HSPI ISSUE BRIEF #19

Transportation and Supply Chain Security: Systemic Changes and Policy Opportunities

Christian Beckner
Paul Gross
Walter Todd, Jr.

THE GEORGE WASHINGTON UNIVERSITY
HOMELAND SECURITY
POLICY INSTITUTE

May 24, 2013

Support provided by

ICF
INTERNATIONAL

Founded in 2003, the George Washington University Homeland Security Policy Institute (HSPI) is a nonpartisan "think and do" tank whose mission is to build bridges between theory and practice to advance homeland security through an interdisciplinary approach. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, HSPI creates innovative strategies and solutions to current and future threats to the nation.

Comments should be directed to hspi@gwu.edu. For more information on HSPI and its programs, please visit http://homelandsecurity.gwu.edu.

A. Introduction

The global transportation system and supply chain are the circulatory system of the global economy, moving people and goods across countries and around the world, facilitating both personal exchange as well as the operations of nearly every industry sector today.

In the past several decades these global networks of transportation and trade have become increasingly integrated and interdependent, decreasing the costs and accelerating the speed of the movement of people and goods. However, this integration and complex interdependency has led to new risks to the system, making it more vulnerable to disruption, whether from a terrorist attack, a manmade accident, or a natural disaster.

We have seen numerous examples of the impact of transportation and supply chain disruptions in the last two decades. For example, in the days following the terrorist attacks of 9/11, the United States saw and felt the impact of a disruption to its transportation system and global supply chain: airline flights grounded nationwide and internationally, trucks lined up for miles at U.S. land borders, and uncertain decision-making about inbound cargo ships. Ultimately the system rebounded and trade and travel resumed; but if these systems had been slowed or delayed for a prolonged period of time, there would have been serious economic consequences for the global economy.

A second recent example of a systemic disruption was the major earthquake and tsunami in Japan in March 2011, which had similar impacts on trade and travel. The supply chains of major automotive companies were disrupted due to key suppliers' factories that had been destroyed by the tsunami. The disaster (including the Fukushima nuclear plant meltdown that resulted from the tsunami) had a significant negative impact on economic factors and travel to Japan.

These examples, and many others, have raised awareness of the vulnerabilities of our global transportation system and supply chain. This awareness has led to an increase in efforts by governments and by the private sector to improve the security and resilience of these systems. But it has also led to increasing awareness among malicious actors about the opportunities to exploit and attack these systems in ways that can cause significant disruption and economic harm.

This paper will examine the progress that has been made to improve the security and resilience of the global transportation and supply chain systems, focusing on U.S. government efforts undertaken since the attacks of September 11, 2001. It will then look at how the context in which our efforts to protect and strengthen these systems has changed in the last few years, particularly with respect to changing threats and shifts in the global economic system. This analysis informs the insights and recommendations found in the concluding section of the paper.

B. Efforts to Date

Within the last decade, the United States and its key global partners have undertaken major efforts to strengthen the security of the global transportation system and supply chain. These efforts have included both legislative and policy initiatives. The section below highlights some of these key initiatives.

Legislation and Policy

In 2006, Congress passed the Security and Accountability for Every Port Act (SAFE Port Act). One provision within this law mandated that the Department of Homeland Security (DHS) develop and implement a strategic plan to enhance supply chain security. The SAFE Port Act also outlined requirements to conduct radiation detection and imaging operations at domestic ports; called for the inspection of "high-risk containers" before arrival to the United States; and established in law a voluntary public-private sector program, known as Customs-Trade Partnership Against Terrorism (C-TPAT), to strengthen and improve the security of the international supply chain.

Following the passage of the SAFE Port Act, DHS released the initial version of its strategic plan, entitled *Strategy to Enhance International Supply Chain Security*, in July 2007. The document provided a high level framework for the secure flow of cargo through various segments of the global supply chain, outlined how U.S.-led security programs are connected with other international security programs, and provided guidance for facilitating the resumption of trade after a natural disaster or terrorist incident.[1] Throughout the document, DHS emphasized the need for strong partnership among the public, private, and international sectors and communities.

The 2010 Quadrennial Homeland Security Review (QHSR) report, released in February 2010, included a strong focus on ensuring “the security and resilience of global movement systems.” The key strategic parameters in the QHSR report informed the development of the *National Strategy for Global Supply Chain Security*, which was issued in January 2012. This document emphasized the importance of international trade and delineated the U.S. government’s policy for strengthening the global supply chain. It identified the need to promote the efficient and

[1] Department of Homeland Security, “Strategy to Enhance International Supply Chain Security,” July 2007, http://www.dhs.gov/strategy-enhance-international-supply-chain-security

secure movement of goods through various transportation channels and the need to foster a resilient supply chain which can withstand and recover from natural or man-made disruptions.[2]

In March 2013, the White House issued a report examining the progress made in the first year after the release of the strategy to implement its key requirements. The update summarized the progress made by various governmental agencies and stakeholders during 2012. The document also outlined additional goals for 2013 related to understanding supply chain threats and risks; advancing technology; building resilient critical infrastructure; identifying and promoting necessary legislation; promoting the development and implementation of priority supply chain standards; improving commercial information analysis and sharing capabilities; streamlining and harmonizing processes and policies and developing customized solutions; and continuing engagement with industry partners, critical infrastructure owners and operators, and other stakeholders.[3]

Key U.S. Government Programs

Based on the previously mentioned legislative and policy initiatives, several key government programs and tools have been developed to strengthen the security of the supply chain. One of the most successful programs has been the C-TPAT program. This voluntary public-private partnership program, led by Customs and Border Protection (CBP), consists of over 10,000 certified industry stakeholders. Participants agree to provide information on international shipments so that the U.S. Government can use its risk based assessment tools to identify and inspect high-risk cargo across multiple transportation modes, facilitating the efficient movement of vetted and low-risk cargo. Another key cargo security program led by CBP is the Cargo Security Initiative, which supports the screening of cargo at major foreign ports before it is boarded on vessels bound for the United States.

From an air cargo standpoint, the U.S. Transportation Security Administration (TSA) has worked extensively since 2007 to ensure the security of cargo shipped on domestic and international inbound passenger aircraft. As required by the *Implementing Recommendations of the 9/11 Commission Act of 2007*, 100% of all cargo is now screened by regulated parties such as air carriers, indirect air carriers, and freight forwarders prior to conveyance aboard commercially operated passenger aircraft.

[2] The White House, "National Strategy for Global Supply Chain Security," January 2012, http://www.whitehouse.gov/the-press-office/2013/03/05/one-year-update-implementation-national-strategy-global-supply-chain-sec

[3] The White House, "National Strategy for Global Supply Chain Security Implementation Update," January 2013, http://www.whitehouse.gov/the-press-office/2013/03/05/one-year-update-implementation-national-strategy-global-supply-chain-sec

A key program that was developed to improve air cargo security in response to recent terrorist plots is the Air Cargo Advance Screening (ACAS) pilot, a collaborative project between TSA and CBP that utilizes many of the targeting tools that CBP has developed for maritime cargo to enhance risk-based screening of air cargo.[4]

Key International and Multilateral Efforts

In addition to its work with domestic industry stakeholders, CBP has also partnered with international trade groups such as the World Customs Organization (WCO) to promote common security standards throughout the global supply chain. Since WCO members support 99% of all international trade, the organization serves as an ideal platform for such an effort. As noted in their Framework For Standards, the WCO aims to establish standards that provide supply chain security and facilitation at a global level to promote certainty and predictability; enable integrated supply chain management for all modes of transport; enhance the role, functions and capabilities of Customs to meet the challenges and opportunities of the 21st Century; strengthen co-operation between Customs administrations to improve their capability to detect high-risk consignments; strengthen Customs/Business co-operation; and promote the seamless movement of goods through secure international trade supply chains.[5]

Public and Private Sector Cooperation

As emphasized in legislation, policy statements, and agency documents, public-private cooperation is imperative for securing the supply chain. This naturally derives from the fact that private industry owns a preponderance of the infrastructure and assets used to convey goods from their point of origin to their final destinations. To date, progress on securing the global supply chain owes much of its success to the active public-private partnership between the U.S. Government and private industry stakeholders.

C. Looking Ahead: Evolving Threats and Systemic Changes

Over the past ten years, the global transportation system and supply chain has evolved to become increasingly complex and interdependent, making the system more vulnerable to disruptive attacks. However, these growing vulnerabilities have been partially mitigated by the progress that has been made to improve the security and resilience of these systems, due to the initiatives described in the previous section and many others.

[4] Program described in this report: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/cargo_control/acas_psplan.ctt/acas_psplan.pdf

[5] World Customs Organization, “WCO SAFE Framework of Standards,” June 2007, http://www.cbp.gov/linkhandler/cgov/border_security/international_operations/international_agreements/wco/wco_framework.ctt/wco_framework.pdf

Assets within the global transportation system and supply chain remain attractive targets to terrorist groups and other adversaries, due in part to the probable direct and indirect economic impacts of attacks carried out against these systems. In the past five years there have been a succession of plots targeting all modes of transportation, including the two al Qaeda in the Arabian Peninsula-led plots in December 2009 (targeting commercial aviation) and October 2010 (targeting air cargo). More recently, in April 2013, Canadian intelligence and law enforcement officials disrupted an al Qaeda-linked plot to target a passenger rail train traveling between Toronto and New York City - a plot that echoed an aspirational plot described by Osama bin Laden in one of the documents found at the Abbottabad compound where he was hiding and ultimately killed.

These recent plots and many others make it clear that terrorist groups will likely continue to try to target the global transportation system and supply chain, and the more sophisticated groups will likely develop novel tactics for carrying out such attacks. One area of particular concern in this regard is the threat of cyber attacks against the transportation system and the global supply chain. To the extent that these systems rely on the Internet and other communications platforms for their operations, they are vulnerable to attacks that could degrade and disrupt their performance, potentially causing significant economic impacts. Given this reality, and the fact that cyber attacks can be carried out in one's home country, but against a target anywhere, without the need for international travel, it is possible that cyber attack tools will become increasingly attractive to terrorist groups and other non-state actors in support of their objectives. Notably, in April 2012 the then-intelligence chief of U.S. Cyber Command noted that terrorist groups including al Qaeda were becoming increasingly interested in developing cyber attack capabilities.[6]

In addition to these changes to the threat, there are a number of broader factors that are changing the general context for transportation and supply chain security. For example, international shipping lines are likely to change significantly in the next few years following the widening of the Panama Canal and the gradual opening of sea lanes in the Arctic Ocean. Commodity trade flows, particularly with respect to the energy sector, are shifting rapidly following the development of new energy sources in the United States and Canada. International travel patterns continue to shift, with increases in travel to the United States coming from countries in Latin America and the Middle East. These broader shifts create the need to reassess and reallocate existing programs and how resources are deployed within them.

[6] Bloomberg News, "Al-Qaeda Seeks Cyber Attack Skills, U.S. Official Says," April 25, 2012. http://www.businessweek.com/news/2012-04-25/al-qaeda-seeks-cyber-attack-skills-u-dot-s-dot-official-says

These changes in the threat and in the broader context for the global transportation system and supply chain create two high-level strategic imperatives for senior leaders in the public and private sector. First, senior leaders need to review existing programs and activities to see whether they are still effective and relevant, and make changes to such programs as needed, including both policy changes and the reprioritizing of operational assets. Second, leaders need to determine whether any new programs or activities are needed to address gaps not otherwise covered by existing programs.

D. Implications and Recommendations

Neither the U.S. government nor the private sector can afford to stand still with respect to transportation and supply chain security, given the dynamic nature of the threat to these systems and the other external factors. In order to continue to build on the good work that has been done in the past decade, the key stakeholders should consider the following recommendations:

Recommendation #1. The U.S. government should recommit to a robust implementation of the National Strategy for Global Supply Chain Security.

The one-year implementation plan for the strategy, released in March 2013, describes the various action items that have been taken in the past year to implement key elements of the strategy. Overall, the report indicates that good progress has been made to implement the key imperatives of the strategy. However, as with any such strategic effort, there are risks that the implementation of this strategy will lose momentum in the absence of sustained senior leadership attention. The White House and the lead agencies defined in the strategy need to maintain focus on these issues, and Congress should push for detailed information on its implementation, including requesting implementation metrics and other relevant quantifiable information.

Recommendation #2. Reevaluate and prioritize current programs and activities to ensure that they are appropriately aligned on current threats and adaptable for future threats. In the twelve years since 9/11 dozens of new measures and capabilities have been added to the U.S. government's transportation security and supply chain security regimes: new screening technologies, training programs, information-sharing systems, overseas capacity building programs, etc. All of these activities are worthy of ongoing risk-based reviews and updates based on changes to threats and to other external conditions.

Such reviews should be conducted on a cross-component basis within DHS and with key partner agencies (e.g. Federal Aviation Administration, Federal Bureau of Investigation, Department of State) in order to identify potential savings and synergies. This review could perhaps take place within the context of the 2013 Quadrennial Homeland Security Review.

For example, one issue that could be examined more closely and clarified is the respective roles and responsibilities of TSA and CBP in securing inbound cargo. While TSA is responsible for reviewing passenger information on all commercial aircraft and securing air cargo before its arrival in the U.S., CBP is responsible for collecting manifest data on air cargo shipments and has the authority to inspect cargo upon its arrival. TSA and CBP have made progress in the last several years to improve cooperation in the context of the Air Cargo Advance Screening pilot, but they could collaborate more closely in a way that would improve mission efficiency and deliver cost savings.

Recommendation #3. Issue public version of supply chain threat assessment for industry awareness purposes.

The one-year implementation report for the 2012 National Strategy for Global Supply Chain Security notes that the National Intelligence Council completed an assessment in December 2012 of threats to the global supply chain system. To the extent possible and consistent with the protection of classified sources, the U.S. intelligence community should release a public version of this report to better inform private sector stakeholders about the threats that they face with respect to their assets and roles in the global transportation system and supply chain.

Recommendation #4. Promote and improve the free flow of data and information across all relevant government agencies and internationally.

U.S. government agencies are reliant on the sharing of information by key foreign partners to facilitate the movement and screening of passengers and cargo. Since 2007, the United States and the European Union (EU) have gradually established a legal framework for carriers operating between the United States and the EU to exchange and transfer Passenger Name Records. After years of negotiation, the U.S.-EU Agreement on Passenger Name Records was renewed and put into effect in April 2012. This agreement will help to prevent, detect, investigate and prosecute terrorist offenses and related crimes as well as other serious cross-border crimes.[7]

Efforts to improve the sharing and exchange of cargo-related data information are underway within the U.S. government, including at DHS and the National Maritime Intelligence Integration Office. These activities can be enhanced by a comprehensive data-driven program that leverages historical shipping information, government certification and intelligence reporting that would help relevant agencies to make informed decisions and determine the appropriate level of screening for inbound cargo shipments and for passengers.

[7] The Council of the European Union, "Council adopts new EU-US agreement on Passenger Name Records (PNR)," (Luxembourg, 2012), http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/129806.pdf (accessed on October 30, 2012).

Recommendation #5. Existing public-private partnerships should be renewed and strengthened.

Much of the global supply chain is owned and operated by a variety of public and private sector organizations. Therefore, success will be dependent on communication, collaboration and the ability to work together to include redefining relationships, roles and responsibilities with the public and private partnerships. Utilizing a multi-layered stakeholder engagement strategy is a critical success factor for the implementation of global supply chain risk management methods. In order to achieve optimal risk-based security and the efficient movement of goods and persons within the global supply chain, continued cooperation between US government agencies (e.g. CBP, TSA, Department of State) and their counterpart agencies in other countries, international organizations (e.g. International Civil Aviation Organization and WCO) and industry partners (such as C-TPAT) is essential. This can be accomplished through synchronizing policy and standards, aligning activities to address the highest risks first and leveraging resources.

Recommendation #6. The US government should deepen its engagement with key international partners on meeting these threats.

The U.S. Government should continue to harmonize security efforts with international and industry partners where feasible as a vital step in securing the global supply chain. Currently, the U.S. Government has achieved some degree of harmonization of screening policies and regulations with the EU, Canada and various major trading partners in aviation security.[8] The U.S. has also aligned maritime-related security rules and policies with WCO.[9] Such cooperation between international trading partners can help authorities to more closely track international cargo through the supply chain. Consideration should be given to expanding the scope of cargo screening programs to include postal, commercial shipping, and international trading partners.

Recommendation #7. The US government should look more closely at the relationship between current and future cyber threats vis-a-vis transportation and supply chain security and resilience.

As noted earlier, it is likely that cyber attacks and disruptions will pose an increasing threat to the global transportation and supply chain systems in the years ahead. As these systems become increasingly connected to the Internet, there will be new opportunities for malicious action that will need to be carefully mitigated against, not just after the fact but during the development of

[8] Department of Homeland Security, "International Activities: Aviation Security," http://www.dhs.gov/international-activities#0 (accessed on October 17, 2012).

[9] Department of Homeland Security, "DHS Announces Partnership with WCO to Strengthen the Security and Resiliency of the Global Supply Chain," http://www.dhs.gov/news/2011/01/06/dhs-announces-partnership-wco-strengthen-security-and-resiliency-global-supply-chain (accessed on October 17, 2012).

new system capabilities. DHS should strengthen its capabilities for analysis of these issues, bringing together subject matter experts from CBP, TSA and the Coast Guard with cyber experts to assess threats and risks. As part of this analytic effort, the Department should carry out red-teaming activities with respect to future transportation and supply chain risks. It should also develop products for key private sector stakeholders about these threats and what can be done to mitigate current and future vulnerabilities.