] Evelyn Cheng, "Self-driving trucks likely to hit the roads before passenger cars." CNBC News. (November 22, 2019). https://www.cnbc.com/2019/11/22/self-driving-trucks-likely-to-hit-the-roads-before-passenger-cars.html

[47] Lauren Rosenblatt, "No driver needed: Self-driving trucks are starting to move cargo on the nation's highways." *Pittsburg Gazette* (March 30, 2020). https://www.post-gazette.com/business/tech-news/2020/03/30/self-driving-trucks-autonomous-cars-Locomation-Wilson-Logistics-Maven-Machines-Idelic/stories/202003290032

[48] Courtney Linder, "A Self-Driving Freight Truck Just Drove Across the Country to Deliver Butter." *Popular Mechanics* (December 11, 2019). https://www.popularmechanics.com/technology/infrastructure/a30196644/self-driving-truck-cross-country/

[49] Larry Kramer, "Use of Landbridge Cuts Containerized Cargo Travel Time." *The Washington Post.* (August 20, 1978). https://www.washingtonpost.com/archive/business/1978/08/20/use-of-landbridge-cuts-containerized-cargo-travel-time/ff1bc2de-c2ad-489a-bba9-c66e7e5cad69/

[50] American Association of Railroads, "Freight Railroads and International Trade" (February 2019). https://www.aar.org/wp-content/uploads/2018/08/Backgrounder-Freight-Railroads-and-International-Trade-August-2018.pdf

[51] Javier Garrido, "Container-ship size: What dimensions can we expect to see?" *Pier Next: Port of Barcelona,* (November 28, 2019). https://piernext.portdebarcelona.cat/en/mobility/container-

ship-size/#:~:text=Depth%20seems%20to%20stabilise%20around,for%20vessels%20over%2015%2C000%20TEUs.

[52] William Kremer, "How much bigger can container ships get?" *BBC News Magazine*. (February 19, 2013). https://www.bbc.com/news/magazine-21432226

[53] Lori Musser, "Not your father's cranes and equipment." American Association of Port Administrators. *Seaport.* November 25, 2019. https://www.aapaseaports.com/index.php/2019/11/05/not-your-fathers-cranes-and-equipment/

[54] *The Economist,* "Special report: China's belt and road - Return to centre." (February 6, 2020), p. 3.

[55] Jordi Torrent, "The New Silk Road: what next after COVID-19?" *Pier Next* (June 4, 2020). https://piernext.portdebarcelona.cat/en/mobility/the-new-silk-road-what-next-after-covid-19/

[56] *The Economist,* "Special report: China's belt and road - Return to centre." (February 6, 2020).

[57] Salvatore Balbones, "The New Eurasian Land Bridge Linking China And Europe Makes No Economic Sense, So Why Build It?" (December 28, 2017) *Forbes Magazine.* https://www.forbes.com/sites/salvatorebabones/2017/12/28/the-new-eurasian-land-bridge-linking-china-and-europe-makes-no-economic-sense-so-why-build-it/#237944e35c9c.

[58] Jordi Torrent, "The New Silk Road: what next after COVID-19?" Pier Next (June 4, 2020). https://piernext.portdebarcelona.cat/en/mobility/the-new-silk-road-what-next-after-covid-19/

[59] Jordi Torrent, "The New Silk Road: what next after COVID-19?" *Pier Next* (June 4, 2020). https://piernext.portdebarcelona.cat/en/mobility/the-new-silk-road-what-next-after-covid-19/

[60] Salvatore Balbones, "The New Eurasian Land Bridge Linking China and Europe Makes No Economic Sens e, So Why Build It?" (December 28, 2017.) *Forbes Magazine.* https://www.forbes.com/sites/salvatorebabones/2017/12/28/the-new-eurasian-land-bridge-linking-china-and-europe-makes-no-economic-sense-so-why-build-it/#237944e35c9c.

[61] *The Economist,* "Special report: China's belt and road - Return to centre." (February 6, 2020).

[62] Jordi Torrent, "The New Silk Road: what next after COVID-19?" *Pier Next* (June 4, 2020). https://piernext.portdebarcelona.cat/en/mobility/the-new-silk-road-what-next-after-covid-19/

[63] Ibid.

[64] *The Economist,* "Special report: China's belt and road - Return to centre." (February 6, 2020).

[65] Jordi Torrent, "The New Silk Road: what next after COVID-19?" *Pier Next* (June 4, 2020). https://piernext.portdebarcelona.cat/en/mobility/the-new-silk-road-what-next-after-covid-19/

[66] *The Economist*, "Special report: China's belt and road - Return to centre." (February 6, 2020), p. 4.

[67] Avery Thmpson, "A Container Ship Is Sailing Through the Arctic for the First Time." *Popular Mechanics* (September 18, 2018). https://www.popularmechanics.com/science/environment/a23307125/container-ship-arctic-voyage/

[68] The Arctic Journal, "A year after its historic voyage, the Crystal Serenity is preparing to sail the Northwest Passage again." (May 24, 2017). https://www.arctictoday.com/a-year-after-its-historic-voyage-the-crystal-serenity-is-preparing-to-sail-the-northwest-passage-again/#:~:text=The%20Crystal%20Serenity%2C%20which%20has,passing%20through%20Canadian%20Arctic%20territory.

[69] National Oceanic and Atmospheric Administration. "What is the law of the sea?" National Ocean Service website. (April 22, 2020). https://oceanservice.noaa.gov/Javierfacts/lawofsea.html#:~:text=The%20law%20of%20the%20sea%20is%20a%20body%20of%20customs,peaceful%20relations%20on%20the%20sea.&text=The%20United%20Nations%20(UN)%20held,resulted%20in%20a%201958%20Convention.

[70] Ocean Conservancy. "Protecting the Arctic- Bering Sea: Gateway to the Arctic." (2020). https://oceanconservancy.org/protecting-the-arctic/take-deep-dive/bering-strait-gateway-arctic/

[71] Encyclopedia Britannica, "Bering Strait." (2020). https://www.britannica.com/place/Arctic-Ocean/Topography-of-the-ocean-floor

[72] Vitaly Chernov, "New Port Planned for Russia's Growing Northern Logistics Chain." *The Maritime Executive.* (March 14, 2020). https://www.maritime-executive.com/blog/new-port-planned-for-russia-s-growing-northern-logistics-chain

[73] United Nations, *The State of Sustainable Supply Chains: Building Responsible and Resilient Supply Chains.* (August 17, 2016). New York: United Nations. P. 16. https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2Fsupply_chain%2Fwebinar-state-sustainable-supply-chains.pdf

[74] FEMA. *Supply Chain Resilience Guide.* (April 2019). p. 32. https://www.fema.gov/media-library-data/1555328671083-d9422177bd55d9c6fafc327a6b239290/SupplyChainResilienceGuide-April2019.pdf

[75] Guna Selvaduray, "Effect of Kobe Earthquake on Small Businesses," (paper presented at the Business Continuity Planning III Conference, Santa Clara, California, (November 20, 2022).

[76] United Nations, *The State of Sustainable Supply Chains: Building Responsible and Resilient Supply Chains.* (August 17, 2016). New York: United Nations.

[77] United Nations, *The State of Sustainable Supply Chains: Building Responsible and Resilient Supply Chains.* (August 17, 2016). New York: United Nations. https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2Fsupply_chain%2Fwebinar-state-sustainable-supply-chains.pdf

[78] Lori Musser, "Not your father's cranes and equipment." American Association of Port Administrators. *Seaport. (*November 25, 2019). https://www.aapaseaports.com/index.php/2019/11/05/not-your-fathers-cranes-and-equipment/

[79] Sarah Coble, "Stanford University Tops List of US Cybersecurity Degree Providers." *Info Security Magazine.* (2020). https://www.infosecurity-magazine.com/news/stanford-best-us-cybersecurity/

[80] DHS/CISA, "Cybersecurity." No date. https://www.cisa.gov/cybersecurity

[81] Sean Duca, "Supply chain remains the weakest link in cybersecurity." *Supply Chain* (January 17, 2020). https://www.supplychaindigital.com/technology/supply-chain-remains-weakest-link-cybersecurity

[82] Frances L. Edwards and Daniel C. Goodrich, *Introduction to Transportation Security.* Boca Raton, FL: CRC Press. 2012.

[83] U.S. Coast Guard, "Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels." Marine Safety Alert 06–19. July 8, 2019. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

[84] Phil Muncaster, "US Coast Guard Sounds Alarm After Ransomware Attack." *InfoSecurity Magazine* (January 2, 2020). https://www.infosecurity-magazine.com/news/us-coast-guard-sounds-alarm/

[85] Phil Muncaster, "US Coast Guard Sounds Alarm After Ransomware Attack." *InfoSecurity Magazine* (January 2, 2020). https://www.infosecurity-magazine.com/news/us-coast-guard-sounds-alarm/

[86] Department of Homeland Security/Department of Transportation, *Transportation System Sector-Specific Plan.* 2015. https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

[87] U.S. Navy, "NIST Offers Strategies to Secure Cyber Supply Chains, Seeks Industry Feedback." *CHIPS Magazine.* February 5, 2020. https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=13154

[88] U.S. Navy, "NIST Offers Strategies to Secure Cyber Supply Chains, Seeks Industry Feedback." *CHIPS Magazine.* February 5, 2020. https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=13154

[89] Transportation Security Administration. *TSA Strategy, 2018–2026*. (2018). https://www.tsa.gov/sites/default/files/tsa_strategy.pdf

[90] U.S. Department of Homeland Security, Transportation Security Administration. *2018 Biennial National Strategy for Transportation Security: Report to Congress*. (Washington D.C., April 4, 2018).

[91] 49 U.S.C. § 114(s)(3)(A), "Transportation Security Administration" (October 5, 2018).

[92] Johns Hopkins. "COVID-19 Dashboard, (June 8, 2020.) Coronavirus Resource Center. https://coronavirus.jhu.edu/map.html

[93] Johns Hopkins. "Asymptomatic Spread Makes Covid-19 Tough to Contain." *HUB Magazine.* (May 12, 2020). https://hub.jhu.edu/2020/05/12/gigi-gronvall-asymptomatic-spread-covid-19-immunity-passports/

[94] Statista. "Value of COVID-19 fiscal stimulus packages in G20 countries as of May 2020, as a share of GDP." Society/Economy. (May 25, 2020). https://www.statista.com/statistics/1107572/covid-19-value-g20-stimulus-packages-share-gdp/

[95] Bureau of Labor Statistics. "The Employment Situation, May 2020." News Release USDL-20-1140. https://www.bls.gov/news.release/pdf/empsit.pdf

[96] Erin Duffin, "Impact of the coronavirus pandemic on the global economy - Statistics & Facts." Statista. (June 4, 2020). https://www.statista.com/topics/6139/covid-19-impact-on-the-global-economy/

[97] Giacomo Tagnini, "Coronavirus Business Tracker: How The Private Sector Is Fighting The Covid-19 Pandemic." April 1, 2020. https://www.forbes.com/sites/giacomotognini/2020/04/01/coronavirus-business-tracker-how-the-private-sector-is-fighting-the-covid-19-pandemic/#369e81cc5899

[98] Erin Duffin, "Impact of the coronavirus pandemic on the global economy - Statistics & Facts." Statista (June 4, 2020). https://www.statista.com/topics/6139/covid-19-impact-on-the-global-economy/

[99] Joe MacDonald, "China Trade Slumps as Anti-Virus Controls Close Factories." *USA Today* (March 7, 2020). https://www.usnews.com/news/business/articles/2020-03-06/china-trade-slumps-as-anti-virus-controls-close-factories

[100] Patrick Burnson, "Cold chain investment for Port of Oakland paying off." *Port of Oakland Newsletter*. June 5, 2020. https://www.portofoakland.com/port-of-oakland-updates/

[101] Joe MacDonald, "China Trade Slumps as Anti-Virus Controls Close Factories." *USA Today* (March 7, 2020). https://www.usnews.com/news/business/articles/2020-03-06/china-trade-slumps-as-anti-virus-controls-close-factories

[102] Margot Roosevelt, "Truckers, dockworkers suffer as coronavirus chokes L.A., Long Beach ports cargo." *LA Times,* March 7, 2020. https://www.latimes.com/business/story/2020-03-07/la-fi-coronavirus-ports-california-economy

[103] Lisette Voytko, "China's Export Restrictions Reportedly Delaying Medical Supply Shipments To U.S." *Forbes Magazine (*April 16, 2020). https://www.forbes.com/sites/lisettevoytko/2020/04/16/chinas-export-restrictions-reportedly-delaying-medical-supply-shipments-to-us/#71aa8a4b1ba4

[104] Lisette Voytko, "China's Export Restrictions Reportedly Delaying Medical Supply Shipments To U.S." *Forbes Magazine (*April 16, 2020). https://www.forbes.com/sites/lisettevoytko/2020/04/16/chinas-export-restrictions-reportedly-delaying-medical-supply-shipments-to-us/#71aa8a4b1ba4

[105] Potomac Institute for Policy Studies. *Security Strategies for Global Supply Chains: Addressing Risk, Seizing Opportunity*. (Washington, D.C., 2018).

[106] Department of Homeland Security/Department of Transportation, *Transportation Systems Sector*. *Activities Progress Report* (2018), p. 3. https://www.cisa.gov/sites/default/files/publications/transportation_systems_sector_activities_progress_report_20190503_508.pdf

[107] Lauren Rosenblatt, "No driver needed: Self-driving trucks are starting to move cargo on the nation's highways." *Pittsburg Gazette* (March 30, 2020). https://www.post-gazette.com/business/tech-news/2020/03/30/self-driving-trucks-autonomous-cars-Locomation-Wilson-Logistics-Maven-Machines-Idelic/stories/202003290032

[108] Helene Cooper, "Chinese Hackers Steal Unclassified Data From Navy Contractor," *New York Times,* June 8, 2018, Section A, page 13.

[109] M. Asgari, et al., "Supply Chain Management 1982-2015: A Review," *IMA Journal of Management Mathematics*, (2016): 6, 12. https://eprints.kingston.ac.uk/35046/1/Asgari-N035046-AAM.pdf

[110] See, for example, George A. Zsidisin and Bob Ritchie, eds., Supply Chain Risk: A Handbook of Assessment, Management and Performance (Springer Science Media, 2009).

[111] W. Ho et al., Supply Chain Risk Management: a Literature Review, International Journal of Production Research, vol 53, 2015, #16, p. 5033.

[112] Op. cit., Table 10, p. 5059.

[113] Rao, Shashank and Goldsby, Thomas J., "Supply chain risks: a review and typology," *The International Journal of Logistics Management*, 22 May 2009, Vol.20(1), p. 99.

[114] On the role and use of concepts in the social sciences, see Gary Goertz, *Social Science Concepts: A User's Guide*, (Princeton University Press, 2006) and John Gerring, *Social Science Methodology: A Criterial Framework* (2nd edition, Cambridge University Press, 2011.

[115] Ho et al., Table 10, p. 5059.

[116] Heiko A. von der Gracht, Inga-Lena Darkow, "The future role of logistics for global wealth – scenarios and discontinuities until 2025," Foresight, 15, no. 5 (2013): 405–419). See also Christoph Markmann, Inga-Lena Darkow, Heiko A. von der Gracht, "A Delphi-based Risk Analysis-Identifying and Assessing Future Challenges for Supply Chain Security in a Multi-Stakeholder Environment," Technological Forecasting and Social Change, 80, no. 8 (November 2013).

[117] Der Gracht, et al., Figure 4, p. 412.

[118] Heiko A. von der Gracht, The Future of Logistics (Gabler Edition Wissenschaft, 2008, pp. 245ff.

[119] Ho, op. cit, p. 5059.

[120] https://www.bsr.org/our-insights/primersfFuture-of -Supply-chains-2025

[121] Council on Foreign Relations (CFR) Workshop. "The Future of Global Supply Chains." June 27, 2016, Accessed November 4, 2019, https://www.cfr.org/report/future-global-supply-chains

[122] Gould, JulieF., Cathy Macharis, Hans-Dietrich Haasis, "Emergence of Security in Supply Chain Management Literature," Journal of Transport Security, 2010, pp. 282–302, p.293.

[123] See https://www.tsa.gov/for-industry/surface-transportation

[124] See, for example, https://www.fbi.gov/contact-us/field-offices/houston/news/press-releases/fbi-and-federal-partners-brief-pipeline-industry-leaders-on-national-security-threats-to-energy-infrastructure

[125] Amy del-Mar Agamez Arias and Jose Moyano-Fuentes, "Intermodal Transport in Freight Distribution: A Literature Review," Transportation Reviews, vol. 37, no. 6, pp. 782–807.

[126] Marinko Maslarich et al., "Intermodal Supply Chain Risk Management," Pomorski Zbornik, 52 (2016): 11–30, especially p. 28.

[127] Transportation Security Administration, *TSA Strategy, 2018-2026.* (Washington, DC: DHS, n.d.). https://www.tsa.gov/sites/default/files/tsa_strategy.pdf

[128] Suisheng Zhao, "China's Belt-Road Initiative as the Signature of President Xi Jinping Diplomacy: Easier Said than Done, Journal of Contemporary China, doi: 10.1080?10670564.2019.1645483

[129] OECD, *Trade Patterns in the 2060 World Economy*, Economics Department Working Papers No. 1142, p. 36.

[130] https://www.weforum.org/agenda/2014/12/the-worlds-changing-trade-patterns/

[131] https://www.congress.gov/event/116th-congress/house-event/109805

[132] Jonathan Jacobson. "Climate Change Could Make Russia Great Again: A golden opportunity for Russia is buried under the ice caps, which are now melting" November 9, 2019, https://www.haaretz.com/amp/world-news/.premium.MAGAZINE-climate-change-could-make-russia-great-again-1.8094614?__twitter_impression=true. See also Charles Digges, "Putin Decrees an Increase in Arctic traffic," *Maritime Executive*, May 16, 2018. Accessed July 7, 2020. https://www.maritime-executive.com/article/putin-decrees-an-increase-in-arctic-traffic

[133] (https://www.portandterminal.com/un-to-shipping-industry-we-are-headed-for-an-environmental-disaster)

[134] Cited in htps.www.althingsupplychain.com/how-can-we-make-supply-chains-more-sustainable

[135] Rob O'Byrne "6 Key Supply Chain and Logistics Trends to Watch in 2017" Logistics Bureau, Dec 19, 2017.

[136] Sarwant Singh, "Future of Logistics: Five Technologies That Will Self-Orchestrate the Supply Chain" September 22, 2016, https;//www.forbes.com

[137] *The Maritime Executive,* "Holt Logistics Joins Blockchain Initiative," April 19, 2018. https://www.maritime-executive.com/article/holt-logistics-joins-blockchain-initiative

[138] https://scm.ncsu.edu/scm-articles/article/homeland-security-is-using-supply-chain-analytics-to-go-after-organized-crime-and-traffickers

[139] Daniel R. Coates, "Worldwide Threat Assessment of the US Intelligence Committee," 13 February 2018. Accessed July 7, 2020. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

[140] Rupert Herbert-Burns, "Playing Catchup," *The Maritime Executive*, October, 2019.

[141] Andrew R. Lee, "Are Stakeholders Finally Taking Maritime Cybersecurity Seriously?" GTSC, Homeland Security Today, US, October 4, 2018.

[142] David Rider, "Maritime Meets Cyber Security," The Maritime Executive, 16 October, 2019.

[143] Nicholas A. Glavin, "Protecting the Maritime Shipping Industry from Cybercrime," Center for International Maritime Security, March 19, 2018.

[144] See Deloitte's 2019 Global Blockchain Survey, https://www2.deloitte.com/us/en/insights/topics/understanding-blockchain-potential/global-blockchain-survey.html?id=us:2ps:3gl:confidence:eng:cons:32019:nonem:na:or5UUOPb:1141606376:346859115084:b:Blockchain:Blockchain_Survey_BMM:nb

[145] See Joseph S. Szyliowicz, Luca Zamparini, et al., eds., Multimodal Transport Security: Frameworks and Policy Applications in Freight and Passenger Transport (Edward Elgar, 2016).

[146] https://www.digitalcommerce360.com/2018/05/15/why-digital-supply-chain-officers-need-to-be-seen-and-heard/

[147] See, for example, A. Michael Knemeyer, Walter Zinn, Cuneyt Eroglu, Proactive planning for catastrophic events in supply chains, Journal of Operations Management, April, 2009, pp. 141–153.

[148] https://www2.deloitte.com/ye/en/pages/risk/articles/third-party-governance-and-risk-management.html

[149] Yaoming Zhou, Junwei Wang, and Hai Yang, "Resilience and Transportation systems: Concepts and Comprehensive Review," IEEE Transactions on Intelligent Transportation Systems, December, 2018, Figure 2, Table 1.

[150] Ibid., p. 11.

[151] https://www.dhs.gov/sites/default/files/publications/transportation_systems_sector_activities_progress_report_20190503_508.pdf

[152] Ibid., p. 2.

[153] Ibid., p. 3.

[154] Ibid., p. 9.

[155] See, for example, US Customs and Border Protection, *Container Security Initiative: Securing the Trade Lanes* (2008, April 8).

[156] Tony Mannisto and Juha Hintsa, "A Decade of GAO's Supply Chain Security Oversight," *Proceedings of the Hamburg International Conference of Logistics,* August 2015, p. 7, https://pdfs.semanticscholar.org/1021/89dcc884cbb157e546497f82c09fc666e63c.pdf?_ga=2.40305766.55267565.1573942791-419257360.1573942791

[157] Ibid., p. 7.

[158] Ibid., p. 9.

[159] "Explore Key Issues by Topic," US Government Accountability Office, n.d., https://www.gao.gov/key_issues/overview#t=1

[160] For an analysis of how "resilience" and "vulnerability" have been conceptualized in regards to transportation, see Aura Reggiani, Peter Nijkamp, and Diego Lanzi, "Transport resilience and vulnerability: The role of connectivity," Transportation Research Part A 81 (2015) 4–15.

[161] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[162] Ibid.

[163] Ibid.

[164] Ibid.

[165] Ibid.

[166] Perkins, Jeanne, Riding Out Future Quakes. Oakland, CA: Association of Bay Area Governments. (2003).

[167] Kevin Krick, "Maritime Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[168] Frances Edwards, Comment at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[169] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[170] Hakim, Danny, "Aboard a Cargo Colossus," New York Times, October 5, 2014, p. BU-4.

[171] Kevin Krick, "Maritime Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[172] Kevin Krick, "Maritime Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[173] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[174] National Academies of Science, Engineering and Medicine, Disaster Resilience: A National Imperative, (2012). Washington DC: National Academies Press.

[175] Edwards, Frances L. and Daniel C. Goodrich, *Introduction to Transportation Security,* (2012), Boca Raton, FL: CRC Press.

[176] US DOT, "Goals and Objectives for a Stronger Maritime Nation: A Report to Congress," Washington, D.C. (February 2020), p. 1.

[177] Seafarer's Log, "DOT Releases National Maritime Strategy." Seafarer's International Union. May 1, 2020. https://www.seafarers.org/seafarerslogs/2020/05/dot-releases-national-maritime-strategy/

[178] Lt. Bill Gasparetti, "Security Since 9/11: Creating the Maritime Transportation Security Act and the ISPS Code." *Homeland Security Today.* February 9, 2018. https://www.hstoday.us/uncategorized/security-since-9-11-creating-maritime-transportation-security-act-isps-code/

[179] Lt. Bill Gasparetti, "Security Since 9/11: Creating the Maritime Transportation Security Act and the ISPS Code." *Homeland Security Today.* February 9, 2018. https://www.hstoday.us/uncategorized/security-since-9-11-creating-maritime-transportation-security-act-isps-code/

[180] Lars Bergqvist, "ISPS Code and Maritime Terrorism." *The Maritime Executive* (July 17, 2014). https://www.maritime-executive.com/article/The-ISPS-Code-and-Maritime-Terrorism-2014-07-17

[181] Xeneta, "Transportation Insights." https://www.xeneta.com/blog/what-are-isps-charges

[182] Lars Bergqvist, "ISPS Code and Maritime Terrorism." *The Maritime Executive* (July 17, 2014). https://www.maritime-executive.com/article/The-ISPS-Code-and-Maritime-Terrorism-2014-07-17

[183] Xeneta, "Transportation Insights." https://www.xeneta.com/blog/what-are-isps-charges

[184] Capt. Rajeev Jassal, "USPS Code: 9 Important and Must Know Elements," MySeaTime. January 5, 2017. https://www.myseatime.com/blog/detail/what-is-isps-code-and-security-levels

[185] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[186] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[187] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[188] Lori Musser, "Not your father's cranes and equipment." American Association of Port Administrators. *Seaport.* November 25, 2019. https://www.aapaseaports.com/index.php/2019/11/05/not-your-fathers-cranes-and-equipment/

[189] ArcBeat. "10 Busiest Seaports in the World." (September 5, 2017). https://arcb.com/blog/10-busiest-seaports-in-the-world

[190] Enoch Yiu, "US security concerns force Cosco-owned Orient Overseas to sell Long Beach port in California." *South China Morning Post*, (April 30, 2019).

[191] Duncan DeAeth," US forces China's COSCO to relinquish ownership of California port." *Taiwan Times,* May 10, 2019. https://www.taiwannews.com.tw/en/news/3699054

[192] Manuel Raras, III, "Factors Impacting Security of Arctic Maritime Routes," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[193] Freight Waves, "Experts Warn of China's Influence at US Ports." Bezinga, October 22, 2019. https://www.benzinga.com/news/19/10/14640988/experts-warn-of-chinas-influence-at-us-ports

[194] Eleanor Albert, "China's Global Port Play: China's port building plans are more complex than conventional wisdom suggests." *The Diplomat.* May 11, 2019. https://thediplomat.com/2019/05/chinas-global-port-play/

[195] Freight Waves, "Experts Warn of China's Influence at US Ports." Bezinga, October 22, 2019 (No page). https://www.benzinga.com/news/19/10/14640988/experts-warn-of-chinas-influence-at-us-ports

[196] Freight Waves, "Experts Warn of China's Influence at US Ports." Bezinga, October 22, 2019 (No page).https://www.benzinga.com/news/19/10/14640988/experts-warn-of-chinas-influence-at-us-ports

[197] Richard A. Clarke and Robert Knacke. *Cyber War.* New York: Ecco. 2010.

[198] Kevin Krick, "Maritime Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[199] *The Economist*, "This Week in Politics." P. 5 (June 27, 2020).

[200] Kevin Krick, "Maritime Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[201] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[202] Reuters, "China, Greece agree to push ahead with COSCO's Piraeus Port investment." November 11, 2019. https://www.reuters.com/article/us-greece-china/china-greece-agree-to-push-ahead-with-coscos-piraeus-port-investment-idUSKBN1XL1KC

[203] CDR Romulus Matthews, USCG, "Port Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[204] Manuel Raras, III, "Factors Impacting Security of Arctic Maritime Routes," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[205] Manuel Raras, III, "Factors Impacting Security of Arctic Maritime Routes," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[206] Natalie Bannerman, "Cinia moves full speed ahead with Arctic Connect," *Capacity,* Aguste 30, 2019. https://www.capacitymedia.com/articles/3824070/cinia-moves-full-speed-ahead-with-arctic-connect

[207] Manuel Raras, III, "Factors Impacting Security of Arctic Maritime Routes," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[208] Manuel Raras, III, "Factors Impacting Security of Arctic Maritime Routes," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[209] United Nations Convention on the Law of the Sea, Part II Territorial Sea and Contiguous Zone, December 10, 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm#:~:text=SECTION%201.,GENERAL%20PROVISIONS&text=The%20sovereignty%20of%20a%20coastal,described%20as%20the%20territorial%20sea.

[210] United Nations Convention on the Law of the Sea, Part V, Exclusive Economic Zone, December 10, 1982. https://www.un.org/depts/los/convention_agreements/texts/unclos/part5.htm

[211] Manuel Raras, III, "Factors Impacting Security of Arctic Maritime Routes," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[212] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[213] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[214] Robert Bernardo, "Bay Area Welcomes CMA CGM Benjamin Back to Port of Oakland," Port of Oakland, (February 25, 2016). https://www.portofoakland.com/press-releases/press-release-509/

[215] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[216] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[217] Joe Pinsker, "How 14,000 Workers Managed to Slow Down the Entire Economy," *The Atlantic*, (February 24, 2015). https://www.theatlantic.com/business/archive/2015/02/how-only-14000-workers-briefly-slowed-down-the-entire-economy/385858/

[218] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[219] Ibid.

[220] Brian Michael Jenkins and Frances L. Edwards, *Saving City Lifelines: Lessons Learned in the 9/11 Terrorist Attacks.* San Jose, CA: Mineta Transportation Institute (2003). https://transweb.sjsu.edu/research/saving-city-lifelines-lessons-learned-9-11-terrorist-attacks

[221] US Customs and Border Protection, C-TPAT: Customs Trade Partnership Against Terrorism, June 1, 2020. https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat

[222] US Congress, Maritime Transportation Security Act of 2002, PUBLIC LAW 107–295—NOV. 25, 2002. https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf

[223] US Congress, Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law No: 107-188 – June 12, 2002. https://www.congress.gov/107/plaws/publ188/PLAW-107publ188.pdf

[224] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[225] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[226] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[227] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[228] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[229] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[230] US Coast Guard, "Automatic Identification System Overview." US Coast Guard Navigation Center, Department of Homeland Security. (April 17,2020). https://navcen.uscg.gov/?pageName=AISmain

[231] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[232] Ibid.

[233] Paul Koscak, "Working together: Catching Smugglers, Terrorists and Lawbreakers Works Better Through Partnership," US Customs and Border Protection, (n.d.). https://www.cbp.gov/frontline/cbp-national-targeting-center

[234] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[235] US Coast Guard, "Long Range Identification and Tracking (LRIT) Overview." Navigation Center. https://navcen.uscg.gov/?pageName=lritMain

[236] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[237] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[238] Ibid.

[239] Ibid.

[240] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020

[241] LCDR Robert Cole, "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[242] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[243] Zain Shauk, "Malware on oil rig computers raises security fears," *The Houston Chronicle* (February 23, 2013). https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php

[244] LCDR Robert Cole, "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[245] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[246] LCDR Robert Cole, "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[247] *The Maritime Executive,* "Report: APM-Run Terminal May Have Had Cyber Loopholes." *The Maritime Executive* (July 10, 2017).

[248] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[249] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[250] Gzim Ocakoglu, European Union, "European Union Supply Chain Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[251] LCDR Robert Cole, "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[252] Mike Freeman, "2 Iranian men indicted for ransomware cyberattacks on US targets, including Port of San Diego." *The San Diego Union Tribune.* (November 28, 2018). https://www.sandiegouniontribune.com/business/technology/sd-fi-charges-port-of-san-diego-ransomware-20181128-story.html#:~:text=The%20Port%20of%20San%20Diego%20reported%20a%20ransomware%20attack%20on,Harbor%20Police%20also%20were%20affected.

[253] LCDR Robert Cole, "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[254] Ash Padwal, Allied Telesis, "Cyber Issues in Transportation Supply Chain Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[255] Ash Padwal, Allied Telesis, "Cyber Issues in Transportation Supply Chain Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[256] Ash Padwal, Allied Telesis, "Cyber Issues in Transportation Supply Chain Security," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[257] Cole, LCDR Robert. "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[258] US Coast Guard, "Navigation and Vessel Inspection Circulars (NVIC)," (n.d.). https://www.dco.uscg.mil/Our-Organization/NVIC/#:~:text=Navigation%20and%20Vessel%20Inspection%20Circulars%20(NVIC)&text=NVIC's%20are%20used%20internally%20by,are%20adequate%2C%20complete%20and%20consistent

[259] US Coast Guard, *Office of Port and Facility Compliance 2019 Annual Report,* p. 10. (May 21, 2020). https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Year%20in%20Review/CG-FAC%20YearInReview%202019_Final.pdf?ver=2020-05-21-081529-687

[260] Cole, LCDR Robert. "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[261] US Coast Guard, Office of Port and Facility Compliance 2019 Annual Report. (May 21, 2020). https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Year%20in%20Review/CG-FAC%20YearInReview%202019_Final.pdf?ver=2020-05-21-081529-687

[262] Cole, LCDR Robert. "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[263] Cole, LCDR Robert. "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[264] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[265] LCDR Robert Cole, "Maritime Supply Chain Security and Cyber Systems," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[266] Ibid.

[267] Ibid.

[268] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[269] California Public Utilities Commission, "Public Safety Power Shutoff/De-Energization." (2020). https://www.cpuc.ca.gov/deenergization/

[270] Mitchell Medigovich, "Power and the Transportation Supply Chain's Security." presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

[271] Ibid.

[272] Ibid.

[273] Ibid.

[274] Asim Hussain, "California's largest planned power shut off (so far): what happened?" Better Electrons: Bloom Energy Blog. (October 25, 2019).

https://www.bloomenergy.com/blog/californias-largest-planned-power-outage-so-far-what-happened

[275] Mitchell Medigovich, "Power and the Transportation Supply Chain's Security." presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[276] Steven John, "11 incredible facts about the $700 billion US trucking industry." *Business Insider.* (June 3, 2019). https://markets.businessinsider.com/news/stocks/trucking-industry-facts-us-truckers-2019-5-1028248577#:~:text=And%20trucks%20move%20more%20than,transported%20around%20the%20United%20States

[277] KOLO 8 News Staff, "Fuel pipeline from California to Reno reopened." KOLO 8 News. (October 23, 2019). https://www.kolotv.com/content/news/Pipeline-that-brings-gas-to-Reno-shut-down-by-PGE-outage-562771441.html

[278] Mitchell Medigovich, "Power and the Transportation Supply Chain's Security." presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[279] Ibid.

[280] Ibid.

[281] Ibid.

[282] Ibid.

[283] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[284] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[285] CDR Romulus Matthews, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[286] Rob Garner, "Solar Storm and Space Weather - Frequently Asked Questions." NASA Sun-Earth website. Section 13. No date. Accessed June 3, 2020. https://www.nasa.gov/mission_pages/sunearth/spaceweather/index.html

[287] Frances L. Edwards, convener, Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[288] Kevin Krick, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[289] NATO, "NATO Policy Directors discuss strengthening resilience and preparations for second wave in the COVID-19 pandemic," (July 8, 2020). https://www.nato.int/cps/en/natohq/news_177101.htm?selectedLocale=en

[290] European Union, "About the EU: Countries." January 13, 2021 Accessed January 14, 2021, https://europa.eu/european-union/about-eu/countries_en

[291] Gzim Ocakoglu, "European Union's Supply Chain Security." Presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[292] Ibid.

[293] News Wires, "Thalys train gunman sentenced to life in jail over foiled 2015 terror attack." France 24. (December 17, 2020). https://www.france24.com/en/france/20201217-thalys-train-gunman-sentenced-to-life-in-jail-over-foiled-2015-terror-attack

[294] European Commission, "European Commission puts forward action plan to improve security of rail passengers in the EU." European Commission, Mobility and Transport: Rail. (August 13, 2018). https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en

[295] Gzim Ocakoglu, "European Union's Supply Chain Security." Presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[296] European Union Agency for Railways, *Rail Freight in the European Union*, 2016. https://www.era.europa.eu/sites/default/files/library/docs/leaflets/rail_freight_in_the_european_union_en.pdf

[297] Gzim Ocakoglu, "European Union's Supply Chain Security." Presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[298] European Commission, *EC Security Guidance for the European Commercial Road Freight Transport Sector.* (2019). doi: 10.2832/97074

[299] Alissa J. Ruben and Aurelian Breeden, "France Remembers the Nice Attack: 'We Will Never Find the Words'. *New York Times.* (July 14, 2017). https://www.nytimes.com/2017/07/14/world/europe/nice-attack-france-bastille-day.html

[300] European Commission, *EC Security Guidance for the European Commercial Road Freight Transport Sector*. (2019). doi: 10.2832/97074

[301] Jan Benini, "Perspectives: NATO Resilience Program," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[302] APEC, "What is Asia Pacific Economic Cooperation?" 2020. Accessed January 12, 2021, https://www.apec.org/About-Us/About-APEC

[303] Jan Benini, "Perspectives: NATO Resilience Program," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[304] Ibid.

[305] Ibid.

[306] Annie Palmer, "Amazon wins FAA approval for Prime Air drone delivery fleet. CNBC. (August 31, 2020). https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html

[307] AIRMIC, "Preventing cargo theft in the luxury goods industry," (February 3, 2015). https://www.airmic.com/news-story/preventing-cargo-theft-luxury-goods-industry

[308] Jan Benini, "Perspectives: NATO Resilience Program," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[309] Ibid.

[310] NATO, "We Are NATO," (2017). https://www.nato.int/wearenato/why-was-nato-founded.html

[311] NATO, "Civil Preparedness." (October 27, 2020). https://www.nato.int/cps/en/natohq/topics_49158.htm

[312] NATO, "Resilience and Article 3." (November 16, 2020). https://www.nato.int/cps/en/natohq/topics_132722.htm

[313] NATO, "Collective Defense, Article 5." (November 25, 2019). https://www.nato.int/cps/en/natohq/topics_110496.htm

[314] NATO, "Civil Preparedness." (October 27, 2020). https://www.nato.int/cps/en/natohq/topics_49158.htm

[315] Jan Benini, "Perspectives: NATO Resilience Program," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[316] NATO, "Allies and Partners address critical infrastructure as a key enabler to enhance resilience," (December 17, 2018), https://www.nato.int/cps/en/natohq/news_161675.htm?selectedLocale=en

[317] Jan Benini, "Perspectives: NATO Resilience Program," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[318] NATO, "NATO Policy Directors discuss strengthening resilience and preparations for second wave in the COVID-19 pandemic," (July 8, 2020). https://www.nato.int/cps/en/natohq/news_177101.htm?selectedLocale=en

[319] Jan Benini, "Perspectives: NATO Resilience Program," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, (January 9, 2020).

[320] Patrick Burnson, "The hijacking of the Maersk Alabama 10 years ago: the threat is still real," *Logistics Management*. (April 12, 2019). https://www.logisticsmgmt.com/article/the_hijacking_of_the_maersk_alabama_10_years_ago_the_threat_is_still_real

[321] Chris Isidore, "West Coast ports shut down as labor dispute heats up," *CNN Business*, (February 14, 2015). https://money.cnn.com/2015/02/12/news/companies/port-shutdown/

[322] Jill Aitoro, "US logistics boss talks risks to the supply chain and protective measures," *Defense News,* n.p. (October 28, 2019). https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/

[323] Robert Muggah, "Why the Latest Cyberattack was Different," *Foreign Policy*. (January 11, 2021). https://foreignpolicy.com/2021/01/11/cyberattack-hackers-russia-svr-gru-solarwinds-virus-internet/

Bibliography

49 U.S.C. § 114(s)(3)(A), *Transportation Security Administration*. October 5, 2018.

Aitoro, Jill, "US logistics boss talks risks to the supply chain and protective measures," *Defense News*, n.p. October 28, 2019. Accessed January 12, 2021, https://www.defensenews.com/interviews/2019/10/28/us-logistics-boss-talks-risks-to-the-supply-chain-and-protective-measures/

Albert, Eleanor, "China's Global Port Play: China's port building plans are more complex than conventional wisdom suggests." *The Diplomat*. May 11, 2019. Accessed February 2, 2020, https://thediplomat.com/2019/05/chinas-global-port-play/

American Association of Railroads, "Freight Railroads and International Trade," February 2019. Accessed July 7, 2020. https://www.aar.org/wp-content/uploads/2018/08/Backgrounder-Freight-Railroads-and-International-Trade-August-2018.pdf

ArcBest. "10 Busiest Seaports in the World." September 5, 2017. Accessed May 1, 2020. https://arcb.com/blog/10-busiest-seaports-in-the-world

Agamez, Arias Amy del-Mar and Jose Moyano-Fuentes. "Intermodal Transport in Freight Distribution: A Literature Review." *Transportation Review*, 37, no.6 (2017): 782–807.

Asgari, Nasrin, Ehsan Nikbakhsh, Alex Hill, Reza Zanjirani Farahani. "Supply chain management 1982–2015: A review." *IMA Journal of Management Mathematics* (2016): 353–397. Accessed November 16, 2019. https://doi.org/10.1093/imaman/dpw004

Balbones, Salvatore. "The New Eurasian Land Bridge Linking China and Europe Makes No Economic Sense, So Why Build It?" December 28, 2017. *Forbes Magazine*. Accessed May 1, 2020. https://www.forbes.com/sites/salvatorebabones/2017/12/28/the-new-eurasian-land-bridge-linking-china-and-europe-makes-no-economic-sense-so-why-build-it/#237944e35c9c.

Bannerman, Natalie, "Cinia moves full speed ahead with Arctic Connect," *Capacity,* August 30, 2019. Accessed July 20, 2020, https://www.capacitymedia.com/articles/3824070/cinia-moves-full-speed-ahead-with-arctic-connect

Benini, Jan, "Perspective: NATO Resilience Program," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

Bernardo, Robert, "Bay Area Welcomes CMA CGM Benjamin Back to Port of Oakland," *Port of Oakland*, February 25, 2016. Accessed February 5, 2020. https://www.portofoakland.com/press-releases/press-release-509/

Bergqvist, Lars, "ISPS Code and Maritime Terrorism." *The Maritime Executive*. July 17, 2014. Accessed February 2, 2020, https://www.maritime-executive.com/article/The-ISPS-Code-and-Maritime-Terrorism-2014-07-17

Bichou, Kahlid, Joseph S. Szyliowicz, and Luca Zamparini (Editors). *Maritime Transport Security: Issues, Challenges and National Policies*. Northampton, MA: Edward Elgar Publishers, 2014.

Bouman, Everet A., Elizabeth Lindstad, Agathe I. Rialland, and Anders H. Strømman. "State-of-the-art technologies, measures, and potential for reducing GHG emissions from shipping – A review." *Transportation Research Part D: Transport and Environment*, 52, Part A (May 2017): 408–421.

Burnson, Patrick, "The hijacking of the Maersk Alabama 10 years ago: the threat is still real," *Logistics Management*. April 12, 2019. Accessed January 12, 2021, https://www.logisticsmgmt.com/article/the_hijacking_of_the_maersk_alabama_10_years_ago_the_threat_is_still_real

Business for Social Responsibility (BSR). "The Future of Supply Chains, 2025." Accessed February 6, 2020, https://www.bsr.org/our-insights/primersfFuture-of -Supply-chains-2025

California Public Utilities Commission, "Public Safety Power Shutoff/De-Energization." (2020). https://www.cpuc.ca.gov/deenergization/

Chamber of Commerce of the United States. "Land Transport Option Between Europe and Asia," report presented at 18th OSCE Economic and Environmental Forum, Vienna, 1–2 February 2010.

Cheng, Evelyn, "Self-driving trucks likely to hit the roads before passenger cars." *CNBC News*. (November 22, 2019). Accessed March 27, 2020. https://www.cnbc.com/2019/11/22/self-driving-trucks-likely-to-hit-the-roads-before-passenger-cars.html

Chernov, Vitaly. "New Port Planned for Russia's Growing Northern Logistics Chain." *The Maritime Executive*. (March 14, 2020). Accessed April 15, 2020. https://www.maritime-executive.com/blog/new-port-planned-for-russia-s-growing-northern-logistics-chain

Clarke, Richard A. and Robert Knake, *Cyber War*. New York: Ecco, 2010.

Daniel R. Coates, "Worldwide Threat Assessment of the US Intelligence Committee." February 13, 2018. Accessed July 7, 2020. https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf

Coble, Sarah. "Stanford University Tops List of US Cybersecurity Degree Providers." *Info Security Magazine*. 2020. Accessed May 30, 2020. https://www.infosecurity-magazine.com/news/stanford-best-us-cybersecurity/

Cole, LCDR Robert. "Maritime Supply Chain Security and Cyber Systems." Presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

Cooper, Helene, "Chinese Hackers Steal Unclassified Data From Navy Contractor." *New York Times*, June 8, 2018, Section A, page 13.

Council of Supply Chain Management Professionals, "30th Annual State of Logistics Report." (June, 2019).

Council on Foreign Relations (CFR) Workshop. "The Future of Global Supply Chains." June 27, 2016, Accessed November 4, 2019, https://www.cfr.org/report/future-global-supply-chains

CSCMP, Thomas J. Goldsby, Deepak Iyengar, Shashank Rao, *Definitive Guide to Transportation: The Principles, Strategies, and Decisions for the Effective Flow of Goods and Services*. Hoboken, NJ: Pearson FT Press, 2014.

DeAeth, Duncan, "US forces China's COSCO to relinquish ownership of California port." *Taiwan Times*, May 10, 2019. Accessed February 2, 2020. https://www.taiwannews.com.tw/en/news/3699054Deloitte, "Third-party governance and risk management: The threats are real." Accessed November 5, 2019. https://www2.deloitte.com/ye/en/pages/risk/articles/third-party-governance-and-risk-management.html

Department of Homeland Security/CISA, "Cybersecurity." No date. Accessed April 15, 2020. https://www.cisa.gov/cybersecurity

Department of Homeland Security, National Strategy for Global Supply Chain Security. Washington, DC: DHS, 2012, p. 1.

Department of Homeland Security/Department of Transportation, Transportation Systems Sector Activities Progress Report, 2018. Accessed January 25, 2020. https://www.cisa.gov/sites/default/files/publications/transportation_systems_sector_activities_progress_report_20190503_508.pdf

Department of Homeland Security/Department of Transportation, Transportation System Sector-Specific Plan. 2015. Accessed January 25, 2020, https://www.cisa.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf

Department of Homeland Security, Transportation Security Administration. 2018 Biennial National Strategy for Transportation Security: Report to Congress. Washington D.C., April 4, 2018.

Digges, Charles, "Putin Decrees an Increase in Arctic traffic." *Maritime Executive*, May 16, 2018. Accessed July 7, 2020. https://www.maritime-executive.com/article/putin-decrees-an-increase-in-arctic-traffic

Duca, Sean, "Supply chain remains the weakest link in cybersecurity." *Supply Chain*, January 17, 2020. Accessed April 15, 2020. https://www.supplychaindigital.com/technology/supply-chain-remains-weakest-link-cybersecurity

Duffin, Erin, "Impact of the coronavirus pandemic on the global economy - Statistics & Facts." *Statista*. June 4, 2020. Accessed June 6, 2020. https://www.statista.com/topics/6139/covid-19-impact-on-the-global-economy/

Edwards, Frances L. and Daniel C. Goodrich. *Introduction to Transportation Security*. Boca Raton, FL: CRC Press, 2012.

Edwards, Frances L., Daniel C. Goodrich, Margaret Hellweg and Jennifer Strauss, "Earthquake Early Warning Systems: International Experience." In Bandana Kar and David Cochran, eds., *Risk Communication in Community Resilience*. London: Taylor & Francis, 2019.

Edwards, Frances L, Daniel C. Goodrich, Margaret Hellweg, Jennifer Strauss, Martin Eskijian and Omar Jaradat, *Great East Japan Earthquake, JR East Mitigation Successes, and Lessons for California High Speed Rail*. Report 12–37. San Jose, CA: Mineta Transportation Institute, 2015.

Encyclopedia Britannica, "*Bering Strait."* 2020. Accessed June 6, 2020. https://www.britannica.com/place/Arctic-Ocean/Topography-of-the-ocean-floor

European Commission, EC Security Guidance for the European Commercial Road Freight Transport Sector. (2019). Accessed October 29, 2020, doi: 10.2832/97074.

European Commission, "European Commission puts forward action plan to improve security of rail passengers in the EU." *European Commission, Mobility and Transport: Rail*. August 13, 2018. Accessed February 2, 2020. https://ec.europa.eu/transport/modes/rail/news/2018-06-12-action-plan-security-rail-passengers_en

European Union, "About the EU: Countries." January 13, 2021 Accessed January 14, 2021, https://europa.eu/european-union/about-eu/countries_en

European Union Agency for Railways, Rail Freight in the European Union, 2016. Accessed January 20, 2021.

https://www.era.europa.eu/sites/default/files/library/docs/leaflets/rail_freight_in_the_european_union_en.pd

Federal Bureau of Investigation. "FBI and Federal Partners Brief Pipeline Industry Leaders on National Security Threats to Energy Infrastructure." Accessed November 7, 2019. https://www.fbi.gov/contact-us/field-offices/houston/news/press-releases/fbi-and-federal-partners-brief-pipeline-industry-leaders-on-national-security-threats-to-energy-infrastructure

FEMA. Supply Chain Resilience Guide. April 2019. Accessed April 15, 2020. https://www.fema.gov/media-library-data/1555328671083-d9422177bd55d9c6fafc327a6b239290/SupplyChainResilienceGuide-April2019.pdf

Freeman, Mike. "2 Iranian men indicted for ransomware cyberattacks on US targets, including Port of San Diego." *The San Diego Union Tribune*. November 28, 2018. Accessed October 21, 2020, https://www.sandiegouniontribune.com/business/technology/sd-fi-charges-port-of-san-diego-ransomware-20181128-story.html#:~:text=The%20Port%20of%20San%20Diego%20reported%20a%20ransomware%20attack%20on,Harbor%2

Freight Waves. "Experts Warn of China's Influence at US Ports." Bezinga, October 22, 2019. Accessed April 10, 2020, https://www.benzinga.com/news/19/10/14640988/experts-warn-of-chinas-influence-at-us-ports

Garrido, Javier. "Container-ship size: What dimensions can we expect to see?" *Pier Next: Port of Barcelona*, November 28, 2019. Accessed January 30, 2020. https://piernext.portdebarcelona.cat/en/mobility/container-ship-size/#:~:text=Depth%20seems%20to%20stabilise%20around,for%20vessels%20over%2015%2C000%20TEUs

Ganin, Alexander A., Emanuele Massaro, Alexander Gutfraind, Nicolas Steen, Jeffrey M Keisler, Alexander Kott, Rami Mangoubi, and Igor Linkov. "Operational resilience: concepts, design and analysis." *Scientific Reports*, 6, no. 1 (2016): 1–12.

Garner, Rob, "Solar Storm and Space Weather - Frequently Asked Questions." NASA Sun-Earth website. Section 13. No date. Accessed June 3, 2020. https://www.nasa.gov/mission_pages/sunearth/spaceweather/index.html

Gasparetti, Lt. Bill. "Security Since 9/11: Creating the Maritime Transportation Security Act and the ISPS Code." *Homeland Security Today*. February 9, 2018. Accessed February 2, 2020, https://www.hstoday.us/uncategorized/security-since-9-11-creating-maritime-transportation-security-act-isps-code/

General Accounting Office, Key Issues, Accessed November 4, 2019, https://www.gao.gov/key_issues/overview#t=1

Gerring, John, Social Science Methodology: A Criterial Framework, 2nd edition, Cambridge University Press, 2011.

Goertz, Gary, Social Science Concepts: A User's Guide, Princeton University Press, 2006.Ho, Willian, Tian Zheng, Hakan Yildiz, and Srinivas Talluri. "Supply Chain Risk Management: a Literature Review." *International Journal of Production Research*, April, 2015, vol. 53, pp. 5031-5069. Accessed January 30, 2020. doi.org/10.1080/00207543.2015.1030467

Gould, Julie F., Cathy Macharis, Hans-Dietrich Haasis. "Emergence of Security in Supply Chain Management Literature." *Journal of Transport Security* (2010): 282–302.

Hakim, Danny, "Aboard a Cargo Colossus," *New York Times*, October 5, 2014, p. BU-4.

Ho, William, et al., Supply Chain Risk Management: a Literature Review, *International Journal of Production Research*, vol 53, 2015, #16.

Hussain, Asim. "California's largest planned power shut off (so far): what happened?" Better Electrons: Bloom Energy Blog. October 25, 2019. Accessed October 15, 2020, https://www.bloomenergy.com/blog/californias-largest-planned-power-outage-so-far-what-happened

Irwin, Douglas. "Understanding Trump's Trade War." *Foreign Policy*, (Winter 2019).

Isidore, Chris. "West Coast ports shut down as labor dispute heats up," *CNN Business*, February 14, 2015. Accessed January 12, 2021. https://money.cnn.com/2015/02/12/news/companies/port-shutdown/

Jacobson, Jonathan. "Climate Change Could Make Russia Great Again: A golden opportunity for Russia is buried under the ice caps, which are now melting." November 9, 2019, https://www.haaretz.com/amp/world-news/.premium.MAGAZINE-climate-change-could-make-russia-great-again-1.8094614?__twitter_impression=true

Jassal, Capt. Rajeev. "ISPS Code: 9 Important and Must Know Elements." MySeaTime. January 5, 2017. Accessed June 5, 2020, https://www.myseatime.com/blog/detail/what-is-isps-code-and-security-levels

Johns Hopkins. "Asymptomatic Spread Makes Covid-19 Tough to Contain." *HUB Magazine*. May 12, 2020. June 6, 2020. https://hub.jhu.edu/2020/05/12/gigi-gronvall-asymptomatic-spread-covid-19-immunity-passports/

Johns Hopkins. "COVID-19 Dashboard." June 8, 2020. Coronavirus Resource Center. Accessed June 10, 2020. https://coronavirus.jhu.edu/map.html

Knemeyer, Michael A., Walter Zinn, Cuneyt Eroglu. "Proactive planning for catastrophic events in supply chains." *Journal of Operations Management*, April, 2009, pp. 141–153.

KOLO 8 News Staff, "Fuel pipeline from California to Reno reopened." *KOLO 8 News*. October 23, 2019. Accessed December 27, 2020, https://www.kolotv.com/content/news/Pipeline-that-brings-gas-to-Reno-shut-down-by-PGE-outage-562771441.html

Koscak, Paul. "Working together: Catching Smugglers, Terrorists and Lawbreakers Works Better Through Partnership," US Customs and Border Protection, (n.d.). Accessed October 28, 2020, https://www.cbp.gov/frontline/cbp-national-targeting-center

Kramer, Larry, "Use of Landbridge Cuts Containerized Cargo Travel Time." *The Washington Post*, August 20, 1978. Accessed January 30, 2020. https://www.washingtonpost.com/archive/business/1978/08/20/use-of-landbridge-cuts-containerized-cargo-travel-time/ff1bc2de-c2ad-489a-bba9-c66e7e5cad69/

Krick, Kevin, "Transportation Supply Chain Security: Challenges and Approaches," presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

Linder, Courtney, "A Self-Driving Freight Truck Just Drove Across the Country to Deliver Butter." *Popular Mechanics*, December 11, 2019. Accessed April 15, 2020. https://www.popularmechanics.com/technology/infrastructure/a30196644/self-driving-truck-cross-country/

Linkov, Igor, Daniel A Eisenberg, Matthew E Bates, Derek Chang, Matteo Convertino, Julia H Allen, Stephen E Flynn, Thomas P Seage. "Measurable resilience for actionable policy." *Environmental Science and Technology*, 47, no. 18 (2013): 10108–10110.

Lummus, Rhonda R. and Robert J. Vokurka. "Defining supply chain management: a historical perspective and practical guidelines." *Industrial Management & Data Systems*, 1999, vol. 99 No. 1, pp. 1–117. Accessed April 15, 2020. https://doi.org/10.1108/02635579910243851

Mannisto, Tony and Juha Hintsa, "A Decade of GAO's Supply Chain Security Oversight." 2015, Accessed 20October 28, 2019, https://pdfs.semanticscholar.org/1021/89dcc884cbb157e546497f82c09fc666e63c.pdf?_ga=2.40305766.55267565.1573942791-419257360.1573942791

Markmann, Christopher, Inga-Lena Darkow, Heiko A. von der Gracht. "A Delphi-based Risk Analysis-Identifying and Assessing Future Challenges for Supply Chain Security in a Multi-Stakeholder Environment." *Technological Forecasting and Social Change*, 80, no. 8 (November 2013): 1815–1833.

Martens, Bobby.J., Michael R. Crum, and Richard F. Poist. "Examining Antecedents to Supply Chain Effectiveness: An Exploratory Study." *Journal of Business Logistics*, 32, no. 2 (June 2011). Accessed April 15, 2020. doi: 10.1111/j.2158-1592.2011.01013.x

Matthews, CDR Romulus, "Maritime Transportation Security," presentation at the Surface Transportation Supply Chain Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

McClory, Craig. "De-Risking the Supply Chain." Spend Matters. June 19, 2012. Accessed June 6, 2020. https://spendmatters.com/2012/06/19/derisking-the-supply-chain/

Medigovich, Mitchell. "Power and the Transportation Supply Chain's Security." Presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

Mentzer, John T., William DeWitt, James S. Keebler, Soonhong Min, Nancy W. Nix, Carlo D. Smith, Zach G. Zacharia. "Defining Supply Chain Management." *Journal of Business Logistics*, May 2011, vol 22, issue 2.

Mes, Martijin and Maria-Eugenia Iacob. "Synchromodal Transport Planning at a Logistics Service Provider." In: H. Zijm, M. Klumpp, U. Clausen, M. Hompel (eds) *Logistics and Supply Chain Innovation*. Lecture Notes in Logistics. Springer, Cham, 2016.

Muggah, Robert. "Why the Latest Cyberattack was Different." *Foreign Policy*, January 11, 2021. Accessed January 19, 2021, https://foreignpolicy.com/2021/01/11/cyberattack-hackers-russia-svr-gru-solarwinds-virus-internet/

Muller, Nicholas. "The Chinese Railways Remolding East Africa." The Diplomat, January 25, 2019. Accessed July 7, 2020, https://thediplomat.com/2019/01/the-chinese-railways-remolding-east-africa/

Muncaster, Paul. "US Coast Guard Sounds Alarm After Ransomware Attack." *InfoSecurity Magazine*. January 2, 2020. Accessed January 30, 2020. https://www.infosecurity-magazine.com/news/us-coast-guard-sounds-alarm/

Musser, Lori. "Not your father's cranes and equipment." *American Association of Port Administrators*. Seaport. November 25, 2019. Accessed May 12, 2020. https://www.aapaseaports.com/index.php/2019/11/05/not-your-fathers-cranes-and-equipment/

National Oceanic and Atmospheric Administration. "What is the law of the sea?" National Ocean Service website. April 22, 2020. Accessed May 12, 2020. https://oceanservice.noaa.gov/facts/lawofsea.html#:~:text=The%20law%20of%20the%20sea%20is%20a%20body%20of%20customs,peaceful%20relations%20on%20the%20sea.&text=The%20United%20Nations%20(UN)%20held,resulted%20in%20a%201958%20Convention

NATO. "Allies and Partners address critical infrastructure as a key enabler to enhance resilience." December 17, 2018. Accessed January 13, 2021, https://www.nato.int/cps/en/natohq/news_161675.htm?selectedLocale=en

NATO. "Civil Preparedness." October 27, 2020. Accessed January 10, 2021, https://www.nato.int/cps/en/natohq/topics_49158.htm

NATO. "Collective Defense, Article 5." November 25, 2019. Accessed January 10, 2021, https://www.nato.int/cps/en/natohq/topics_110496.htm

NATO. "NATO Member States." August 31, 2020. Accessed January 10, 2021, https://www.nato.int/cps/en/natohq/nato_countries.htm

NATO. "NATO Policy Directors discuss strengthening resilience and preparations for second wave in the COVID-19 pandemic," July 8, 2020. Accessed January 13,2021, https://www.nato.int/cps/en/natohq/news_177101.htm?selectedLocale=en

NATO. "Resilience and Article 3." November 16, 2020. Accessed January 13, 2021. https://www.nato.int/cps/en/natohq/topics_132722.htm

NATO. "We Are NATO." (2017). https://www.nato.int/wearenato/why-was-nato-founded.html

News Wires. "Thalys train gunman sentenced to life in jail over foiled 2015 terror attack." France 24. December 17, 2020. https://www.france24.com/en/france/20201217-thalys-train-gunman-sentenced-to-life-in-jail-over-foiled-2015-terror-attack

Ocakoglu, Gzim. "European Union Supply Chain Security." Presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

Ocean Conservancy. "Protecting the Arctic- Bering Sea: Gateway to the Arctic." 2020. Accessed May 12, 2020. https://oceanconservancy.org/protecting-the-arctic/take-deep-dive/bering-strait-gateway-arctic/

Padwal, Ash, Allied Telesis. "Cyber Issues in Transportation Supply Chain Security." Presentation at the Surface Transportation Supply Chan Security Workshop, Mineta Transportation Institute, San Jose, CA, January 9, 2020.

Palmer, Annie. "Amazon wins FAA approval for Prime Air drone delivery fleet." August 31, 2020. Accessed January 12, 2021, https://www.cnbc.com/2020/08/31/amazon-prime-now-drone-delivery-fleet-gets-faa-approval.html

Perkins, Jeanne. Riding Out Future Quakes. Oakland, CA: Association of Bay Area Governments. (2003).

Pinsker, Joe. "How 14,000 Workers Managed to Slow Down the Entire Economy," *The Atlantic*, February 24, 2015. Accessed July 7, 2020, https://www.theatlantic.com/business/archive/2015/02/how-only-14000-workers-briefly-slowed-down-the-entire-economy/385858/

Pistole, John S. "TSA's Ongoing Efforts to Expand and Improve Risk-Based Security," testimony before the House Committee on Appropriations, Subcommittee on Homeland Security (February 27, 2013). Accessed July 21, 2020, https://www.tsa.gov/news/press/testimony/2013/02/27/tsas-ongoing-efforts-expand-and-improve-risk-based-security

Port of Rotterdam, "HMM Algeciras, the largest container ship worldwide, on its way to Rotterdam." Press release, May 26, 2020. Accessed June 10, 2020. https://www.portofrotterdam.com/en/news-and-press-releases/hmm-algeciras-the-largest-container-ship-worldwide-on-its-way-to-rotterdam#:~:text=HMM%20is%20the%20new%20name,largest%20container%20shipping%20line%20worldwide

Potomac Institute for Policy Studies. Security Strategies for Global Supply Chains: Addressing Risk, Seizing Opportunity. Washington, D.C., 2018.

Rao, Shashank, Goldsby, Thomas J., Supply chain risks: a review and typology." *The International Journal of Logistics Management*, 20, 22 May 2009, pp. 97–123.

Reggiani, Aura, Peter Nijkamp, and Diego Lanzi. "Transport resilience and vulnerability: The role of connectivity." *Transportation Research* Part A 81 (2015) 4–15.

Reuters. "China, Greece agree to push ahead with COSCO's Piraeus Port investment." November 11, 2019. Accessed December 15, 2020, https://www.reuters.com/article/us-greece-china/china-greece-agree-to-push-ahead-with-coscos-piraeus-port-investment-idUSKBN1XL1KC

Rodrigue, Jean-Paul. "How Serious Are the Alternatives to the Panama Canal." Inter-American Development Bank. Accessed July 7, 2020, http://logisticsportal.iadb.org/node/4212?language=en

Rodrigue, Jean-Paul and Brian Slack. *The Geography of Transport Systems*. New York: Routledge, 2020.

Rosenblatt, Lauren. "No driver needed: Self-driving trucks are starting to move cargo on the nation's highways." *Pittsburg Gazette*, March 30, 2020. Accessed April 15, 2020. https://www.post-gazette.com/business/tech-news/2020/03/30/self-driving-trucks-autonomous-cars-Locomation-Wilson-Logistics-Maven-Machines-Idelic/stories/202003290032

Ruben, Alissa J. and Aurelian Breeden. "France Remembers the Nice Attack: 'We Will Never Find the Words.'" *New York Times*, July 14, 2017. Accessed January 3, 2021, https://www.nytimes.com/2017/07/14/world/europe/nice-attack-france-bastille-day.html

Seafarer's Log. "DOT Releases National Maritime Strategy." Seafarer's International Union. May 1, 2020. Accessed June 14, 2020, https://www.seafarers.org/seafarerslogs/2020/05/dot-releases-national-maritime-strategy/

Selvaduray, Guna. "Effect of Kobe Earthquake on Small Businesses." paper presented at the Business Continuity Planning III Conference, Santa Clara, California, November 20, 2002.

Shauk, Zain. "Malware on oil rig computers raises security fears." *The Houston Chronicle*, February 23, 2013. Accessed July 14, 2020. https://www.houstonchronicle.com/business/energy/article/Malware-on-oil-rig-computers-raises-security-fears-4301773.php

Skulmoski, Gregory J., Francis T. Hartman and Jennifer Krahn. "The Delphi Method for Graduate Research." *Journal of Information Technology Education*, 6 (2007): 1–21.

Smythe, Tiffany C. "Assessing the Impacts of Hurricane Sandy on the Port of New York and New Jersey's Maritime Responders and Response Infrastructure," National Science Foundation Quick Response Grant 238. May 31, 2013. Accessed July 7, 2020. https://hazards.colorado.edu/uploads/quick_report/smythe_2013.pdf

Statista. "Value of COVID-19 fiscal stimulus packages in G20 countries as of May 2020, as a share of GDP." Society/Economy, May 25, 2020. Accessed June 6, 2020. https://www.statista.com/statistics/1107572/covid-19-value-g20-stimulus-packages-share-gdp/

Szyliowicz, Joseph S. and Luca Zamparini (Editors). Air Transport Security: Issues, Challenges and National Policies. Edward Elgar Publishers, 2018.

Szyliowicz, Joseph S., Luca Zamparini, Genserik L.L. Reniers, and Dawna L. Rhoades (Editors). Multimodal Transport Security: Frameworks and Policy Applications in Freight and Passenger Transport. Northampton, MA: Edward Elgar Publishers, 2016.

The Arctic Journal, "A year after its historic voyage, the Crystal Serenity is preparing to sail the Northwest Passage again." May 24, 2017. Accessed May 12, 2020. https://www.arctictoday.com/a-year-after-its-historic-voyage-the-crystal-serenity-is-preparing-to-sail-the-northwest-passage-again/#:~:text=The%20Crystal%20Serenity%2C%20which%20has,passing%20through%20Canadian%20Arctic%20territory.

The Economist, "Biting the bullet." September 23, 2017, pp. 65–66.

The Economist, "Ninety percent of everything," June 20, 2020, p. 66.

The Economist, "Over the white cliffs of Dover," July 18, 2020, p. 6.

The Economist, "Special report: China's belt and road - Return to centre." February 6, 2020.

The Economist, "This Week in Politics." June 27, 2020, p. 5.

The Maritime Executive, "Report: APM-Run Terminal May Have Had Cyber Loopholes." July 10, 2017. Accessed July 14, 2020, https://www.maritime-executive.com/article/report-apmt-rotterdam-may-have-had-cyber-loopholes

Thompson, Avery. "A Container Ship Is Sailing Through the Arctic for the First Time." Popular Mechanics September 18, 2018. Accessed May 12, 2020. https://www.popularmechanics.com/science/environment/a23307125/container-ship-arctic-voyage/

Timmons, Heather, "Houston's vital port will reopen on Friday, after being mostly spared by Hurricane Harvey," Quartz, August 31, 2017. Accessed July 7, 2020. https://qz.com/1067032/hurricane-harvey-the-port-of-houston-is-reopening-after-being-spared-by-the-storm/

Tingstad, Abbie, Michael T. Wilson, Katherine Anania, Jordan R. Fischbach, Susan A. Resetar, Scott Savitz, Kristin Van Abel, R. J. Briggs, Aaron C. Davenport, Stephanie Pezard, Kristin Sereyko, Jonathan Theel, Marc Thibault, Edward Ulin, Developing New Future Scenarios for the U.S. Coast Guard's Evergreen Strategic Foresight Program. Santa Monica, CA: RAND Corporation. 2017. Accessed February 2, 2020, https://www.rand.org/content/dam/rand/pubs/research_reports/RR3100/RR3147/RAND_RR3147.pdf

Torrent, Jordi. "The New Silk Road: what next after COVID-19?" Pier Next. June 4, 2020. Accessed June 15, 2020. https://piernext.portdebarcelona.cat/en/mobility/the-new-silk-road-what-next-after-covid-19/

Transportation Research Board. (2020). TRID. Accessed April 15, 2020. http://trid.trb.org

Transport Security Administration. "Surface Transportation Resources." no date. Accessed April 15, 2020. https://www.tsa.gov/for-industry/surface-transportation

Transport Security Administration. TSA Strategy, 2018–2026. no date. Accessed April 15, 2020. https://www.tsa.gov/sites/default/files/tsa_strategy.pdf

United Nations Conference on Trade and Development. *Review of Maritime Transport*, 2019. April 15, 2020. https://unctad.org/en/PublicationsLibrary/rmt2019_en.pdf

United Nations Convention on the Law of the Sea, Part II Territorial Sea and Contiguous Zone, December 10, 1982. Accessed July 20, 2020, https://www.un.org/depts/los/convention_agreements/texts/unclos/part2.htm#:~:text=SECTION%201.,GENERAL%20PROVISIONS&text=The%20sovereignty%20of%20a%20coastal,described%20as%20the%20territorial%20sea

United Nations Convention on the Law of the Sea, Part V, Exclusive Economic Zone, December 10, 1982. Accessed July 20, 2020, https://www.un.org/depts/los/convention_agreements/texts/unclos/part5.htm

United Nations, The State of Sustainable Supply Chains: Building Responsible and Resilient Supply Chains. August 17, 2016. New York: United Nations. Accessed January 30, 2020. https://d306pr3pise04h.cloudfront.net/docs/issues_doc%2Fsupply_chain%2Fwebinar-state-sustainable-supply-chains.pdf

U.S. Census Bureau, "Foreign Trade," 2018. Accessed June 8, 2020. https://www.census.gov/foreign-trade/balance/index.html

US Climate Resilience Toolkit, "Anticipated Arctic Transit Routes," last modified January 3, 2017. Accessed February 2, 2020, https://toolkit.climate.gov/image/1212

US Coast Guard, "Automatic Identification System Overview." US Coast Guard Navigation Center, Department of Homeland Security. April 17,2020, Accessed May 25, 2020, https://navcen.uscg.gov/?pageName=AISmain

US Coast Guard, "Cyber Incident Exposes Potential Vulnerabilities Onboard Commercial Vessels." Marine Safety Alert 06-19. July 8, 2019. Accessed April 15, 2020. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf

US Coast Guard, "Navigation and Vessel Inspection Circulars (NVIC)," n.d. Accessed July 7, 2020, https://www.dco.uscg.mil/Our-Organization/NVIC/#:~:text=Navigation%20and%20Vessel%20Inspection%20Circulars%20(NVIC)&text=NVIC's%20are%20used%20internally%20by,are%20adequate%2C%20complete%20and%20consistent

US Coast Guard, Office of Port and Facility Compliance 2019 Annual Report. May 21, 2020. Accessed October 25, 2020, https://www.dco.uscg.mil/Portals/9/CG-FAC/Documents/Year%20in%20Review/CG-FAC%20YearInReview%202019_Final.pdf?ver=2020-05-21-081529-687

US Congress, Maritime Transportation Security Act of 2002, Public Law 107–295—Nov. 25, 2002. Accessed July 7, 2020. https://www.congress.gov/107/plaws/publ295/PLAW-107publ295.pdf

US Congress, Public Health Security and Bioterrorism Preparedness and Response Act of 2002, Public Law No: 107–188 June 12, 2002. Accessed July 7, 2020. https://www.congress.gov/107/plaws/publ188/PLAW-107publ188.pdf

US Customs and Border Protection. "Container Security Initiative: Securing the Trade Lanes." PowerPoint presentation, April 8, 2008.

US Customs and Border Protection, C-TPAT: Customs Trade Partnership Against Terrorism, June 1, 2020. Accessed July 7, 2020. https://www.cbp.gov/border-security/ports-entry/cargo-security/ctpat

US DOT, "Goals and Objectives for a Stronger Maritime Nation: A Report to Congress," Washington, D.C., February 2020, p. 1.

Vineyard, Jared, "Hurricane Sandy Update: New York and New Jersey Ports," International Shipping, November 1, 2012. Accessed July 7, 2020. https://www.universalcargo.com/hurricane-sandy-update-new-jersey-and-new-york-ports/

von der Gracht, Heiko A. The Future of Logistics: Scenarios for 2025, Wiesbaden: Gabler Verlag, 2008.

von der Gracht, Heiko A., Inga-Lena Darkow. "The future role of logistics for global wealth – scenarios and discontinuities until 2025." *Foresight*, 15, no. 5 (2013): 405–419.

Voytko, Lisette, "China's Export Restrictions Reportedly Delaying Medical Supply Shipments to U.S." *Forbes Magazine* (April 16, 2020). Accessed June 6, 2020. https://www.forbes.com/sites/lisettevoytko/2020/04/16/chinas-export-restrictions-reportedly-delaying-medical-supply-shipments-to-us/#71aa8a4b1ba4

World Bank, "Gross Domestic Product 2018." Accessed April 15, 2020. https://databank.worldbank.org/data/download/gdp.pdf

Xeneta, "Transportation Insights." No date. Accessed June 10, 2020. https://www.xeneta.com/blog/what-are-isps-charges

Yiu, Enoch. "US security concerns force COSCO-owned Orient Overseas to sell Long Beach port in California." South China Morning Post, April 30, 2019. Accessed June 10, 2020. https://www.scmp.com/business/companies/article/3008324/us-security-concerns-force-cosco-owned-orient-overseas-sell-long

Zhang, Mo and A.J. Pel, "Synchromodal hinterland freight transport: Model study for the port of Rotterdam." *Journal of Transport Geography*, 52 (2016) 1–10. 2015.

Zhou, Yaoming, Junwei Wang, and Hai Yang. "Resilience and Transportation systems: Concepts and Comprehensive Review." *IEEE Transactions on Intelligent Transportation Systems* (December 20, 2019): pp. 4262–4276.

Zsidisin George A. and Bob Ritchie, eds., *Supply Chain Risk: A Handbook of Assessment, Management and Performance*. Dordrecht, The Netherlands: Springer Science Media, 2009.

About the Authors

Frances Edwards

Frances Edwards is the deputy director of the Mineta Transportation Institute's Allied Telesis National Transportation Security Center and, since 2006, the director of the San Jose State University Master of Public Administration program. She is the Principal Investigator for this research. She is the co-author or editor of four books, thirteen publications for MTI, and numerous articles and book chapters. She is a certified emergency manager.

Dan Goodrich

Dan Goodrich is the senior transportation security scientist for the Mineta Transportation Institute. He was the lead discussant for the workshop, developed the adversary materials bibliography, as well as contributing to this report. He is a certified emergency manager, a master exercise practitioner, and a certified security specialist, with sixteen years' active military service, including US Marine Corps Security Forces. He is the co-author of *Introduction to Transportation Security*.

Joseph Szyliowicz

Joseph Szyliowicz is Professor Emeritus at the Korbel School of International Studies, Denver University and the Founder of its Intermodal Transportation Institute. He led the development of the bibliography, as well as co-authoring the report. He is an internationally renowned scholar, working with NATO, the European Union and the Asia Pacific International Cooperation Group, as well as holding fellowships at Oxford and Hebrew University. He is the author of numerous books on transportation modes and transportation security.

Bill Medigovich

Colonel William (Bill) Medigovich (USAR, Ret.) is a research associate with Mineta Transportation Institute. He has a long and distinguished career in public service, including Army Intelligence, California Department of Justice, director of the California Office of Emergency Services, administrator of FEMA Region IX, and director of the US Department of Transportation's emergency management enterprise worldwide. He is co-author of *Generic Continuity of Operations/Continuity of Government Plan for State-Level Transportation Agencies* for MTI.

Liz Lange

Liz Lange is a student research assistant with the Mineta Transportation Institute. She provided logistics support for the workshop, assisted with the production of the report, and created portions of the bibliography. She completed her Master of Public Administration degree.

Autumn Anderton

Autumn Anderton was a student research assistant at the University of Denver who created portions of the bibliography. She has completed her master's degree.

MTI FOUNDER

Hon. Norman Y. Mineta

MTI BOARD OF TRUSTEES

Directors

MTI MINETA TRANSPORTATION INSTITUTE