NETWORK-CENTRIC SECURITY FOR CANADA-U.S. SUPPLY CHAINS

Author
Joel Webber

Published jointly with The Fraser Institute,
Vancouver, British Columbia

May 2005

About CSIS

The Center for Strategic and International Studies (CSIS) is a nonprofit, bipartisan public policy organization established in 1962 to provide strategic insights and practical policy solutions to decisionmakers concerned with global security. Over the years, it has grown to be one of the largest organizations of its kind, with a staff of some 200 employees, including more than 120 analysts working to address the changing dynamics of international security across the globe.

CSIS is organized around three broad program areas, which together enable it to offer truly integrated insights and solutions to the challenges of global security. First, CSIS addresses the new drivers of global security, with programs on the international financial and economic system, foreign assistance, energy security, technology, biotechnology, demographic change, the HIV/AIDS pandemic, and governance. Second, CSIS also possesses one of America's most comprehensive programs on U.S. and international security, proposing reforms to U.S. defense organization, policy, force structure, and its industrial and technology base and offering solutions to the challenges of proliferation, transnational terrorism, homeland security, and post-conflict reconstruction. Third, CSIS is the only institution of its kind with resident experts on all the world's major populated geographic regions.

CSIS was founded four decades ago by David M. Abshire and Admiral Arleigh Burke. Former U.S. senator Sam Nunn became chairman of the CSIS Board of Trustees in 1999, and since April 2000, John J. Hamre has led CSIS as president and chief executive officer. Headquartered in downtown Washington, D.C., CSIS is a private, tax-exempt, 501(c) 3 institution. CSIS does not take specific policy positions; accordingly, all views expressed herein should be understood to be solely those of the author(s).

About the Fraser Institute

The Fraser Institute is an independent Canadian economic and social research and educational organization. It has as its objective the redirection of public attention to the role of competitive markets in providing for the well-being of Canadians. Where markets work, the Institute's interest lies in trying to discover prospects for improvement. Where markets do not work, its interest lies in finding the reasons. Where competitive markets have been replaced by government control, the interest of the Institute lies in documenting objectively the nature of the improvement or deterioration resulting from government intervention. The work of the Institute is assisted by an Editorial Advisory Board of internationally renowned economists. The Fraser Institute is a national, federally chartered nonprofit organization financed by the sale of its publications and the tax-deductible contributions of its supporters.

Center for Strategic and International Studies
1800 K Street, N.W.
Washington, D.C. 20006
Tel: (202) 887-0200
Fax: (202) 775-3199
Web: www.csis.org/

The Fraser Institute
1770 Burrard Street
Vancouver, B.C. V6J 3G7
Tel: (604) 688-0221
Fax: (604) 688-8539
Web: www.fraserinstitute.ca/

Contents

Foreword

The container is the potential Trojan horse of the 21st Century…. A terrorist attack using a container to conceal a so-called RDD—or "dirty bomb"—could potentially stop global trade in its tracks, unless we have a maritime security system that can detect and deter such an attack…. The threat of a terrorist attack using a cargo container is not just an academic one.—Robert Bonner, Commissioner, U.S. Customs and Border Protection[1]

Manufacturing today is conducted through a complex network of firms that produce and assemble components into finished products. The links between firms in manufacturing networks form supply chains. The science of logistics, aided by the application of advanced information technologies, has permitted these networks to increase output and lower costs by virtually eliminating inventories of components waiting for assembly and inventories of finished products waiting for shipment to retailers or consumers. Taut supply chains are one reason for the remarkable productivity improvements, and corresponding economic growth, experienced in North America and, to a lesser extent, in Europe and Asia.

Yet, this shift to networked manufacturing has come with new risks. When whole networks of firms are dependent on just-in-time deliveries, even brief disruptions to shipping schedules can be costly. This was vividly demonstrated when traffic back-ups at U.S.-Canada border crossings on September 11, 2001, forced plant closures across Ontario and the midwestern United States.

Some of the most forward-looking firms recognize this problem and are lobbying for government action. John Meredith is group managing director of Hong Kong-based Hutchinson Port Holdings (HPH), the world's largest port operator, with 44 facilities in 17 countries. Although it has no U.S. operations, 40 percent of containers entering the United States pass through an HPH facility.

"Millions and millions of products are flowing into (the United States) and no one at the moment is tracing where they came from and tracing how they got there," Meredith said in a recent interview.[2] "And that is the Trojan horse," Meredith added, using the same phrase as Commissioner Bonner. "We would like to offer our services, our systems [to enhance security]. Just tell us what needs to be in place. We can't do it ourselves."

Joel Webber's innovative paper offers an important answer to Meredith's plea. Webber shows a way for business to tell government what to do, or rather, to work with government to dramatically broaden and deepen supply chain security. Though Webber focuses on the world's longest undefended border, between Canada and the United States, his design has the capacity to grow globally.

Webber's approach combines three key ideas:

- Network-centric security, instead of today's stop-and-search security.

- Pooling supply chain and security expertise in a private/public sector consortium, instead of having government officials impose a plan.
- Employing commercial and security incentives to create compliance, rather than compulsion.

Network-Centric Security

Webber shows how existing technology could transform the information-poor supply chain into an information-rich environment. Network-centric security would pool information from all participants in the supply chain, from port operators to shippers to receivers. Using computer and satellite tracking capabilities, the system would follow each box from its loading to delivery. It would provide thick information including: where and how the box was loaded, by whom and the level of trust/security the loader commands, what's in the box, where the box is/has been/will be, whether the box has been tampered with, its velocity, hazards along the way, advance notice to authorities and other shipping modes of arrival, etc. In fact, Webber shows how supply chain leaders are already doing this through their own proprietary systems.

The architecture of this information infrastructure would allow companies in all aspects of the supply chain to feed information into the system and pull out the information they had legal access to, whether their own information or information partners permitted them to share. A company plugged into a network-centric supply system would have secure access through the system to thick information on its own shipment movements but would not have access to another company's movements. (This is similar to how banks have access to the information on their transactions through the interactive system but not to other bank's transactions.) The interactive system would provide both the information security and thick information required for functionality, for example knowing in an instant how much can be removed from an individual's account a continent or more away.

In a network-centric supply chain security system, appropriate government security agencies with high security clearances would have access to thick information on the system but would be under the compulsion of criminal law to maintain the confidentiality of this information. They would be able to view the whole system in the way security officials can now view the entire air traffic system and make appropriate security determinations.

Such a network-centric system would dramatically lessen risks, both through direct security measures and indirectly by increasing information and thus, providing a forensic trail for suspicious activities or apprehended threats that today generate little information. In the event of an attack, it would also provide key information to isolate the problem and limit the shutdown. In fact, the Customs-Trade Partnership against Terrorism (C-TPAT) is using a very similar model of voluntary compliance.

Private/Public Approach

But this must be a business-friendly system. Webber notes that for the most part, government security experts and supply chain experts live in different silos. A pure government mandate would likely be costly, inefficient, and inflexible as has too often been the case in the past. Webber's second key innovation shows how the private sector can lead, working with government, though a joint consortium that potentially could have similarities to the International Standards Organization (ISO) model.

Businesses, especially competing businesses, have found ways to work together to develop standards in areas from computing to television. Developing standards and implementation strategies would be a key task of the new security consortium though direct government involvement would be a necessity. The consortium would also manage company and agency membership in the system.

Webber's proposal would build on the expertise of supply chain leaders, develop common standards across supply chain actors, and give them the capacity to hook into the system, just as a small local bank can become part of the worldwide interactive banking system by buying the appropriate technology and implementing standardized security measures to protect the valuable information that flows over the system.

Developing such a system has many challenges, most notably how to pool information available from many actors across differing systems and then make this information available to only authorized company officials and security personnel. These types of challenges have been met many times before, for example in the interactive network mentioned above. It might seem that supply chain leaders would not wish to lend their expertise and participate and would rather stick to their proprietary systems. But, more than anyone else, the best and most successful supply chain companies have incentives to keep the chain safe and operational. Meredith has repeatedly offered to share HPH's top-notch security and tracking systems to help government improve security.

Developing an Incentive Structure

The network-centric system Webber envisions obviously makes economic sense, otherwise, supply chain leaders would not have already moved in that direction. Yet, aside from these leaders, the world's supply chain remains quite primitive in many ways. For example, just-in-time-delivery systems function effectively only within regional blocks, like North America, but not on a world basis. As noted, information is notoriously thin for containers on the move. Ironically, this weakness provides an opportunity to improve supply chain security.

A network-centric approach offers new efficiencies in the global shipment of goods. Commercial (and security) advantages include the following information: (1) that the supplies actually exist and are in the chain; (2) where they are; (3) their current and future velocity; (4) when they will arrive; (5) hazards along the way (and how to handle the hazards in advance); (6) advance notice to participants in the supply chain for smooth transfer; (7) advance notice and

predictability, essential for just-in-time systems, to the ultimate receiver, reducing liability; and (8) other insurance-related costs, etc. Potentially even more important is the information provided when things go wrong. Moreover, just as International Organization for Standardization (ISO) tells customers that even a small company has world-class standards, so to would membership in this system assure potential customers of a company's supply chain capabilities. This is important for companies that manage their own shipping.

The commercial incentives could be strong, especially for small and medium enterprises (SMEs) which would be able to achieve the functionality of a Wal-Mart or a FedEx logistical system without creating or buying such a system. The advantages could be immense in an era of inventory control and security of supply concerns. One key is that the system be scaled to include all size companies. This is possible. For example, even the smallest bank can join one of the ATM networks. Because of the commercial advantages, government does not need to compel small banks to join.

Webber also proposes government-based incentives including: facilitated cargo clearance; reduced costs, with those inside and outside the system charged the costs of customs security (obviously higher for those outside the system); and possibly reduced legal liability and insurance costs. Some companies in the supply chain may remain outside the system and they will continue to be monitored by current security methods. But, at first glance, the incentives appear persuasive over the long term.

The supply chains that span the U.S.-Canada border are unique in the global context. They are heavily reliant on land transportation that travels primarily through just a handful of key border crossings. Major shipments are routinely timed for delivery within hours, and sometimes to the minute. Taken together, these shipments comprise the largest bilateral trading relationship, measured by volume or value, between any two countries on Earth throughout recorded history.

Adapting the most advanced twenty-first century trade relationship to cope with the most perilous of twenty-first century risks will require the innovative application of more than technology. It will call on the creative ideas of many. Joel Webber begins an important debate with this paper and gives us great encouragement that the outcome of this debate will surely be a continuation and even expansion of free and secure trade for decades to come.

Illustrating the timeliness of this proposal, in December 2004, the U.S. commissioner of customs and border protection (CBP), Robert Bonner, proposed that CBP reward deployment of so-called "smart container" technology—along with a shipper's or carrier's good standing in C-TPAT and use of Container Security Initiative ports—with "green lane" expedited passage through customs.[3] The "smart container" concept overlaps with what this study calls a "network-centric" approach to freight security.

The Fraser Institute and the Center for Strategic and International Studies are pleased to bring Webber's analysis to a wide readership in both our countries. On

behalf of our institutions, we would like to thank the author for bringing his work to us and for enduring the too-often glacial pace of publication. We are also grateful to Andre Belelieu at the Center for Strategic and International Studies, former Ambassador Martin Collacott, and anonymous reviewers at the Fraser Institute for their thoughtful comments on various drafts and for their help in editing and publishing this paper.

Fred McMahon
Director, Centre for Globalization Studies
The Fraser Institute

Christopher Sands
Senior Associate, Canada Project
Center for Strategic and International Studies

[1] Robert C. Bonner, "Remarks by Robert C. Bonner" (speech, 5th Annual CBP-Trade Symposium, Washington, DC, January 13, 2005).
[2] John Meredith, interviewed by CNN Presents, *CNN Presents*, CNN, September 19, 2004.
[3] Robert C. Bonner, "Remarks by Commissioner Robert C. Bonner" (speech, Trade Support Network meeting, Manhattan Beach, CA, February 1, 2005).

Network-Centric Security for Canada-U.S. Supply Chains

Joel Webber

Executive Summary

Desmond Morton writes that post–September 11 civilization faces a "war without fronts."[1] All core economic and social infrastructures are potential targets. This paper asks how to protect one of those infrastructures—the supply chain—from asymmetric attack. Moreover, the supply chain, just like air transportation, can provide weapon delivery vehicles directly to populated areas and sensitive targets. This paper focuses where international cargo flows are among the world's largest in volume and economic significance: the Canada-U.S. border. Success here should offer lessons applicable worldwide.

In this new conflict, the logistics system poses a special attraction for terrorists. First, the large spaces within sea containers or truck vans can conceal, and then deliver for detonation at a targeted location, weapons commensurate with their great size.

Second, in addition to substantial loss of life and property at the targeted location, such an attack would present governments with only two alternatives, each of which is unthinkable: Governments could stop cargo flows for the days, weeks, or longer required to ascertain the attacks' source. Or governments could avoid economic disruption by letting cargoes continue to move but at the price of further risks to life and property that we have no way of measuring.

For the next stage of post–September 11 supply chain security, Canada and the United States can better protect their mutual freight flows against terrorist penetration by engaging the logistics system on its own operational terms, thereby keeping it moving while also making it safe. A network-centric approach would match real-time data flows with cargo that is constantly moving through numerous hands and dispersed geographically across the globe.[2]

Today's stop-and-search protocol relies on interruption of logistics movements to secure them from terror. Therefore, we should augment (not replace) manual searches and machine scans at ports and border checkpoints, which are today's main source of direct observation of freight flows. Using

wireless devices, electronic seals, sensors, and logistics software already available, a network-centric protocol would report on cargoes for possible asymmetric interference in real time, at multiple times, and at any location chosen.

To that end, this paper offers a network-centric security protocol to augment the existing one and then outlines how Canada and the United States can bring this about.

At its core, this network-centric approach to supply chain security makes terrorist penetration materially more difficult by rendering the supply chain visible—remotely and in real time—to those who can protect against such penetration.

This proposed shift away from interrupting the supply chain in order to observe it at limited places and times and toward continuous and remote observation, would yield two benefits:

- By keeping cargoes moving, it would impede tamper and benefit commerce. "Freight at rest is freight at risk."[3] Continuity of movement reduces opportunity for terrorist interference. From a commercial standpoint as well, such continuity in freight movement is optimal, while stoppage or slowdown is problematic.
- It would reallocate security responsibility to those better able to shoulder it: the businesses that ship, carry, and import cargoes.

In terms of policy, Canada and the United States could implement a network-centric logistics security protocol by reallocating the current distribution of security responsibilities among public and private participants, retaining responsibility for policy and intervention with government, while enlisting private owners and operators as both the prime players in their perimeter security and the main source of data gathering on the security statuses of their own supply chains.

The how-to question goes largely to operational detail—data network construction that corresponds to the scattered and constantly moving physical network comprising the supply chain. But more subtle—and benefiting from less precedent—are questions of standards selection, auditing and enforcement, and the structuring of incentives to motivate serious effort and investment from the firms whose cooperation is critical to this approach.

As for these questions, there is a constant reality; most logistics infrastructure is privately owned and operated. The business world, not government, is where most of the relevant expertise resides and where most of the operational work is done. This should guide us as to the standards, audit, and operations questions.

As for incentives, only individual firms can decide which inducements will yield positive return-on-investment calculations. As a working hypothesis, this paper suggests expedited port and border clearance, tax benefits, and liability protections as good first moves toward a robust incentive structure. Ultimately, however, each firm determines its own return on investment, and therein lies the answer as to which incentives will be effective and which will not.

As for operational responsibilities, much of the detection and prevention—though none of interdiction and actual confrontation of terrorists—would lie with the private firms that own and operate the lion's share of the logistics system.

When fully implemented, the system would look much as it does today. This network-centric approach would complement (but not replace) the existing freight security protocol developed after September 11. First, strengthened staffing and added Vehicle and Cargo Inspection System (VACIS) units and other equipment at ports and border checkpoints would continue. Second, "layering" techniques—advance manifest data, driver background profiles, etc.—would continue to enhance and inform searches and scans. Third, the network-centric approach would solely address data flow and anomaly detection. Confronting and interdicting terrorists would remain the task of government (not private) parties.

On the other hand, there would be important differences. First, supply chains validated under the network-centric protocol would typically be expedited through ports and borders (i.e., without interruption). Agents would have the discretion to stop loads for any reason, but the default mode for qualified supply chains would be freedom from stops for search, scan, or paperwork.

Second, the role of private firms in securing freight against terror would become much more consequential due to better tools and new accountability. Businesses that ship, carry, or receive goods would commit operations and IT personnel. The necessary hardware, software, and systems integration would appear as noticeable sums on their income statements.

Immediately, this proposal brings up the question of feasibility and whether or not the danger merits such an effort. The electronic connectivity required would involve technological retrofitting and information integration in a logistics system that, with the exception of particular logistics leaders, is notoriously fragmented and manual. It would also involve government agencies ceding to private firms tasks directly related to homeland security, notably the ascertainment of what is in the cargo container to begin with, while firms would routinely disclose to government data they would otherwise consider proprietary.

The answer to the feasibility question lies in the novelty and pervasiveness of the post–September 11 asymmetric threat. As radical as this network-centric proposal may seem, its feasibility should be considered in the context of the threat's character—a "war without fronts." For freight flows, this impacts a logistics infrastructure made up of private property much more than of government-run port and border checkpoints or other infrastructure.

It is the unprecedented stealth and lethality of the new threat that thrusts private firms into a security role in protecting their own infrastructure and operations.

Finally, a network-centric approach denotes a basis for integrating the various institutions, individuals, tools, and related techniques already assembled for post–September 11 supply chain security—it is not a substitute for them. This integration will include:

- Perimeter and related physical security;

- IT integrity and cyber risks;
- Employee and visitor access controls;
- Potential compromise of raw materials, packaging, and products;
- Background checks on drivers and all other employees with access; and
- Organizational connections to police, fire, and other first responders, as well as to all pertinent national security and border agencies.

Nevertheless, not integrating these separate measures: the geographic dispersal, numerous handlers, and constant movement inherent in the logistics network, will continue to severely limit their collective impact. Electronic connectivity can, in real time and without stopping cargo movement, combine the above measures into a coherent response. In this way, we can protect freight flows without having to interrupt them.

The Network-Centric Protocol

The network-centric approach to freight security—or "smart container" applications as they are called in certain Canada Border Services Agency (CBSA) and U.S. Customs and Border Protection (CBP) circles—begins with a reallocation of responsibility between government and the private sector as much as it does with the technological retrofitting of the logistics system. Its core tactic is to augment current reliance on direct observation of freight, when such freight is present at ports and border checkpoints, with the remote monitoring of supply chain conditions at all times and places at which shippers, carriers, or government security personnel might wish information about them.[4]

To continue primary reliance on a security protocol so limited in time and place excludes direct observation at noncheckpoint and nonport locations. It is similarly restricted to those timeframes when such cargoes are present at those locations. For a logistics system that is most productive (and least vulnerable to interference) when it is on the move, the current protocol is inherently self-defeating.

Augmenting this stop-and-search protocol with one based on remote observation of freight—real time via electronic applications—would require wireless devices, electronic seals, sensors, and software platforms that have been available for many years but are still in early stages of commercial adoption.[5] Such a protocol would capture, transmit, collect, and analyze specified data categories for cargo at various times while en route. Systems integration and actual deployment of existing applications to capture specified data sets has already been successful in multiple past and ongoing government pilot programs.

But despite trials and experimentation, a network-centric protocol for cargo security is not the policy of either Canada or the United States. What strategic form such a policy might take in either country is still a matter of ongoing development and debate.

Canada and the United States pursued tactical cooperation within minutes after the September 11 attacks. Monthly cabinet-level meetings have implemented an action agenda at our mutual border, in Canadian and U.S. seaports and airports, and in customs, intelligence, and defense agencies in both Ottawa and Washington.

The network-centric protocol for which this paper argues offers a basis for strategy. This new protocol would supplement (not replace) existing port and border checkpoint searches and scans with several broad implications. First, no more than 6–7 percent of entering containers—and similar percentages of trucks, railcars, and air cargo unit load devices—would be subject to search or scan.[6] By certifying qualifying supply chains this way, Canada and the United States would free more search-and-scan resources for cargoes that had not been validated under the electronic chain-of-custody protocol.

Second, a key incentive to this new protocol's private adoption would consist of expedited treatment at ports and borders, with the goal of eliminating stops for customs and other regulatory purposes. By qualifying supply chains (via the carriers and shippers that manage them), rather than placing primary operational reliance on the stop-and-search techniques of CBSA and CBP, Canada and the United States would enlist the managements of those leading firms whose port and cross-border trade make up our international commerce. It would then use digital technology to provide more thorough security, as well as faster throughput.

Third, this would do more than simply harden a category of presently soft targets against their use to destroy Canadian and American life and property. Deployment of this network-centric protocol would enable a forensic capability to better identify those supply chains that are relatively safe, versus those that continue to be questionable following a terrorist attack. Ironically, it is our lack of what CBP commissioner Robert Bonner has called a "continuity of trade contingency plan" that creates further incentive for a terrorist attack on our two economies in the first place.

Finally, we will look at some of the leading objections to the new framework. In addition to stressing the magnitude of implementation, these objections tend to emphasize the impediment that the logistics system's fragmentation presents to successful integration. The argument for a network-centric protocol does not rest on minimizing this fragmentation. Indeed, it is just this geographic dispersal, 24/7 operation, and multitude of participants that offer such an attractive target for asymmetric penetration by terrorists. In short, such fragmentation itself argues for deployment of a network-centric protocol.

Finally, this section concludes with a statement of concept by an official of Transport Canada that succinctly sketches the vision for a network-centric protocol.

Reallocating Responsibilities

In the early aftermath of the September 11 attacks, Canada and the United States lacked the luxuries of lead time and deliberation. Within hours, Customs and

Revenue Canada (now part of CBSA) and the U.S. Customs Service (now U.S. CBP, a part of the U.S. Department of Homeland Security established in 2002)—buttressed respectively by the Royal Canadian Mounted Police (RCMP), the Immigration and Naturalization Service (INS), and other agencies—used stop-and-search techniques that until then had been deployed mostly against smuggling and narcotics trafficking.

Terrorist detection was not unknown—witness the dramatic U.S. Customs interdiction of Ahmed Ressam during his attempted Victoria, British Columbia/Port Angeles, Washington crossing on December 14, 1999. But this detection was not as yet the priority of port and border agencies that it has become since September 11. Also, as in the Ahmed Ressam incident, detection and interdiction depended on extraordinary personal performance of the sort Diana Dean (the U.S. Customs agent involved) demonstrated in that incident.

From the first minutes after the towers were hit, with U.S. Customs' declaration of "Level 1" alert status and comparable Canadian action, both governments demanded and received maximum opportunity for direct observation of any container, truck, or object crossing their mutual border or entering their respective ports. For three days, the border came to a virtual, if not an official, halt as agents used existing search-and-scan techniques against potential terrorist penetration of cargo flows.

In the following months, these measures for the direct observation of freight loads and equipment were augmented by enhanced staffing, added VACIS and other scanning equipment, and advanced screening at offshore embarkation ports outside North America (a program announced by CBP commissioner Robert Bonner within months of the attacks for "pushing the borders out" from North America—it was later incorporated into the Container Security Initiative).

Three years later, Canada and the United States should ask if they could improve on the array of people, assets, and organizations protecting their mutual trade flows.

In view of the developments recited above, the direct observation of freight loads to detect indications of tamper or other interference was assigned mainly to Customs and Revenue Canada and U.S. Customs. (There have been noteworthy but minor exceptions in airfreight—applications of the "known shipper rule" for belly-hold cargo and self-inspection of dedicated air cargo freighters.)

But even with those limited air cargo exceptions, present rules and protocols give government the job of direct observation of all marine, rail, intermodal, and truck cargoes since September 11. Indeed, even shippers and carriers qualifying for the Customs-Trade Partnership Against Terrorism (C-TPAT) and the Partners in Protection (PIP) programs—despite collaboration in their supply chain practices with Canadian and U.S. agencies—enjoy no formal, stated, and measurable reduction in scrutiny from searches and scans. CBSA and CBP do, however, offer unspecified expedited treatment to PIP and C-TPAT members, but neither Ottawa's CBSA nor Washington's CBP confirms exactly what this means or how it is manifested in practical terms. Finally, the Free and Secure Trade

(FAST) program, as a matter of fact, does afford expedited treatment for qualifying truck operations whose terms are definite and whose operational impacts can be measured—but this covers only a limited percentage of freight flowing between Canada and the United States.[7]

In light of this, it is clear the allocation of responsibility is weighted to the public sector, with a secondary role assigned to private business. The commercial sector's role takes the form of various information disclosures to support the "layering" strategy enunciated by the two governments in order to take advantage of the offer of voluntary participation in cooperative programs like C-TPAT, PIP, and FAST.

As a result, the stop-and-search methods that comprise the primary method of direct observation of freight flows for security purposes are targeted largely by the information disclosures under the heading of "layering." From 2002 onward, the governments added the following to supplement their own intelligence-gathering activities to further refine where the search-and-scan resources at ports and borders will be used:

- Transmission of specified manifest information at lead times set by regulation (along with special information filings relating to food, pharmaceuticals, and HAZMAT),
- New registration of truck drivers and others accompanying freight across borders, and
- A miscellany of informational requirements peculiar to certain modes (for instance, "known shipper" rule in air cargo for below deck on passenger aircraft).

The network-centric approach would afford a more balanced allocation of public-sector and private-sector responsibility. It would not diminish the information disclosure adopted to date, but note that such disclosure is not the same as direct observation.

Notably, the advance manifest listing of freight contents simply reflects someone's representation and is not verified unless the freight itself is searched or scanned.

The network-centric approach would ultimately reallocate responsibility from the public to the private sector to reduce the existing burden on the party whose contact with the freight load is relatively brief and episodic (i.e., government). The validated word of the business stuffing the container or packing the truck trailer—confirmed via electronic confirmation that such container or packing had not been tampered with en route—would replace the stop-and-search process at ports and borders in validated supply chains.

Correspondingly, this would assign to private participants measurable responsibilities—in data gathering and related security functions—rather than mere regulatory compliance and possible voluntary adherence to C-TPAT or PIP (FAST, in fact, has objective standards, conformity to which is the condition of expedited border treatment for truck operations that qualify).[8]

First, terrorist intervention such as we saw on September 11, unlike invading military forces or local criminals, integrates itself into the fabric of civilian operations. Unlike more traditional attacks, it can come from within those operations or attack isolated segments of such operations from the outside. Either way, the asymmetric threat consists in its stealth, and thereby places a premium on intimate knowledge of those private freight operations.

In seeking to identify hidden dangers among cargoes or related infrastructure, it makes little sense to assign primary duty to a party whose contact with the container, truck, aircraft ULD, or rail car is fleeting and episodic. Granted, private shippers' and carriers' contacts with and control of their loads are imperfect—in large part because they are fragmented—but they are closer and more sustained than that of any government agency.

Canada and the United States could make better use of the capabilities inherent in the very logistics system they seek to secure by shifting more of the work of detection and prevention to those private firms that manufacture goods for shipping, run carrier operations, or receive goods for onward distribution or final use.

Some will object that substantial, tangible nongovernmental responsibility will raise concerns of trustworthiness in a homeland security setting and that this proposal would embody a radical departure from the national security role traditionally assigned to government. As to the first, our governments have long vetted and validated firms through security clearances and related processes in defense contracting and other security-sensitive roles. As to the second, such shifting of security accountabilities to private parties is a necessary consequence of a new enemy targeting private infrastructure rather than traditional military targets. September 11's unprecedented stealth requires a new directness is response.

Moreover, current technology makes direct observation of loads by businesses possible in ways not available when customs agencies first focused on searches as their main means of transport security.

Before the advent of wireless technology and software systems, the idea of reallocating to shippers, carriers, and recipients the duty to report direct observations about their cargoes would have required disruptive searches performed by those private businesses themselves. Once such manual steps were completed, there would be no means of detection against tampering once the cargo left a business' custody. The new technology can substitute direct observation by electronic device for direct observation by search, either manual or automated (such as by VACIS and other nondestructive inspection equipment), and continue such direction electronically once it changes hands. It would substitute an electronic chain-of-custody for physical, manual custody.[9]

Third, as the below description of the high technology sector's voluntary logistics organizations like the Technology Asset Protection Association (TAPA) and MIT/Auto ID Center (succeeded by EPCglobal) indicates, motivated businesses working together in a common supply chain can (and in the past have)

create complementary security protocols among themselves. In addition to adopting the needed software platforms and wireless technology, firms wishing to avail themselves of the incentives on offer (such as bypassing searches and paperwork, tax benefits, and liability limitations) could jointly adhere to the agreed techniques of manual perimeter security and other business processes necessary to prevent terrorists from penetrating cargo flows undetected.

While both TAPA and EPCglobal were formed for logistics goals not primarily related to post–September 11 terror concerns, they reflect the ability of the private sector to integrate logistics functions among multiple commercial parties without government supervision, funding, or standards setting.

Fourth, the relatively recent availability of direct observation via remote electronic means raises the possibility of a new, two-fold paradigm for government's role. Government would function much as a systems architect in addition to being a protector or regulator by working with logistics businesses to design the data flows, collection systems, and related analysis. More precisely, the actual specification would likely be as much or more a product of industry collaboration as government design. But government would place its imprimatur on such architecture and then make use of it in gathering data (along with private parties) in furtherance of its continued role as the chief security authority for freight flows.

Moreover, implementation of such architecture would be part and parcel of government's policy, with the related retrofitting of supply chains with necessary applications and related systems integration a condition to participating private firms enjoying any of the incentives offered.

Finally, as to the existing protocol of search and scan for direct freight observations, this would continue, albeit with resources freed up from the validation of supply chains no longer requiring such treatment. Government's conventional role as protector and regulator—as embodied in searches, scans, and other interventions with freight flows—would be enhanced by eliminating such coverage from those supply chains whose status is validated via the network-centric security protocol. None of this would reduce an agency's absolute discretion to stop any cargo.

Doing Direct Observation Remotely

A single idea underlies both the current stop-and-search system at ports and border checkpoints and the network-centric approach for which this paper argues: the primacy of direct observation.

As with the direct observation used in the present strategy, the network-centric strategy relies on a remote version of the same function. Manual searches use human senses of sight, touch, smell, and sound in the immediate presence of a cargo. Using those senses, agents inspecting loads and related infrastructure both confirm the presence of certain expected and desired indicators (e.g., an unbroken mechanical seal on a container) and are alert for indications of what should not be present (e.g., a metal box amidst a load of agricultural produce).

VACIS and related nondestructive inspection equipment make similar direct observations by substituting gamma ray, X-ray, or other technologies for human senses to scan freight and the physical assets in which it moves. Both searches and scans require the immediate presence of the load or equipment, hence the focus on ports and border checkpoints as locations.

Moreover, even automated nondestructive scanning (such as VACIS affords) is time consuming. While the time required to capture the image on the review screen is indeed short (a few seconds), the bulk of time goes to inspecting the scan image itself and interpreting its meaning. This often takes several minutes for a particular scan.

By supplementing the existing stop-and-search protocol with one that relies on remote electronic reporting, the network-centric approach would provide similarly high-reliability reports on a load's location and condition—along with supplementary data more fully detailed below.

A network-centric strategy could provide remote reporting and real-time data by providing two critical functions:

- The capability to ask a question about loads and carrying equipment within a logistics system; and
- An automated exceptions report function that notifies government and business observers of anomalies—unexpected variations from patterns that might suggest a security breach—taking place in the logistics network.

This, in turn, would require an information system framework with two critical features:

- Ongoing collection of specified data from cargo loads or the vehicles carrying them and the transmission of that data to a central software platform; and
- Ongoing access to such a central software platform by authorized firms and government agencies to provide real-time information about loads and vehicles.

Applications Required

Achieving these functions would require the following types of applications:

- A central logistics-management software system capable of gathering track and trace data from wireless devices (typically satellite/global positioning systems (GPS) for locating and otherwise communicating with loads and units on the earth's surface over several miles, and radio frequency identification devices connected thereto via radio waves—to identify loads at levels of subcontainers, pallets, individual boxes, and other small containers). Such platforms have existed since the mid-1990s;
- Decision support software to automatically collect and analyze data flows from the central logistics-management software system for anomalies that might indicate the need for a further inquiry within specific loads or entire

supply chains. Using algorithms, such software would provide automated alerts where movements, conditions, or other events in supply chains depart from empirical patterns, thereby indicating that further inquiry may be warranted. These have been called "exceptions reports" in commercial logistics-management systems. For instance, a specified intermodal train may usually take a specified number of hours to travel from the Alameda Corridor in California to Chicago during a particular time of year. There will be no report if this trip goes according to pattern. Alternatively, an early-season snowfall on the tracks in the Rockies might prompt delays, which would be the subject of an "exceptions report" to the carrier's operations center, to the shipper's logistics departments, and to the various personnel at the business waiting to receive the goods;

- Long-distance wireless technology for communicating with freight loads and containers at a distance of many miles. Most common in this respect are global positioning systems (GPS) and other satellite-based systems. These have been around for a long time. For instance, Schneider National has equipped its trucks with QualComm satellite transponders since the early 1990s. In addition, terrestrial communication systems such as Advance Mobile Phone Service, North American "cell phones," and Code Division Multiple Access (CDMA) are available;
- Short-distance wireless technology, like a radio frequency identification device (RFID), for communicating among freight loads and containers in close quarters—at distances measured in feet rather than miles (the Auto-ID Center at MIT, which closed in October 2003 and transferred its technology standards-setting role to EPCglobal, is the foremost developer of standards for this sort of functionality). Passive RFID functionality "announces its identity when hit with a non-line-of-sight electromagnetic field."[10] Upon such a "hit," the contents of the item tagged with the radio frequency identification device would become instantly known remotely. The most prominent adoption of this technology is evident in Wal-Mart's June 2003 announcement that its top 100 suppliers must ship their products with such devices by 2005—at both the case and pallet level. Since then, the U.S. Department of Defense (as a purchaser of goods), and numerous additional private firms, has announced similar RFID requirements for their vendors;
- Electronic seal and sensor devices. Electronic seals "combine manual seal elements with electronic components to measure seal integrity, store data, and provide communications."[11] Most of these use RFID technology, though some use infrared signals and others direct-contact communications technologies.[12] The significance of electronic capability is to avoid both the manual verification process attendant to mechanical seals and the delay required to stop the load and inspect the seal. In addition, the electronic seal—in contrast to the mechanical type—can be queried all along a cargo's journey rather than solely at an individual's physical location.

Related technology could, as warranted, include sensors of various sorts (temperature, pH level, pressure, presence of explosive or nuclear materials, radiological readings, hatch covers or doors open versus closed, container full/partial/empty, and battery condition), whose readings would be transmitted to the software platform via RFID or GPS technology.[13] The key indications would likely be intrusion detection and dislodging of doors, bars, and hatch covers.

Finally, not only have these devices been around for several years, they are the subject of a formal report commissioned by the U.S. Maritime Administration (MARAD) and published in 2003, describing their functionality and evaluating their operational effectiveness.[14]

Proposed Protocol Features

A network-centric freight security protocol would require the following features:

Integration

While the above tools are available commercially, integration in the context of specific supply chains would be required and would pose a nontrivial hurdle to implementation. That said, software platforms, long-distance communication devices like GPS, short-distance transmission technologies such as RFID, and electronic seals and sensors within containers or other freight units have been successfully integrated and their capabilities deployed in multiple settings.

Direct Observation in Real Time

First, the data points composing the network's visibility are based on direct observation. Simply put, at a particular time, one or more aspects of the cargo's attributes (e.g., freedom from tamper) are reported by instrumentation affixed to it, and this information is transmitted by the information network to the central data-collection system.

Second, reference to "real time" need not necessarily be literal, though it can be. The context in which discussions of freight security take place is the present, and largely manual, system of information transmission. From a cost-benefit standpoint, for instance, it may not be worth a constant satellite report on a sea container's location via GPS communicating with a ship, which in turn retransmits RFID-conveyed data from containers, boxes, and pallets. So-called "batch processing" aggregates messages into time periods of minutes or hours—as the operator chooses.

The key here is that today's widespread lack of automated data gathering leaves the logistics system to resort to faxes and telephone calls to identify information about loads in the system and the vehicles that carry them. Real-time awareness, whether literal or at chosen intervals, would be required for any sort of contemporaneous awareness of events within the supply chain.

Chain of Custody

Stephen Flynn coined the term "electronic chain of custody" to describe the collection of data relating to cargo loads and the units that carry them as they are

conveyed from one party to another in the supply chain.[15] This refers to the use of long-range and short-range wireless devices to collect data on the status of cargo—at the load level (such as pallets and boxes via RFID) or at the unit or vehicle level (such as a GPS uplink to identify the location of a truck trailer on the surface of the earth). The devices would collect transmissions from the loads or units via devices on those objects—such as evidence of surface intrusion from an electronic seal on the surface of a sea container or a reading of temperature or pressure within a rail tank car carrying a hazardous gas or liquid. Another prominent expert, Craig Harmon, refers to this as the "chain of possession."[16]

It is fragmentation in the structure of logistics flows—the multiple "hand offs"—that prompts the need for such an approach. In contrast, the freight integrators (FedEx, UPS, and DHL/DeutschePost), have physical and operational integration, as well as data integration, and would not be described in terms of such a "chain of custody." Custody does not change hands from pick-up through to delivery—all trucks, aircraft, personnel, and related data are controlled and managed by one entity (FedEx, UPS, or DHL/DeutschePost).

In the more typical multi-party supply chain, it is the sum of these "disconnects" that poses the major impediment to the data integration required for the network-centric strategy. These same "disconnects" are also the main vulnerability points that provide an opening to terrorist intervention in the logistics system and various hand-off points include:

- Originator of cargo flow (shipper)
- Transport operators (rail, dray, over-the-road, air, and ocean)
- Third-party logistics provider (agent with either its own transport and/or warehousing assets or owning no such assets and contracting with others for transport and warehousing assets)
- Recipient (consignee)
- Freight forwarder
- Subcontractor (such as consolidator or deconsolidator at distribution center)
- Bonded warehouse
- Law enforcement (such as customs or a weight station)

Specified Data

The following cargo data sets are suggestive only and are borrowed from a list prepared by Johns Hopkins University Laboratory and cited in the presentation, "Logistics Security in the Supply Chain: Strengthening the Link,"[17] presented September 18, 2003:

- Status

  Where is (or was) the container?
  Is there a problem with it?
  Is the cargo intact?

Has the container been tampered with or damaged?

- Direction

  Where is the container going?
  What are the dimensions?
  What does the container weight?

- Content

  What is inside the container?
  Do the contents match what is expected?

- Identity

  What container is this?
  What seal is this?
  Do the seal and container IDs match?
  Where did the container originate?
  Where is the container headed?
  What is the planned route?
  What transport vehicle is this?
  What carrier is this?
  What transport operator is this?

- Legality

  Is the transport operator in compliance with applicable law?
  Is the carrier in compliance with applicable law?
  Is the transport equipment in compliance with applicable law?
  Are the above three licensed to carry this kind of container?
  Are any route restrictions being violated?

- Safety

  Is this container safe?
  Should the transport (truck, rail car, etc.) or container be inspected?

- Access

  Should this container be exiting?
  Should this container be entering?
  Is the transport operator authorized to carry this specific container?

The possible variations on the above data sets are extensive.[18]

What is significant is this: commercial and security experts would need to agree on some selection of data categories in order to provide visibility into the supply chain for remote real-time awareness.

Practical Testing/Pilot Programs

The array of devices and functionalities summarized above under "Applications Required" have been deployed in many and varied settings. A lay person's familiarity with tracking a UPS parcel via the Internet or receiving an automated alert to a United Airlines flight delay on one's PDA give some illustration of current capabilities. This paper does not undertake an exhaustive coverage here.

However, in considering operational viability in security-specific protocols, policymakers can look to a handful of pilot programs under government auspices in Canada, the United States, and elsewhere. In particular, these both reflect Canadian and U.S. government consideration of the tools necessary for a network-centric freight security system, and they provide some tangible experience with those tools in actual logistics operations.

Operation Safe Commerce—Northeast

Operation Safe Commerce—Northeast targeted potential terrorist interference with a supply chain focused on sea containers.[19] Federal and state officials proposed this before September 11, 2001, and launched it shortly after the attacks. Led largely by Raymond Gagnon, former U.S. Marshal for New Hampshire, this project was billed as a public/private partnership consisting of the governor of New Hampshire and the U.S. attorneys for New Hampshire and Vermont as chairs. Additional federal/state partners included U.S. Customs, U.S. Coast Guard, U.S. Border Patrol, the Volpe Transportation Systems Center (DOT), the New Hampshire Department of Resources and Economic Development, and the New Hampshire International Trade Association (a state agency).

Developed in response to the identified need for enhanced cargo security, the first phase of this project was to (1) identify gaps in direct observation within the supply chain, and (2) demonstrate the ability of off-the-shelf technology to provide such direct observation to monitor, track, and seal cargo from point of origin to point of delivery. In addition to the above officials, it included the Lawrence Livermore Laboratories in California, the Port of Montréal, the U.S. Coast Guard New England district, and U.S. Customs (now U.S. CBP) region office for New England.

Receiving funding from the U.S. Department of Defense Technical Support Working Group, Operation Safe Commerce hired the Volpe Center—a think tank within the U.S. Department of Transportation—to provide technology and transportation expertise.

Private-sector partners included Osram Sylvania (a New Hampshire manufacturer of lighting products), BDP International (a third-party logistics firm), and C.P. Ships (a large carrier operating ocean ships across the Atlantic and into Montréal, among other routes).

The supply chain extended from an automobile headlight factory in Nove Zamky, Slovakia, to a factory in Hillsborough, New Hampshire. The lamps traveled in sea containers—400,000 tail lamps per container—via truck chassis from their origin to the Port of Hamburg in Germany. From there, the containers went to the Port of Montréal and were then taken by truck chassis to the New Hampshire factory.

Engineers at the Volpe Center used the following methods of data gathering:

- Chose commercially available tracking and monitoring technology to monitor a test container from Slovakia to Hillsborough;

- Installed electronic monitoring devices at five locations along the land routes; and
- Installed a global positioning system (GPS) transceiver and data logger on the container, along with a seal and an intrusion detection device.

GPS is a satellite-based technology that can locate objects accurately virtually anywhere on the earth's surface. The seal technology was designed to detect intrusion against the structural integrity of covered areas of the container's surface.

In so designing the above, the project gathered data from the cargo vehicle (sea container), its origin and destination were known, its location tracked, and its freedom from tamper indicated by the seal technology sensors that transmitted to Volpe Center data collection via GPS uplink.

Federal operational personnel in the northeast led operations, with Stephen Flynn, now Jeanne Kirkpatrick fellow at the Council on Foreign Relations and former U.S. Coast Guard commander, giving ongoing assistance.

In terms of the six elements of network-centric freight security set forth above, the pilot succeeded in attaining the first four relating to real-time data on the points of information needed to evaluate security and isolate lapses thereof.

As for the fifth, central systems, those are available commercially and were accessed by the project participants. As for the sixth, decision-making roles, those can be established and allocated if the real-time data and analysis are in place.

Operation Safe Commerce—U.S. Federal Grant Program

U.S. CBP and the U.S. Transportation Security Administration (TSA) jointly administer this program, with ongoing management assigned to the Office for Domestic Preparedness within the U.S. Department of Homeland Security. It consists of grants of $58 million awarded for projects at the Ports of New York/Newark, Los Angeles/Long Beach, and Seattle/Tacoma.

This is distinct from the program of the same name above and reports on activity to date focus more on grant awards and more preliminary stages of pilot projects. Details as to operational features, data categories, and real-time visibility into the networks subject to the grants are still sparse.

However, the scope of this "Operation Safe Commerce" includes electronic seal technology for sea containers and related radio frequency identification device and GPS (satellite) transmission technologies, along with logistics-management software known as "supply chain event management" (SCEM) systems. Using this description, they seek to use electronic instrumentation to directly observe the "box's" journey, capture it in real-time data via the stated wireless devices for collection, and then analyze it via SCEM.[20]

This is arguably the "flagship" pilot program within the U.S. government demonstrating the network-centric approach. It is, as of this writing, in the planning stage for its third iteration ("Operation Safe Commerce 3").

Detroit-Windsor Truck Ferry

The Detroit-Windsor truck ferry is one example of an electronic application directly related to homeland security.[21] The project uses wireless data transmission—through GPS uplink miles away from the border checkpoint—to provide customs officials evidence that a truck and its load have already been identified as safe and can proceed without search or stop.

Since 1990, this firm has carried hazardous materials and oversize freight—two categories not allowed on the Ambassador Bridge or in the nearby Detroit-Canada tunnel—across the Detroit-Windsor border. This firm, using a $135,000 port security grant from the U.S. Department of Transportation, implemented an advanced notification and tracking system that electronically receives specified data on all trucks carrying hazardous materials across the U.S.-Canada border via ferry.[22]

The author was specifically referred to this project by Transport Canada in order to provide an example of data gathering relating to the first three elements in the above list of network-centric elements. Note that this program does not use electronic seal technology to provide real-time indication of tamper.

Because truckloads of hazardous materials are identified as potential sources of terrorist harm, an electronic transmission of such data, in advance of reaching the border, was viewed as a priority.

Critical elements of the system include the following:

- Prearrival notice of vehicles transporting hazardous cargo across the border.
- Automated system providing an accurate and detailed activity report for each cargo trip including information on driver, vehicle, and HAZMAT profile of cargo.
- Complete traffic and activity analysis capabilities for law enforcement.
- Seamless driver registration system with 100 percent driver participation.
- Advance information availability through Web-accessible registration.[23]

Among government agencies using the system, all said it had a positive impact on their awareness of hazardous material transportation at the border, with 86 percent of those rating it “very positive” and the rest “generally positive.”[24] All stated that the information supplied by the system had generally been complete.

The truck and load can be admitted through the border crossing without a stop for search. Through the satellite uplink, the data is transmitted to border authorities several miles away from the border, avoiding both the need for inspection and physical production of paperwork at the crossing.

This has been operating smoothly for several months and provides a reliable substitute to searches and paperwork.

Smart and Secure Tradelanes (SST)

This is touted as "the first automated global network that improves the security and efficiency of cargo containers shipped into the U.S."[25] It combines the three largest port operators in the world: Hutchison Port Holdings, P&O Ports, and PSA Corporation—together with about 60 technology providers, manufacturers, and shippers who convey goods in Asia, Europe, and the United States.

The SST initiative covers 15 of the world's busiest ports. The program tracks sea containers en route from one shipper location to another through various ocean and other carriers using:

- Logistics software platforms to integrate data gathered;
- Automatic identification technologies from various vendors (including bar code, radio frequency identification device, and satellite/GPS);
- Sensors within containers to report real time on loads and their conditions; and
- Electronic seals (including functionalities to digitally lock containers and to transmit real-time alerts about tampering and other events with containers and loads).[26]

Notably, SST is largely the product of private effort. Hutchison Port Holdings has taken the lead along with the Strategic Council of Security Technology. SST has some connections with the federal "Operation Safe Commerce" program (for instance, the Port of Seattle participates in both Operation Safe Commerce and in SST) and with CBP, TSA, and other government agencies, but it is largely a product of private effort.

The projects have not yet been completed but since early 2003, they have been providing real-time visibility into sea container supply chains in Europe, Asia, and North America.

State of Washington Electronic Seals at Canadian Border

The State of Washington's Department of Transportation, using grant funds from the U.S. Federal Highway Administration, has an ongoing project to test the use of electronic seals for container clearance at borders. By affixing a container door seal transponder to the sea container itself, the project has provided (electronic) documentation sufficient to avoid a second, manual review process for containers bound for Canada unloaded at the Port of Seattle. These containers are then transported in secure, "bonded" status.[27]

This program's goals include:

- Better security through intrusion detection (perhaps, though not yet, recording the time, date, and geographic location of such intrusion);
- Better efficiency at the border by increased throughput by replacing error-prone paperwork with electronic transponder readings; and

- An integrated network of transportation information ultimately made possible by the electronic seal technology attached to loads and cargo units.

Although this program has not yet fully substituted electronic data flows for searches and documentation in the primary border-crossing context, it has accomplished this goal in the "bonding" process for containers unloaded at Seattle and bound for Vancouver via truck. For this "bonding," the agencies still rely on direct observation to confirm status. But now, automatic data transmissions substitute for the stops, searches, and paperwork previously required at the Blaine, Washington-British Columbia checkpoint.

APEC Security Initiative

Late October 2003's meeting of the Asia-Pacific Economic Cooperation (APEC) forum in Bangkok, Thailand ended with minister-level focus on a network-centric freight security pilot.

Deploying wireless devices from Savi Technology (for direct electronic observations) and an Oracle software platform (for transmission, collection, and analysis), the "Secure Trade in the APEC Region," or "STAR-Best," program drew endorsement from the U.S. secretary of state, Thailand's transport minister, and the prime minister of Singapore (Singapore is a major transfer point for Asia-North America container shipping).[28] These operations involved electronic seals and transponders to track sea containers moving between the ports of Laem Chabang, Thailand and Seattle.

Subsequent Pilot Programs in the Works as of Early 2005

Ottawa is working on a new pilot program including Transport Canada, CBSA, and other agencies as a follow-up project to "Operation Safe Commerce—Northeast" described previously. Involvement will include many of the same Provinces, New England States, and the Port of Montreal.[29] Here, having validated the concept of "smart container" or what this paper calls a "network-centric" approach, the pilot would review various integrated technology applications for their effectiveness in implementing this approach.

Washington has several programs to test both the operational viability and to identify new technology applications of this "smart container" or "network-centric" approach. "Operation Safe Commerce," the U.S. federal grant program described previously, is completing its "OSC2" phase and is preparing for a third "OSC3" under the auspices of various DHS agencies.[30] U.S. CBP has its own "Smart Box" program to this end. The Homeland Security Advanced Research Projects Agency (HSARPA), a scientific R&D arm of DHS, has publicly called for ideas and applications for "smart container" to be funded by this arm of the science and technology directorate of DHS.[31]

Recent Product Launches

In the last 12 months, firms in both Canada and the United States have reached the point of launching smart container-type applications that are ready for

commercial deployment by shippers and carriers. In the United States, for instance, GE has joined with All Set Marine of Sweden to offer "smart container" functionality, with commercial sales expected by the end of 2005. In Canada, WayFare Identifiers, Inc. (WFI) has its own offering of "smart container" functionality. Aspects of this capability are on offer from other firms as well (see footnote as to author's personal and business contacts with both GE and WFI).[32]

Arguments Pro and Con

Advocacy of the network-centric view in freight security would likely attract a series of objections. Six prominent ones follow, each with a reply on behalf of the network-centric view.

OBJECTION #1: LOGISTICS INDUSTRY FRAGMENTATION MAKES THIS UNWORKABLE.

The integration characteristic of the network-centric model's most commonly seen present-day examples—FedEx, UPS, and DHL—is precisely the opposite structure of most supply chains. The fragmentation presented by the multiple hands through which a sea container or truck van must pass going from shipping manufacturer to distributor or end-user, and the 24/7 operations and geographic dispersal involved, present the chief challenge to implementing the network-centric protocol.

To a large degree, whether or not supply chain security commensurate with available scientific applications is worth pursuing depends on how, if at all, the freight "integrator" model of logistics technology can be applied to shippers and carriers whose operations are not owned and operated by one firm. Does the commonplace example of FedEx, UPS, and DHL truly apply to enterprises seeking to integrate only their interrelated data? Or must one "own" the entire network of load and vehicle assets, people, and data in order to have the needed level of visibility and security in the supply chain?

The argument for the current stop-and-search approach and against a network-centric model rests largely on the fact that—except with freight "integrators" such as FedEx, UPS, and DHL—cargo assets are managed by a succession of firms during a given journey.

Further, this has led to a nonelectronic (i.e., manual) status quo for freight information rather than the use of state-of-the-art electronic data-gathering hardware and software platforms. Telephone calls, faxes, and the paperwork that accompanies loads (bills of lading, paper manifests, etc.) are the primary source of logistics information—especially between different companies (such electronic information integration is considerably more advanced within particular firms involved in either shipping, carrying, or receiving freight).

This is not to suggest that these firms lack IT capabilities. But, except for the supply chain management early adopters, by far the majority have not yet chosen to replace enterprise systems peculiar to their own firm. For every class-of-the-field Wal-Mart, Hutchinson Port Holdings, or FedEx, there are numerous firms that remain either manual or within conventional enterprise resource planning (ERP) silo systems restricted to their own operations.

The same is true of carriers. Despite the existence of Roadway Express, Yellow, or Schneider as class-of-the-field outliers with state-of-the-art Web capability, most of their counterparts lack any such connectivity.

Reply: Supply chain fragmentation is the reason that it poses such a vital vulnerability and fortunately, software and wireless tools have been designed for multifirm collaboration.

The fragmentation argument not only proves the difficulties of implementing a network-centric supply chain security protocol, it also underscores why terrorists are likely to find this an attractive threat vector from which to penetrate civil infrastructure and deliver weaponry to our populations.

Fortunately, the fragmentation traits do not prove that a network-centric protocol is impossible to achieve. Quite the contrary, despite the very partial extent of logistics technology adoption, the applications are available (with more being added constantly). Ranging from universally known ERP names like SAP, Oracle, and Microsoft to dozens of specialists in logistics-management software such as Descartes Systems (Toronto area) and G-Log (Connecticut), much software has been written to integrate the multiple operations of a firm and its many suppliers, customers, and others with whom it must communicate in order to do business.

These systems have been designed precisely to address the fragmentation characteristic of modern supply chains. Being a freight "integrator" certainly helps in implementing the data gathering necessary for real-time information on freight moves, but with the availability of these systems, it is by no means a necessary condition.

Today it is possible to gather data from disparate, otherwise unrelated assets and people without having those assets under one's ownership or those people on one's payroll. There are numerous scientific applications in logistics-management software and wireless communications devices (notably satellite/GPS, terrestrial telecommunications, and RFID technology) developed for reasons of commercial efficiencies. While the scale of adoption among nonintegrators is small, the functionalities are available commercially.

Beginning mostly during the last decade, entrepreneurs developed software applications and wireless devices to enable business efficiencies. Shippers such as Wal-Mart, the world's largest retailer, installed complex software and wireless combinations that automatically replenish inventories as customers buy shelf stock at individual stores. Carriers like Schneider National, the largest privately held trucking firm, deployed satellite technology to individual truck rigs in the early 1990s to identify location in real time and give immediate data on performance metrics.

Chemical firm Stolt Nielsen, grocer Giant Eagle, automaker Ford Motor Company, pharmacy CVS Corporation, and housewares maker Newell Rubbermaid each run supply chains with scores of suppliers, carriers, and customers, and each uses logistics-management software to run their businesses.

It is hard to make the case that only freight integrators can integrate the data in a supply chain.

In short, the relevant applications in wireless and logistics-management software have been designed for the very fragmentation that characterizes most supply chains. Although not yet used universally, they are used to operate leading firms in supply chain management.

Objection #2: Physical infrastructure limits prevent freight-flow improvements.

Even if customs agency rules and processes were made more efficient from a security administration standpoint, much of this progress would be of little operational advantage due to infrastructure bottlenecks and related physical constraints. For instance, it is of little value to have efficiencies granted to a Canadian trucking firm taking auto parts from London, Ontario to eastern Michigan if the Ambassador Bridge over which the relevant trucks must travel has no "extra" lanes for advantaged traffic.

This argument is also made from other modes' points of view. For instance, many seaports' intermodal terminals have throughput limitations having much more to do with square footage versus cargo volume than with customs' regulatory impediments. Similarly, the passage of Asia-originated freight into the Port of Long Beach (from where it is subsequently carried by rail) faces major volume restrictions from the limitations of the Alameda Corridor for the inland, eastbound rail journey from that port.

Reply: Post–September 11 slowdowns have a large stop-and-search aspect.

First, studies offer empirical evidence of what truck drivers, stevedores, and logistics managers have observed from operations since September 11: materially increased delays and related costs due to enhanced security at border check points and seaports.[33] Security delays caused by an enhanced, rigorous stop-and-search environment have increased markedly.

There is no doubt that transportation infrastructure in both Canada and the United States is stretched, and the end of the recent recession has exacerbated bottlenecks that were less severe in lower-volume contexts.

Second, design and viability of future infrastructure will be driven by the regulatory climate anticipated. Without a new structure, enhanced security will require a great deal of stop-and-search activity. This will require more truck plazas and agent facilities and more dockside and airport space for customs personnel to review paperwork and search or scan loads and the equipment carrying them.

On the other hand, if borders (and ports) cease to be seen as venues for looking at boxes and security seen as remote data gathering from freight all along its route, the bricks and mortar plazas and freight yards can be reduced to a large extent with electronic data flows. With this, a more modest physical infrastructure at border checkpoints and ports then becomes possible.

Objection #3: Electronic seals are the subject of significant dispute.

First, use of electronic seals and sensors are said to offer more than they can deliver. It suggests a misleadingly high level of security in that it fails to address the human factors, fragmented processes, and largely manual context in which the seals and related sensors would be used. In short, what is to stop an enterprising terrorist from compromising the seal or sensor?

Second, these are not in widespread use, and they have never been deployed on a large basis—only in post–September 11 pilot programs. In short, the practicalities of actual deployment in the context of millions of sea containers, truck vans, etc. are daunting, if not beyond achievement.

Third, they add an impractical level of expense to industries like ocean shipping and long-haul trucking (both truckload and less than a truckload [LTL]) that these low-margin sectors cannot sustain financially.

Reply: The technology exists; its functionality has been proven in third-party tests.

The premise of requiring electronic seals and related devices is this; a network of geographically dispersed assets moving 24/7 that is not under the control of a single firm (as with the freight "integrators") requires some direct evidence of the cargo and its carrying unit's real-time condition.

Without such direct electronic evidence, there is no tangible proof that tampering has not taken place as the cargo and its carrying unit changes hands among sequential truckers, ship operators, warehousemen, etc.

Taking the objections in their above order:

First, even those who oppose deployment of electronic seals as part of a new security protocol do not suggest that this technology fails to provide a remote electronic indication of a breach in surface integrity or other conditions reports as designed. There is debate as to whether or not "false positive" readings are yet at an acceptably low level. Nevertheless, as stated in the introduction above, the U.S. Federal Maritime Administration's Office of Intermodal Development completed testing of seal technologies and found that "all the seals performed at the levels the manufacturers said they would."[34]

These devices are no substitute for disciplined security protocols and vetting of the individuals who access the cargo units, cargoes, and facilities through which they pass. What they could be is a means to confirm, through a single database despite sequential hand offs between multiple parties, the structural integrity of a box's surface and its freedom from attempts at tamper during the journey.

Second, while such devices are not yet in widespread use from the standpoint of world shipping and transportation, leading firms like Savi Technologies (San Diego, California) and Hi-G Tek (Israel) have refined the operational traits of their devices and have been recognized by the relevant standards-setting body—the ISO TC 104.[35] Similarly, TransCore (Harrisburg, Pennsylvania) is a major integrator so recognized. These are just a handful of the numerous names in this field.

These are not pilot programs. They are operational, with technical teams from each such firm expected to have this operational soon. The same is true of the seals tested by MARAD.[36]

Third, the expense argument is usually presented in the abstract. The fact that the industry, working through the ISO TC 104 committee and the above three firms, has taken the time and resources to work out a harmonized protocol is strong evidence that some firms expect this to be economically viable for them. This is not to say that standards have been agreed to, far from it. Reaching such standards of interoperability is arguably the largest remaining challenge to adoption and operative use of electronic seal technology.

But the fact that firms are already offering these devices in the market and making them available for deployment reflects a great deal on their practical viability.

Questions have been raised about the low-margin traits of certain ocean and truck carriers, and some have asked what amount is required to retrofit the entire sea container industry (to take an example). Neither of these relate to the proposal argued for here. It is a security protocol to be voluntarily accepted by those willing and able to achieve it, not to be mandated to all.

Note four final observations about cost concerns:

One, per-unit cost of devices is largely a function of manufacturing volume. The likely volumes in the context of a tangible incentive, like bypassing customs and related paperwork, is significantly higher than in the absence of such incentives. What we know now is that device makers perceive sufficient potential demand to manufacture electronic seals and related applications.

Two, there is more to the economic case than simply assessing the total cost of devices and their installation on the "boxes" and their integration into a firm's IT system. For instance, in context of the Smart and Secure Tradelanes project (SST) outlined above, Hau Lee and his colleagues at Stanford University Global Supply Chain Management Forum found that the active RFID technologies applied in that program yielded economic benefits in the range of $400 per move. In that phase one stage of the SST project, "A single end-to-end SST move of a typical container nets $378–462 of potential value to the shipper when subtracting the operating and variable costs."[37]

The study analyzed savings in terms of percentage of average total-container value shipped in SST phase one:[38]

Area of Potential Benefit	**Potential per Container Benefit**
Reduction in safety stock	$173–211
Reduction in pipeline inventory	$91–111
Reduction in service charges	$56–68
Administrative labor	$31–38
Reduction of pilferage, inspections, loss	$28–34

Total	$378–462

With regard to the economic case, what is significant is not so much to grasp the analytical tools deployed by people like Hau Lee and the Supply Chain Forum at Stanford, but to be aware that such tools exist and to avoid sweeping negative generalizations that lack a similarly detailed and evidence-based factual case.

Third, regardless of an individual firm's return-on-investment calculation and related cost and savings assumptions, it is vital to remain aware that no firm would be required to participate.

Those firms objecting to installation and integration costs, or not believing that return on investment or savings would be positive, would be at liberty to remain out of the program—albeit with continued subjection to the current, manual security protocol and its delays and expenses.

OBJECTION #4: NECESSARY TECHNOLOGY ADOPTION IS NOT YET FAR ENOUGH ALONG FOR CARGO.

Whatever the technology tools available, implementation of technology that gathers, transmits, and analyzes data from multiple sources among suppliers, carriers, and customers has not yet taken place on a large scale.

Automated tracking and tracing of a freight load continues to be more the exception than the rule. Real-time access to such a load's origin and destination is rare, and remote access to freight load integrity, the freedom from tamper addressed by electronic seal applications, is rarer still.

Reply: Leaders already adopting and integrating.

The fact that some leading shippers and carriers have already adopted wireless and logistics-management applications shows the viability of a network-centric approach. Moreover, recent technology adoptions in corporate supply chains reflect the power of commercial factors, without a push from government, to induce data integration of multiple and distinct firms into true logistics networks.

In a landmark development, Wal-Mart furthered its leading role in supply chain connectivity by announcing in June 2003 that by January 1, 2005, it will require its top 100 suppliers to have all their package cases and the pallets on which they are placed "chipped" with RFID tags.[39] This means that tiny radio frequency identification tags conveying identification and location information within loads will be embedded into these cases and pallets so that the Wal-Mart IT system can track, locate, and deploy them. Wal-Mart later expanded this mandate to its top 125 suppliers, adding that all of its suppliers would be expected to comply by 2006. Already in March 2004, Wal-Mart required that its top 30 pharmaceutical suppliers comply with this mandate.[40]

Second, later in 2003, the U.S. Department of Defense announced a mandate that its top suppliers (it has been vague as to the exact number) be RFID compliant by 2005. Given that its supplier base numbers in the thousands, this mandate may be even more influential than Wal-Mart's in promoting real-time electronic connectivity.

These RFID developments relate directly to a network-centric approach, as these tags emit a radio signal read by remote electronic readers several feet away. These readers, in turn, are integrated with a software platform such as a logistics-management or inventory-control program. As a recent article in *CFO* magazine states, "When all goes well, RFID tags provide precise information about the whereabouts of merchandise as it moves along a company's supply chain."[41]

While Wal-Mart received the most publicity in this regard, a recent commentary on Wal-Mart's CIO's address to suppliers on November 4, 2003, cited related adoptions by, "All these big players from Wal-Mart to the Department of Defense, DuPont, Bayer, the big ports and carriers."[42]

Add to this Procter & Gamble, Gillette, and the 100 participants in the MIT Auto-ID/EPCglobal partnership among 100 global companies, and real-time visibility is not the focus of just a few obscure firms.[43]

Objection #5: This would cost too much.

To be sure, adopting the network-centric protocol will cost money. Just taking RFID adoption as an example, AMR Research, a prominent commentator and consultant on supply chain and other technology applications, estimates that a typical consumer products manufacturer that ships 50 million cases per year will have to spend "between $13 million and $23 million to deploy" the RFID devices.[44] There is considerable comment that this will pose major implementation problems across the 100 suppliers affected and the firms with whom they work—in addition to Wal-Mart.

Reply: Asserted, but not proven.

The contention that the technology needed for real-time data access to logistics networks "would cost too much" has several flaws:

- Widespread port and border shutdowns would harm businesses materially in another incident.

  It assumes that the current system suffices to protect our economies from disruption due to a terrorist incident. To the degree that North America experiences another September 11-type incident, there is likely to be a rethinking of the entire current freight security protocol. "Rethinking" is a dignified term for it, as the informal comments of both government and business personnel indicate an expectation of chaos in the event of "another incident." Policymaking in this arena may be chaotic as well.

  In such an instance, it is reasonable to assume that a virtual stoppage at ports and borders might take place. The same Hobson's choice faced after September 11 continues under our inspections-based system, and shutdown for days, weeks, or longer is a distinct possibility.

- The failure to address costs of sole or primary reliance on the present strategy.

The argument that excessive cost prevents a network-centric approach fails to address the costs of the current system. Particularly as to delays now built into daily operations, the costs might be considered large.

A post–September 11 study focusing on the southeastern Michigan and southwestern Ontario economies projects that by 2010, "the cost to shippers of slowed deliveries between the two regions is projected to reach at least $350 million a year, costs that filter down to the producers and consumers."[45]

Notably, this paper suggests that qualifying shippers and carriers receive expedited clearance through ports and border checkpoints as (partial) compensation for adhering to standards. Specifically, the optimal clearance would take the form of a transponder signal from a truck trailer, railcar, sea container, or unit load device whose receipt by government agencies indicates such qualification. It would proceed without stopping or a review of paperwork through the checkpoint.

- The return-on-investment case for real-time visibility.[46]

  As noted above, some leading logistics operators are already adopting the necessary technology for real-time visibility into their logistics networks without government encouragement or coercion. [47]

  Many leading firms have been slowly adopting logistics-management software and wireless application communications devices. These adoptions have been for purposes of commercial efficiencies like the cash-to-cash cycle (largely inventory efficiency), cost reduction, and customer satisfaction. For this reason, vague generalizations that such technology "costs too much" warrant skepticism.

For years, Wal-Mart has run an automated system of inventory replenishment based on an enterprise software platform and related wireless connectivity between the central system, regional distribution centers, and the shelf stock of individual stores. This firm has pursued real-time electronic data flows for a long time. Wal-Mart was "Among the first retailers to use computers to track inventory (1969), just as it was among the first to adopt bar codes (1980), EDI for better coordination with suppliers (1985), and wireless scanning guns (late 1980's)."[48]

Wal-Mart's recent RFID initiative has been launched for commercial purposes, and no one predicts they will lose their 100 top suppliers due to this.

In an A.T. Kearney report on the Wal-Mart initiative, they concluded that this would require investment of U.S.$400,000 at each distribution center and $100,000 at each retail outlet to read and manage data. To obtain the desired savings from this adoption, a major chain would have to "spend $35 to 40 million to integrate the information into its reporting systems, which will be needed to gain much of the potential savings."[49]

The same report concluded that these measures could reduce inventories by 5 percent and corresponding labor costs in warehouses by 7.5 percent.

Another firm, Deloitte Consulting, suggested that the A.T. Kearney estimates were too conservative and instead projected labor savings in warehouses at 20 percent.[50]

During the summer of 2003, Schneider National, the trucking leader mentioned previously that installed satellite technology on trucking rigs in the early 1990s, announced a new application. It joined a consortium with the Qualcomm wireless communications firm to provide satellite tracking of truck trailers that are not tethered to a tractor.[51] Real-time location of a truck trailer tethered to a tractor, and now to one detached and abandoned elsewhere, can now be located by satellite. This work was pursued for commercial efficiencies and not due to government security mandates.

Wal-Mart, Schneider National, and the other industry leaders already adopting wireless and logistics software to their operations (for commercial reasons) indicate that the excessive cost argument is weak, and the specifics of each firm's return-on-investment case for technology vary.

But the fact that companies are already providing the technology needed for real-time visibility and that carriers and shippers are already buying it reflects that opponents of the network-centric approach have not made their case.

At least they have not made their case for all shippers and carriers. There are still truck firms that will not spend U.S.$50 per lock to protect trailer contents. Within the transportation community, as in any other, there are both leaders and laggards.

As the widely quoted A.T. Kearney report on the costs of Wal-Mart RFID concludes, after predicting considerable need for investment by affected suppliers, "The future is already here, it's just not evenly distributed."[52]

Finally, and perhaps most importantly, the argument of excessive cost assumes shippers and carriers would alone shoulder the expenses of implementation and operation. This assumes a negative answer to the question whether or not government should bear most or all of the cost of securing the supply chain post–September 11. This paper argues below that the network-centric security protocol is just as much a cost of defending Canada and the United States as military procurement or the maintenance of a standing army.

Objection #6: Encompassing a few Fortune 100 supply chains will not suffice to address a material amount of total cargo flows.

Relatively few supply chains have as yet adopted the applications referenced above as part of the network-centric strategy. These tools, as sophisticated as they are, cannot be applied in material numbers to the vast bulk of cargoes. Most supply chains are not nearly ready for this.

Reply: Adoption will be incremental, and a small number of large supply chains will have large impact on total volumes.

First, as a matter of transition and sequencing, adoption of the network-centric approach to supply chain security—in the Canada-U.S. context and elsewhere—

need not be done all at once. The policy proposed in this paper would be adopted by individual supply chains voluntarily.

Second, this policy would serve as a supplement to the present stop-and-search protocol at ports and border checkpoints, which forms the foundation of today's practices. Some supply chains would adopt before others and as that takes place, conventional search-and-scan resources would be increasingly freed up to focus on less-developed supply chains.

Third, there are supply chains whose volumes contribute disproportionately to total port and cross-border commerce. These not only enjoy a managerial and technological head start on the process of network-centric adoption, but by themselves, they account for large volumes of international commerce. Wal-Mart, featuring so prominently in technology adoption, accounts for a full 10 percent of U.S. imports from China—worth U.S.$12 billion last year.[53]

This is not just about one company. In the United States, for instance, Kmart, Target, Costco, and Sears—plus Wal-Mart—account for 60 percent of general merchandise sales (15 percent of all retail sales).[54] That percentage translates into a significant portion of sea containers entering Canada and the United States.

It is realistic to consider that leading manufacturers, retailers, and carriers may be willing and capable of adopting the needed technology, and thereby providing the needed remote direct observation and real-time visibility.

If given sufficient incentives, additional firms might join their ranks and firms already on this path to adoption might accelerate their efforts. Rejecting such adoption out of hand is not warranted.

Statement of Vision

Transport Canada's Tony Shallow crystallized the author's perspective on the network-centric framework for Canada-U.S. freight security after September 11. In a 40-minute talk about his agency's efforts to reduce border congestion and provide better border security for trucks in particular, he made the following observation:

> The new security imperative is how to insure security. The answer is the same one supply chain management people have been asking on the commercial side: We need to make the process electronic. On [border freight efficiencies], we need to take carrier and customs operations out of the paper realm and into an electronic stream of data. We need to pre-clear [away from the border] electronically. *The solution to both questions is rooted in electronic transparency throughout the supply chain* (italics supplied).[55]

Policy Context and Recommendations

It is a commonplace notion that post–September 11 asymmetric warfare transforms the task of homeland defense in such a way that we need to

fundamentally rethink existing security protocols. This paper's thesis presupposes that securing supply chains against terror in the post–September 11 world is dynamic, with multiple stages of development. It asks in the longer term what the next stage of development should be, and it proposes an answer.

As for policy planning for the long-term security of the supply chain, we need a practical how-to document from both governments. Both Canada[56] and the United States[57] have set forth formal post–September 11 security policy documents, and their leaders have informally set forth principles of homeland defense doctrine as well.[58] We need to go beyond such frameworks to fill in the details of a transportation security strategy (such as the U.S. Congress tasked the secretaries of homeland security and transportation to deliver in the recent intelligence reorganization bill).[59] For the next stage of homeland security development in transportation, we need specifics as to standards, fiscal support, and expected performance.

As for policy actions, the following practical steps would promote the network-centric approach to supply chain security between Canada and the United States:

- Give assurance to both governments and the public that in regard to border protection, defense, and other traditional roles protecting public safety from dangers both foreign and domestic, Ottawa, Washington, and their related local governments would retain their existing powers. Notably, agencies would keep the power to stop cargoes for any reason. But the default mode of freight movement in adherence to the network-centric protocol would be continuous movement rather than stop-and-search activity as a regular aspect of border checkpoint crossing and port entry.
- Those private parties owning and operating the logistics system would be induced to participate in the network-centric protocol not by regulatory demand but via incentives. It would be voluntary, though encouraged by the following inducements:
  - Expedited treatment at ports and borders. The default mode would consist of no stopping, with related documentation conveyed electronically and expected to be reviewed prior to arrival at ports and borders. (Note that current references to "green lane" by Commissioner Robert Bonner would seem to refer to such treatment, but detail, of course, will determine the operative impact.)
  - Dollar-for-dollar tax credits to reimburse businesses for specified hardware, software, selected services (notably maintenance of satellite or GPS uplinks), and dues to the standards-setting and audit organizations needed to implement the network-centric protocol.
  - Limitations on tort liability from terrorist incidents that impact participating firms. Those who adopted the data-gathering and related operational security steps would receive protection from tort liability akin to the "SAFETY" statute already enacted in the United States.

- Launch a new, unprecedented form of cooperation between the public and private sectors (and among individual private companies) in the definition, implementation, and verification of security standards. Government cannot just mandate these, as both operational access and related expertise lie with those who actually own and operate the logistics system.

Post-9/11 Supply Chain Security: The Next Stage

As stated above, and as the recent congressional enactment mandates for the United States, both Canada and the United States need a policy-planning document suited to the new asymmetric threat environment. As the legislation states, we need to identify and evaluate vulnerable transportation assets and systems and develop "risk-based priorities across all transportation modes, and realistic deadlines for addressing security needs associated with those assets."[60]

This is appropriate and necessary for the new threat environment, just as NSC 68 was prepared by the U.S. State Department's Policy Planning Staff in response to President Truman's request for basic principles for the novel threat environment that marked the beginnings of the Cold War. President Truman's terms of reference focused on the "probable fission bomb capability and possible thermonuclear bomb capability of the Soviet Union."[61] NSC 68 provided alternative courses of action, selected a robust defense, and most notably, recommended a fiscal component whose adoption would raise U.S. defense outlays three fold.[62] President Truman accepted both the strategic doctrine and the three-fold increase in defense spending.[63]

Policy actions in post–September 11 supply chain security require a similar framework that addresses two aspects specifically. First, terrorist abuse and penetration of logistics infrastructure in order to take life and destroy property raises unprecedented questions of how to involve the business sector. Traditionally not a participant in national security (except as a supplier), the individual companies who own and operate the systems of cargo loads and transportation assets already have more ready access and greater expertise in cargo logistics than any government body. Can government create mandates for business and expect excellence in response?

No, because government lacks the expertise, and it needs more than just compliance from business. This threat requires the best performance of which business is capable in order to enhance security and to monitor the related data flows that provide that security.

Second, traditionally government has funded standing armies, navies, and air forces to secure its territory. Private firms, on the other hand, have pursued commercial (not public policy) ends using their own funding. While exceptions are abundant in areas such as subsidies and regulatory mandates, the prospect of substantial public funding for equipment and services to protect an individual business's operations presents novel questions.

Bluntly stated, any such involvement would be unprecedented. It might be considered off-putting to those free market advocates who seek to separate, or at least minimize, the reach of government and business in each other's operations.

But an NSC 68-like document for post–September 11 supply chain security needs to address these fundamental questions. Just as that earlier study forced a sea change in U.S. national security strategy, both in terms of defense doctrine and the money to pay for it, a response commensurate with the novel threat here would be similarly significant.

How should the private and public sectors reallocate their respective roles, both operational and fiscal, to secure against the asymmetric threat? How robust a defense are we willing to mount, and should government or private firms foot the bill?

For those who believe that the asymmetric threat illustrated by September 11 changes geopolitical defense dynamics in basic ways, the novel questions that supply chain security presents are not surprising. This does not, however, make them any easier to address.

Retention of Traditional Government Security Role

This paper does not suggest any reduction or reallocation, in either Canada or the United States, in the national defense or public safety powers historically associated with government agencies. Canada Customs and Border Services Agency and U.S. Customs and Border Protection would each retain the power to stop any item or person for any reason. Similarly, Canadian sovereignty as to its territorial integrity and that of the United States would not be changed at all.

The proposed network-centric security protocol, like the present stop-and-search protocol, goes to the question of how government can get direct information on cargo status while such cargo is en route. The network-centric approach relies on direct data that is gathered remotely and electronically, while the stop-and-search method requires the box or truck trailer to be in the immediate presence of government agents, their scanning equipment, and other infrastructure.

But the network-centric approach would reallocate the direct observation role from public agents to private systems to a large extent, though not completely. It would foster company-by-company security standards in supply chains and then integrate their efforts via data collection, sharing, and analysis. It would thereby provide both Canada and the United States with the tools to ensure the other that particular supply chain operations were free of terrorist penetration, and it would provide them the needed information to conduct forensic tracing to better locate the source of danger where an incident occurs.

Incentives to Adoption

To retrofit technology applications and rework related businesses' processes toward the electronic connectivity needed for such network-centric integration

requires promotion of business cooperation with apt incentives. Mandates would be a blunt and awkward tool for such a sophisticated and mission-critical task.

What sort of incentives do we need? While this paper offers working hypotheses, only an individual firm can determine its own return on investment, and Canadian and U.S. policy should respond meaningfully to that fact of life. Both the Canadian and U.S. national government would need to offer an array of incentives and monitor actual business adoption.

Firms' behavior in response to these incentives would validate their adequacy or provide valuable feedback indicating a need to rework them. Subsequent fine-tuning might be part of an iterative process between public and private sectors in this regard. With that caveat, the following incentives would be good starting points:

- Expedited treatment at ports and border checkpoints (often this is called "green lane"). Clearly, the key would be in the details.
- Tax credits for capital expenditures on the wireless devices, electronic seals, logistics software platforms, and fees for needed services (e.g., access to the satellite backbone).
- Reliable exemption from tort liability arising from asymmetric attacks (not otherwise) for firms in certified compliance with the protocol as set forth by the standards-setting and auditing organizations provided for below.

These raise significant issues that we need to anticipate briefly below.

Philosophical Issues

As between public and private sectors, which should bear financial responsibility for supply chain security?

This philosophical question is worth addressing. By bringing a "war without fronts" to an infrastructure mostly owned and operated by private business, September 11 shifted accustomed public-sector roles in security and public safety to a new venue—away from the conventional battlefield and onto what was heretofore viewed as the venue of private operations.

Despite this shift in the context of national defense and public safety activity, this paper takes the view that protecting admittedly private supply chains from terrorist penetration is as much a public-sector responsibility as is NORAD protecting the skies above North America or the Canadian and U.S. navies protecting our shores. The fact that asymmetric threats have their locus in private operations and infrastructure invites an ideological question of whether or not this undertaking is itself private as well. This paper assumes that whatever the venue, this has an expressly public purpose: national defense and public safety.

This may merit a more extended treatment elsewhere. Notably, the IT applications called for here might result in powerful commercial impacts on efficiency and customer satisfaction. But this paper takes the view that retrofitting freight flows and reworking their operations toward electronic connectivity as a

means to protect the supply chain from terrorist interference is, in principle, simply part of the larger task of defending our nations and publics from threats.

Depending on one's resolution of this philosophical issue, one is likely to view financial reimbursement for wireless devices, electronic seals, and software platforms (either through direct payment from government or indirectly through a tax benefit) as business subsidy or, as this paper does, defense expenditure.

Finally, this question of who bears national defense costs when they arise in a private infrastructure context (transportation or otherwise) does not receive much explicit attention. Notably, Canada's 2004 Throne Speech and the FY2006 U.S. federal budget both reflect extreme pressure on discretionary expenditures in each national government. Neither government is offering much financial support despite the geopolitical nature of asymmetric threats.

In the Cold War context, at least in the U.S. experience, President Truman's receipt and endorsement of NSC 68 resulted directly in a three-fold increase in Department of Defense expenditures in 1947. Despite that administration's desire to redirect expenditures after World War II to a peacetime footing, the strategic implications of NSC 68 compelled him in another direction. Post–September 11 thinking in Ottawa and Washington needs to be similarly responsive to the new climate we face.

Practical Issues

If the public sector has chief responsibility for cargo security, as it has for other, more traditional long-standing security burdens, what types of incentives have the best chance of being meaningful to logistics businesses in order to elicit the response needed?

Policy should proceed on express statements by business managers to government (and on educated guesses as to appropriate business incentives), and its implementation (or lack thereof) should be evaluated in response. Public reporting on the state of post–September 11 logistics between Canada and the United States indicates at least three potential categories to positively impact firms' returns on investment—each of which gives rise to possible government-sponsored inducements to participation:

- Slowdowns at the border and at ports.

  This is the subject of reporting in various business press and academic circles, and complaints about delay and undue documentation burdens are significant. While there is ample ad hoc comment in business circles about this phenomenon, formal studies on this are addressed at greater length in the footnotes hereto.[64]

  Responding to this, policy should offer expedited treatment at ports and border checkpoints. This would include not only exemption from searches and scans, but also avoidance of stops for review of paperwork. These activities would all be replaced by electronic data flows. "Green lane" treatment is often referred to, for instance, in Commissioner Bonner's three-fold test for expedited treatment in return for: a) C-TPAT

membership in good standing, b) use of Container Security Initiative ports, and c) deployment of "smart container" technology.

Of course, description of expedited treatment goes to a default mode practice. As part of the continuing ultimate authority that Ottawa, Washington, and all their respective ministries, agencies, and local government units have over logistics security, any and all of these bodies should retain the right to intervene in freight flows and stop their movements for inspections or otherwise at their sole discretion.

Finally, and perhaps most important for policymakers, in considering expedited treatment, it is vital that a quid pro quo be established between businesses' contribution and government's response. At present, PIP in Canada and C-TPAT in the United States each promise the benefits of expedited treatment, but the precise nature and scope of these benefits are unspecified. Businesses cannot use them as the basis for either operational or financial planning, except in the most general way.

Moreover, there is, as of this paper's publication, no incentive structure to motivate a firm's adoption of "smart container," or network-centric, applications beyond those available for all other PIP, C-TPAT, or FAST members.

Without some definition of benefit, a return-on-investment calculation cannot be made. This is not to say the shippers, carriers, or importers are driven solely by profit. But it would be the rare firm that would undertake substantial investment with no defined benefit in return.

- Substantial business effort requires substantial expenditure.

  Because these firms need at least a neutral return on investment on efforts to conform to the network-centric protocol, major investment will require major business sacrifices or setbacks, at least without reimbursement of some sort.

  Responding to this, policy should offer tax credits to approved aspects of the technology retrofitting that private businesses would need in order to implement the network-centric approach. As will be discussed later, and as the Stanford Supply Chain Forum study by Hau Lee and his colleagues described above indicates, such a system will offer commercial advantages for participants. However, government has a key defense role in protecting the supply chain. Expenditures for the private sector may exceed those justified by commercial advantage. Government would participate with nonmonetary (such as expedited clearance) and monetary (such as tax credits) incentives for those outlays required to establish the needed electronic connectivity behind the proposed protocol. This would cover capital expenditures for wireless devices, electronic seals, and logistics software platforms, along with their installation costs and related periodic fees for satellite or GPS uplinks (or possibly fees for terrestrial systems such as CDMA).

This would not cover other operational impacts from retrofitting or process rework to establish electronic connectivity (for instance, it would not cover surveillance cameras, which however helpful in protecting supply chains from terrorist interference, have non-homeland security applications such as to protect inventories for commercial loss purposes).

Tax credits are suggested, as presumably such retrofits already would enjoy deductions as ordinary and necessary business expenditures or as capital expenditures amortizable over their useful life under both Canadian and U.S. laws.

On the other hand, to the degree substantial technology and related investment are available (but not supported by government, via tax credits or otherwise), Canada and the United States create two problems for themselves. First, they risk establishment of a zero-sum game between businesses' perceived self-interest and homeland security. Instead of providing incentive to a particular carrier, shipper, or importer to move toward the most robust protection from terrorist interference of which they are capable, a failure to pay for needed technology and other security tools provides a minimal incentive. They might well cut off creativity that could be applied for our society's benefit.

By asking for robust performance but refusing to shoulder the financial impact, government might well "reward" creative and ambitious responses to protect the logistics infrastructure with added costs and no support of the kind necessary to businesses whose return-on-investment calculations need to support a profitable enterprise.

Second, government failure to financially support logistics security measures, network-centric or otherwise, undercuts the logic of private involvement in homeland security. Firms' financial staffs might well ask, how can a business' security technology expenditure be urged on patriotic or public interest grounds if the government itself, charged with protecting the nation, fails to find that same expenditure compelling enough for its own budget?

- September 11–type physical threats present important liability exposure to those firms whose operations might be subject to such attacks.

  Firms that prove their security up to measurable standards should be provided protection from risk against tort sanctions designed to promote such security and to punish (or reimburse victims for) its absence. The events of September 11 have already changed the landscape as to "war clause" exclusions in insurance, and the U.S. District Court for the Southern District of New York, which is handling tort litigation claims arising out of the tragedy, has issued a ruling that materially enhances the risk to freight participants from a terrorist incident against a supply chain.[65]

  While still not as tangible and current as expedited passage through checkpoints or reimbursement of expenditures, liability protection might

prove a significant inducement to participation in the network-centric protocol. On the other hand, one might guess that by itself, the fear of tort liability in a September 11-type scenario is not sufficient to support substantial investment in the absence of either government support or sufficiently expedited treatment to build a return-on-investment case.

Finally, regarding practical incentives, integration of the supply chain via remote, real-time electronic data gathering and analysis presents both efficiencies and opportunities for customer satisfaction beyond the above. While these have enjoyed some degree of adoption, they have not yet become widespread among shippers, carriers, and recipients of freight.

The connectivity that provides remote, real-time awareness for security purposes can also indicate supply chain events and conditions relating to the following commercially relevant matters:

- Confirmation that goods in transit are in existence and are already in motion;
- Location of such goods, and with this, an estimate of when they would be available to a particular recipient at a particular location;
- Current and future velocity (e.g., seasonal variations on a given railroad, ocean lane, or long-distance truck route can be identified empirically and, with appropriate algorithms, likely transit times inferred);
- Likely arrival times (again, per current and future velocity as stated above);
- Hazards and impediments along the route (for alternative routing and other response); and
- Automated notification to recipients based on items 3 through 5 above, with instructions to enable, either automatically or via manual messaging, a smooth transfer.

Generally stated, the typical loss of control a shipper experiences when freight leaves its loading dock, and the corresponding loss of control by carriers and recipients down the line of the route, would be transformed by an integrated electronic awareness of supply chain events for both security and commercial purposes.

Behavior Issues

What types of incentives are likely to induce the sophisticated and effortful performance needed from the private sector to implement the protocols of the network-centric approach? Or more bluntly, what policy inducements are most likely to elicit the desired performance levels and not to simply prompt passive compliance behaviors?

As to the behavior question, we need to consider both the rewards to which profit-making companies might respond to and the potential for unexpected consequences or outright misuse.

To be successful, a policy designed to promote specific business actions—capital expenditures, possible added operations costs, and in any event, changes in business processes—needs to respond to individual businesses' goals. In free-market economies like Canada and the United States, businesses, of course, exist to make a profit for their owners.

This is not to say that such owners are motivated solely by the prospect of enhanced profit, but they will typically undertake burdens only with this overarching purpose in mind. The network-centric approach calls for change sufficiently substantial that it could affect this purpose.

Policy here requires a realistic outlook of individual firms' return-on-investment calculations in regard to implementing the electronic connectivity and related security protocols of the network-centric approach. Logistics is a business context where pennies per ton-mile are constantly monitored as either cost to shippers or revenue to carriers, and organizational headcounts have been significantly reduced.

As for incentives, this is the point; it may be reasonable to ask companies to take actions that do not add to profits, but expecting they will reduce those profits through material amounts of net additional costs is dubious. Return-on-investment calculations presented to firms' finance offices must at least be neutral, if not positive. In the most practical terms, this goes to where a public-spirited executive within a shipping or carrier firm wants to implement the network-centric approach.

Specifically, what ammunition does he or she need in the meeting with the corporate controller or chief financial officer?

That is on the positive side, where corporate action is aligned in purpose and function with the security goals of deterring terror in supply chains. Negatively, firms might make insincere use of such inducements, either not adding materially to freight security or burdening government spending with technology only tenuously related to the network-centric protocol. Any favored treatment or financial inducement could easily result in businesses "gaming the system."

As with any good government goal, supply chain security could pose an occasion for misuse. As is more fully set forth in the "Recommendations" section below, this can be mitigated as a problem, if not fully eliminated, by narrowly tailoring inducements to the electronic connectivity preconditions of network-centric security that Canada and the United States would seek to bring about.

Specifically, this means that benefits would be directly tied to supply chain security goals and efforts more tenuously connected to security would not be rewarded, at least not by government.

Most importantly, only those costs directly necessary to retrofitting freight loads and other infrastructure with wireless devices, electronic seals, and software platforms would be subject to tax credits or whatever form of benefit is provided for incentive. This would consist of capital expenditure for such devices, seals, and platforms, along with two additional categories. The first would be installation costs, which could be tied directly to such security purposes.

The other noncapital expenditure for which benefit should probably be provided is the periodic service costs for satellite and GPS uplinks (or similar terrestrial systems like CDMA). These relatively expensive services go directly to the remote connectivity of geographically dispersed freight. Inadvertently encouraging private business to stint on these by under funding them would be self-defeating.

Also, a word on the two other categories of inducement recommended here. First, as to expedited passage through ports and border checkpoints, this privilege would be lost and the firm enjoying it sanctioned if conventional customs purposes were evaded. If an otherwise qualifying firm fails to pay duties it owes or if smuggling or drug involvement were indicated, the affected firm would lose the privilege or face other sanctions.

Second, as to protection from tort liability relating to terrorist incidents, the protection would be carefully drawn to impact only those situations where a supply chain has experienced interference due to asymmetric force. Those tort incidents not associated with such terror or instrumentalities associated with it would not be covered. Whatever merits or demerits envisioned in tort reform, the focus on homeland security considerations should be paramount.

Finally, it is likely that operations will be impacted by maintenance and use of such data gathering and analysis tools, prompting additional wage and benefit expenditures as the result of this network-centric protocol. Also, security measures not directly involved but nevertheless a part of the required protocols—such as limited access to facilities, surveillance cameras, vetting of employees' backgrounds, etc.—are illustrative of the additional costs incurred by firms under a more aggressive security protocol.

For behavioral reasons of potential abuse, we should restrict financial incentives to those categories demonstrably directly connected to the electronic connectivity whose implementation is the key to the network-centric approach.

Standards

We need a governance structure for the setting of functional standards and for the process of ascertaining conformity to them. Achieving this is complicated by the divergence between government's institutional primacy in national security and public safety and business' functional primacy in freight operations.

To bridge this gap, we should consider an organizational framework for both standards-setting and audit functions that would be independent of any one government or of any individual company. In that regard, neither the command and control mode of the former, nor the commercial dynamic that drives the latter, would likely, by itself, be adequate to produce the best standards of which current technology is capable or the independence necessary to credibly validate logistics firms' security performances.

Such new governance structures could be established under Canadian and U.S. government auspices but accountable to distinct boards of directors or

similar bodies, each independent from the control of any single government or firm.

The first structure, a functional standards-setting body, could promulgate functional standards required of specific types of businesses such as manufacturers, carriers, or related logistics service providers. These functional standards could be nontechnical in nature, focusing on the type of information output (e.g., data about what? Provided how frequently?) or on the security measures taken by the individual company (e.g., perimeter security specifications, personnel access controls, etc.).

Such a security standards-setting body could produce requirements for specified categories of logistics businesses that would be understandable by operations people competent in the daily business processes of moving freight, but who are not necessarily schooled in engineering or the hard sciences.

The second structure could be another standards-setting group. This could be a technical standards-setting body. As such, it would establish standards of electronic connectivity and related security functions to which individual firms must conform in order to enjoy membership in the network-centric protocol and the corresponding incentives. In contrast to the security-standards body's work, which would likely be understandable by those from general logistics operations or government backgrounds and not necessarily to those in engineering or the hard sciences, this body's work product would be highly technical in nature and likely quite voluminous in its specifications of technical functionality.

Finally, the third structure should consist of an audit arm. It could maintain a staff or manage qualified third parties to conduct periodic validation of individual firms' adherence to the requirements established by the two standards-setting groups described above and report to government and logistics-sector participants on the results of such audits. While there should probably be an appeals process internal to this part of the governance structure, it would be important to insulate the audit structure from outside intervention. In particular, intervention perceived as a response to lobbying would undermine confidence in the system.

Not to put too fine a point on this, but one would want to avoid a system that could be manipulated by the odd telephone call from either Parliament Hill or Capitol Hill to Ottawa ministries or Washington agencies on behalf of particular firms that otherwise might not be passing muster on objective grounds.

Legally, this governance framework could be embodied in a Canadian-U.S. agreement implemented in turn by both parliamentary and congressional legislation. By creating the right governance structures to respond to the new threat, we could create common institutions to link the public and private sectors in both Canada and the United States. Such institutions would bring their own distinctive checks and balances. In this way, we would both maintain the primacy of government authority in securing our respective countries and, at the same time, defer to private businesses' greater expertise in, and operational access to, the logistics system.

The deployment of new technology to integrate otherwise divergent and disconnected security efforts lies at the core of the proposal of a network-centric protocol for the next stage of Canadian and U.S. freight security.

The needed scientific applications—wireless devices, electronic seals, and related logistics software platforms—are largely ready made. Systems integrations within firms or among small collections of businesses have been done many times. True implementation of electronic connectivity would require architecting a common basis for data flow and analysis across whole industries or other large groupings of firms. To the modest extent that some such applications have already been adopted in the logistics system, they relate to individual firms or supply chains made up of a handful of cooperating businesses supplying the lead firm.

Because this effort would be unprecedented in the breadth and depth of its operations, the identification and promulgation of common standards, largely from scratch, would be required.

But the area of standards raises the following substantial issues:

Why Not Let Government Take the Lead?

There are substantial precedents for Ottawa and Washington taking the lead in both standards setting and the confirmation of adherence to those standards. These, like supply chain security, extend to highly technical subject matters largely within the operations and expertise of private enterprise.

Among prominent examples, medical devices and pharmaceuticals are one area and civil aviation is another. Health Canada and the U.S. Food and Drug Administration (U.S. FDA) in the first case, and Transport Canada and the U.S. Federal Aviation Administration (U.S. FAA) in the second, have final word both in the establishment of functional requirements and in the certification that specific product lines and individual units from private industry have met those requirements.

As for the electronic connectivity in logistics operations required for the network-centric approach, Canada and the United States are both actively pursuing some of the applications required. The efforts of the Intelligent Transportation Office of Transport Canada in remote electronic freight reporting and the efforts of the U.S. Department of Transportation's MARAD (marine) testing of electronic seal technology are some examples.

Despite these important efforts, both governments' deep experience lies not in such tests but in national defense in the conventional sense (e.g., policing and border controls). As for the logistics system, the public sector, at least predominantly, acts from outside the logistics system to provide protections to it.

The situations of health technology and aviation cited above are exceptions to this pattern. With limited exceptions, mostly related to research funding, neither Ottawa's nor Washington's ministries and agencies develop new products or conduct basic research in these areas as a core competency.

However, since the early twentieth century, safety oversight of health and civil aviation have been core government functions for both Canada and the United States. The difference for electronic connectivity is this; such health and civil aviation expertise has been built within the public sector over decades, while neither Ottawa nor Washington enjoy any such familiarity with wireless, electronic seal, and logistics software technologies or with the systems integration needed to make them work within a cohesive security framework.

Moreover, this long history has given Health Canada and the U.S. FDA and Transport Canada and the U.S. FAA something more than expertise. These agencies enjoy public confidence for both of their expertise and for their ability to share it with the public with both rigor and independence.

In contrast to historical prestige for national defense and public safety, no government agency in either country enjoys similar prestige and public trust on the subject matters at issue with the network-centric approach. Among agencies like Transport Canada, Canada Border Services Agency, the U.S. Department of Homeland Security (including U.S. CBP), and the U.S. Department of Transportation, there are no bodies with the experience, expertise, or public prestige in logistics software, wireless applications, and related network-centric technologies to set standards in this area.

As a result, we should consider carefully what measures would convince the public of the substantive merit of new standards needed, the objectivity of those pronouncing them, and the effectiveness of validating those standards in the context of specific firms and operations.

Definition of Standards

Policy should identify the results desired and defer to experts in IT, logistics operations, and other relevant disciplines on the content of such standards. The requirements of policy would consist of specifications of the type of electronic connectivity and related security practices integrated in the network-centric protocol.

Therefore, while the actual statement of operational and technical standards would likely be as voluminous as the proverbial telephone book, a statement of desired functionality should be manageable, along the lines of statutory or regulatory-type detail.

In addition to the practical security functionalities required, policy should spell out organizational detail so as to achieve substantive rigor, real-world practicality, and the necessary independence of the auditing body or bodies for their objectivity.

Models here are significant. The International Organization for Standardization (ISO) is a prime example. The ISO develops standards for quality industrial processes of various sorts. While having the specificity sufficient to guide engineers and manufacturers, for instance, ISO standards raise levels of safety, reliability, and interchangeability that are accepted by industrial and business firms, as well as government and other regulatory bodies.[66]

The standards come from committees drawn from the private sector (some composed of general managers and some composed of technical experts), which the ISO convenes for the purpose of standard setting. Both standards and validation procedures are specified this way. This worldwide set of industrial standards is created without government input, though governments, as well as businesses, use this input for decisionmaking.

The ISO is perhaps the most well-known body in the standards-setting area, but it has parallels with more narrowly focused standards-setting groups, including ones more directly related to the movement of goods in commerce. These include firms involved in the secure shipping of high-technology finished goods (TAPA),[67] distribution firms joining together to cooperate in the use of RFID in commercial settings (EPCglobal),[68] and informal groupings of suppliers and large purchasers agreeing to use privately developed common standards.[69]

Each of these models reflects two critical realities.

First, all are designed to avoid situations where one party or faction of firms can overbear the will of objective participants in the setting of standards. Whatever the imperfections or risks of this goal, this is the design and ISO, TAPA, and EPCglobal enjoy reputations for independence from influences that might unduly favor any particular firm for nonsubstantive reasons.

Second, governance is designed in each case to reflect the expertise of representatives drawn from the very industries and operational environments subject to the standards. By drawing talent from the locus of the subject activities, this approach promotes deployment of knowledgeable talent and real-world practicality.

Is This Not Already Underway?

This discussion goes to the creation of standards for supply chain security. In particular, both business-process standards that govern shipper and carrier practices employed to prevent terrorist interference, as well as technology standards that govern performance of RFID, GPS, and software applications used as tools in the network-centric approach.

In the time since September 11, 2001, for instance, the International Maritime Organization has issued rules that touch on maritime business processes (the International Ship and Port Facilities Rules), the International Standards Organization has issued (or, arguably, is still in the process of establishing) technical specifications on electronic seals usable in sea containers and truck trailers (ISO CD 18185), and the World Customs Organization is joining the efforts of 164 customs administrations to enhance post–September 11 cargo security.

But none of these go to the issue of comprehensive supply chain security on a network-centric model. They go to particular aspects of it. That is why government-sponsored organization is critical for standards development when it comes to homeland security requirements in the logistics infrastructure.

Auditing Organizations' Adherence to Standards

The standards set for electronic connectivity, as well as the related security measures being integrated, would only be as good as their auditing and enforcement.

The standards-setting organizations referred to above—and professions like law or accounting that require independence for objectivity, as well as competency criteria to determine a particular firm or operation's adherence to requirements—offer models for organizational frameworks here.

As for ISO, TAPA, and EPCglobal, each have audit functions that are instructive for structuring, staffing, and managing an auditing organization in the area of electronic-connectivity standards for the purpose of supply chain security. Their coverage encompasses the full range of those organizations' standards.

From the perspective aimed more specifically to a proactive testing approach, firms like Huffmaster, Inc. offer so-called "RED Teams" testing that (with a company's authorization) provide an independent means to penetrate security where security concerns go beyond access control to "possible product tampering or sabotage."[70]

As with standards setting, there are ample models in existence for the audit and enforcement of electronic connectivity (and other dependent security measures) in the network-centric approach to protecting the supply chain.

Legal Embodiment

Finally, the formal legal vehicle for implementing this new, longer-term protocol and its standards could be two fold.

First, Canada and the United States could enter into an appropriate form of agreement between themselves pertaining to the policy goal of a complementary combination of the security protocol embodied in present law and practice and the new network-centric approach. Moreover, this model could then be applied to other international groupings—such as the European Union or ASEAN (Association of Southeast Asian Nations).

This agreement might specify the elements of policy recommendations as set forth above. Presumably, standards setting and auditing would need to be uniform between Canada and the United States, but some consideration should be given to how equivalent incentives between Canada and the United States might contribute to smooth implementation. The absence of uniformity might give rise to unintended corporate behaviors in response to disparate treatment, with firms reincorporating on one side of the border in response or allocating incentives-relevant activities in some undesirable way.

Second, Canada and the United States could separately enact appropriate legislation to guide ministerial and agency action in accordance with the policy recommendations. Again, the need for uniformity would seem to be imperative as to standards, with a separate consideration applying to incentives.

Finally, there is the potential for disadvantaging small- and medium-size firms from opting into the network-centric protocol by virtue of their smaller size and possibly lagging technological adoption. The extent of this possible problem is unknown, and the availability of third party logistics firms (3PL's) and other sources of technology external to such firms, while established in providing electronic connectivity for conventional logistics technology, is as yet untried in the area of network-centric security.

Equalizing this situation between smaller and larger firms may require financial-assistance adjustments above and beyond the incentives outline above if 3PL's or other outside sources of technology integration do not arise in the marketplace to fill this need at a cost-affordable price for such small- and medium-size firms.

Concluding Postscript

In mid-2004, the September 11 Commission criticized U.S. agencies for a "failure of imagination" in not adequately anticipating the attacks.[71] Months later, former GE CEO Jack Welch emphasized the "ability to see around corners" in describing the traits needed in the next president of the United States.[72]

Foresight is critical in this climate, and Canada and the United States should assume that Al Qaeda and its counterparts know the operational basics of freight operations and that they have access to digital applications in logistics that for years have been used by industry leaders. While both governments have taken aggressive tactical actions to protect our mutual freight flows from terror in this new threat environment, neither has come to a conclusion on a basic strategy.

On the one hand, we see forceful and decisive action as U.S. CBP commissioner Robert Bonner promises a "Green Lane" policy at ports and borders in return for firms that deploy a "Smart Container" application (alerting of tampering attempts while cargo is en route, along with C-TPAT membership in good standing and the use of Container Security Initiative ports for maritime moves).[73] Further, Commissioner Bonner is spearheading a revised C-TPAT program marked by a new supply chain-wide scope, with rigorous new demands on importers for "a documented and verifiable process for determining risk throughout their supply chain[s]."[74]

On the other hand, Canada's CBSA, under its president, Alain Jolicouer, is receptive, but neither he nor anyone else in Ottawa has yet stated agreement. In Washington, authority for cargo security is dispersed across several agencies both within and without the U.S. Department of Homeland Security. As James Loy, deputy secretary of homeland security, states:

> Everybody right now has pieces of the puzzle. Customs and Border Protection has C-TPAT and CSI [Container Security Initiative]. The Coast Guard has the ISPS Code [port security regulations that took effect July 1, 2004]…We need a national cargo-security strategy that brings all of those pieces together. *We started that*

> *process with the DHS cargo summit last month* (italics supplied).[75]

In the immediate aftermath of the attacks, Canada and the United States did what they had to with the tools they had on hand—resulting in primary reliance on the stop-and-search model, although supplemented with various information-gathering procedures under the heading of "layered" security.

Longer term, we have access to data-gathering and analysis tools that expand our ability to directly observe cargoes beyond checkpoints. (Such observations are now, for the most part, limited.)

Whether we opt for the stop-and-search model or the network-centric one has important implications for both our physical safety and economic stability. The sooner we decide on one over the other, the greater our ability to protect ourselves against possible asymmetric threats hidden within our freight system will be.

Notes

[1] Desmond Morton, "Historical Perspectives on Canada's Asymmetric War" (lecture, York University Conference on Terror and Security in the Aftermath of September 11th, Montréal, Canada, May 14, 2002).
[2] As set forth more fully in footnote 4, reference to "real-time" in this context is not usually going to be achieved in the literal sense.
[3] John C. Tabor, "Supply Chain Security Module" (presentation, Council of Logistics Management 2003 Annual Meeting, Chicago, IL, September 22, 2003).
[4] Reference to "all" times can, in fact, be achieved via currently technology. But those designing systems for electronic data gathering and analysis may opt for something with a less-than-perfect "real time" functionality. It is more likely that such data will be gathered and transmitted in one of two ways. First, using a "batch" process, system designers may opt to store data readings for eventual transmission at scheduled intervals (such as every 15 minutes or every six hours). Or such systems may gather data remotely within the logistics system for response when requested (for instance, company HQ or governmental security office may "ping" a sea container located in a given ship at sea via a combined GPS and localized RFID connection). Either way, the concept is to free cargo security from being limited solely to those occasions when a load and its means of conveyance are located in the immediate physical proximity of a customs or other government agent at a port, border checkpoint, or other location.
[5] Please refer to note 4 for an important qualification to the literal meaning of "real time."
[6] This number is the subject of various claims and estimates, none of which exceeds 10 percent.
[7] U.S. Customs and Border Protection, "Fact Sheet: U.S. Customs and Border Protection—FAST program," http://www.cbp.gov/xp/cgov/newsroom/fact_sheets/fact_sheet_fast1.xml.
[8] Ibid.
[9] Stephen E. Flynn, "The Neglected Home Front," *Foreign Affairs* 83, no. 5 (September/October 2004).
[10] Jonathan Byrnes, "Who Will Profit From Auto-ID?" http://workingknowledge.hbs.edu/item.jhtml?id=3651&t=dispatch.
[11] Michael Wolfe, "Automating Security: A Rationale for Electronic Cargo Seals" (review draft, North River Consulting Group, 2003).
[12] Ibid.
[13] Craig Harmon, "Intermodal Freight" (presentation, MIT Auto-ID Center Conference on Homeland Logistics Security 2003, Chicago, IL, September 18, 2003).
[14] Science Applications International Corporation, "Cargo Handling Cooperative Program: Program Sector: Agile Port and Terminal Systems Technologies: Program element: Cargo,

Equipment Tracking and Identification Technology Demonstrations: Task Title: Container Seal Technologies and Processes, Phase I, Final Report," http://www.marad.dot.gov/publications/E-Seals/E-Seals%20Report_PART%20I.pdf.
[15] Flynn, "The Neglected Home Front."
[16] Craig Harmon, "Logistics Security in the Supply Chain: Strengthening the Link" (presentation, MIT Auto-ID Center Conference on Homeland Logistics Security 2003, Chicago, IL, September 18, 2003).
[17] See MIT Auto-ID Center Web site for these materials from the September 2003 conference.
[18] For another view on possible data categories—in a marine-specific context—see pp. 5–8 in the undated September 2004 report, "Departmental Advisory Committee on Commercial Operations of Customs and Border Protection (COAC), Maritime Transportation Security Act Subcommittee Recommendations to COAC and the U.S. Department of Homeland Security, Deliverable #2: Secure Systems of Intermodal Transportation,"
http://www.apl.com/security/docs/secure_system_001.pdf.
[19] Raymond Gagnon (project director, Operation Safe Commerce–Northeast, and former U.S. marshal for New Hampshire) in discussion with author, September 2003.
[20] Barry Wilkins, "Operation Safe Commerce/Port of Tacoma" (presentation, Council of Logisitics Management 2003 Annual Meeting, Chicago, IL, September 24, 2003); U.S. Department of Transportation, "DOT and Customs Launch 'Operation Save Commerce' Program,"
http://www.dot.gov/affairs/dot10302.htm; and Business Wire, "Unisys Selected for Operation Safe Commerce Project,"
http://www.itsa.org/ITSNEWS.NSF/0/19af51eb506448e185256d5600668a86?OpenDocument.
[21] Gregg M. Ward (vice president, Detroit-Windsor Truck Ferry) in discussion with author, May 2003.
[22] Ibid.
[23] U.S. Department of Transportation, "Port Security Grant DTMA 1G02021, Proof-of-Concept Final Report," March 12, 2003.
[24] Ibid.
[25] Hutchinson Port Holdings, "Sen. Patty Murray and U.S. Government Officials Unveil Real-Time Port Security Initiative in Operation,"
http://www.hph.com.hk/news/news_archive/2003/hph-5feb03.htm.
[26] Strategic Council on Security Technology, "HPH Plans to Extend Smart and Secure Tradelanes to Yantian Port in China to Upgrade Security of U.S.-Bound Container Shipments,"
http://www.scst.info/releases/apr24b_03.html.
[27] Edward McCormick, "E-Seal Operational Test, Phase 2,"http://trac57.trac.washington.edu/tracdb/reports/atb-statusreport.jsp#8; Intelligent Transportation Systems, "WSDOT Intermodal Data Linkage Freight ITS Operational Test Evaluation: Final Report,"
http://www.itsdocs.fhwa.dot.gov/JPODOCS/REPTS_TE/13770.html; and Peter Briglia (program manager, Intelligent Transportation Systems, Washington State Department of Transportation) in discussion with the author, October 2003.
[28] Ibid. and U.S. Trade and Development Agency, "USTDA Director Askey and Secretary of State Powell Promote Transportation Security at APEC Summit,"
http://www.tda.gov/trade/press/Oct20_03.html.
[29] Nick Cartwright (Transport Canada) in discussion with author, February 2005.
[30] Kathleen Conway (director, Office of Interdiction and Security, Office of Field Operations, U.S. CBP) in discussion with author, February 2005.
[31] U.S. Department of Homeland Security, "Advanced Container Security Device: Broad Agency Announcement 04-06,"http://www.hsarpabaa.com/Solicitations/AdvContSecDev_BAA_FINAL_508.pdf.
[32] From 1996 to 2001, the author worked as vice president for a unit of GE Company—GE Rail Services—then a part of GE Capital. In this capacity, he both met and worked with an individual who is now general counsel of GE Infrastructure, parent to GE Security, the unit that markets the GE "smart container" offering. He also worked with various individuals at GE's R&D lab—now called GE Global Technologies, of Niskayuna, NY—regarding wireless logistics technologies. This R&D unit, now GE Global Research Center, contributed intellectual property for these

applications. As for WFI, the author began working for this firm in December as this paper was being finalized by CSIS and the Fraser Institute.
[33] John C. Taylor and Douglas R. Robideaux, "Canada-US Border Cost Impacts and Their Implications for Border Management Security," http://policyresearch.gc.ca/page.asp?pagenm=v6n3_art_10.
[34] Richard Walker, "Insecurity Over E-Seals," *Traffic World* (January 19, 2004), p. 34. Types tested included: "All Seal" from All Seal Tracking (Sweden), "DataSeal" from Hi-G-Tek (Israel), "eSeal" from eLogicity (Singapore), "Mac-Sema + Navilink" from CGM Security Solutions (United States), and "SmartSeal" from Savi Technology (United States).
[35] MIT Auto-ID Center, "Informational Statement: Common Electronic Cargo Seal Protocol," http://www.autoid.org/1_2003%20Documents/Sep/104sc4wg2n0144_HrmnzSt.doc.
[36] Walker, "Insecurity Over E-Seals," p. 34.
[37] A Smart and Secure Tradelanes White Paper, "Phase One Review: Network Visibility: Leveraging Security and Efficiency in Today's Global Supply Chains," http://www.chainlinkresearch.com/parallaxview/whitepapers/SST_PhaseOneReport_Synopsis.pdf.
[38] Ibid.
[39] Demir Barlas, "Wal-Mart's RFID Mandate," http://www.line56.com/articles/default.asp?ArticleID=4710&Keywords=Wal%2DMArt; Jonathan Collins, "The Cost of Wal-Mart's RFID Edict," http://www.rfidjournal.com/article/view/572/1/1/; and Christine Spivey Overby, Chris Charron, and Kate Delhagen, "Wal-Mart's RFID Endorsement: The Tipping Point," http://www.forrester.com/ER/Research/Brief/Excerpt/0,1317,16962,00.html.
[40] Philip Alling, Scott D. Brown, and Edward W. Wolfe, "Compliance Deadlines Loom: Supply Chain Giants Drive Early Adoption of RFID,"http://www.bearstearns.com/bscportal/htmlnew/research/rfid_0104.htm
[41] Ester Shein, "Radio Flier: Wal-Mart Presents its Vendors with an Offer They Can't Refuse," *CFO* (November 2003): 33.
[42] ChainLink Research, "The Tiny Chip that Will Change the World: *SmallSmartFast* and the Wal-Mart Suppliers Meeting," http://www.chainlinkresearch.com/parallaxview/articles/TinyChip_ChangetheWorld.pdf.
[43] Shein, "Radio Flier," 33.
[44] Collins, "Wal-Mart's RFID Edict."
[45] Roma Luciw, "Detroit-Windsor Trade Corridor Clogged, Study Says," *Toronto Globe and Mail*, November 4, 2003.
[46] See note 4 as to the practical meaning of "real-time" in this context.
[47] More specific to security-motivated electronic connectivity and visibility adoptions, the Smart and Secure Tradelanes (SST) program described above reports (at its first phase) benefits amounting to approximately $400 per container load experienced by shippers of "average-value goods." This estimate from Stanford University included "modeling of safety stock and other inventory benefits."
[48] Bradford C. Johnson, "The Wal-Mart Effect," *McKinsey Quarterly*, no. 1 (2002).
[49] Barnaby J. Feder, "Wal-Mart Plan Could Cost Suppliers Millions," *New York Times*, November 10, 2003.
[50] Ibid.
[51] Qualcomm, "Qualcomm Creates Industry Consortium to Provide Direction on Untethered Trailer Asset Management System," http://www.qualcomm.com/press/releases/2003/press1243.html.
[52] A.T. Kearney, "Meeting the Retail RFID Mandate: A Discussion of the Issues Facing the CPG Companies," http://www.atkearney.com/shared_res/pdf/Retail_RFID_S.pdf.
[53] Dexter Roberts, "China: The Next Big Conquest?" *BusinessWeek Online*, October 6, 2003 (subscription required).
[54] Johnson, "The Wal-Mart Effect."
[55] Tony Shallow (coordinator, Environmental Management Committee, Transport Canada) in discussion with author, May 2003.

[56] Government of Canada, "Securing an Open Society: Canada's National Security Policy," http://www.pco-bcp.gc.ca/docs/Publications/NatSecurnat/natsecurnat_e.pdf.
[57] The White House, "The National Security Strategy of the United States of America," http://www.whitehouse.gov/nsc/nss.pdf.
[58] Donald H. Rumsfeld, "Transforming the Military," *Foreign Affairs* 81, no. 3 (May/June 2002).
[59] U.S. House of Representatives, "Intelligence Reform and Terrorism Prevention Act of 2004," http://a255.g.akamaitech.net/7/255/2422/13dec20041150/www.gpoaccess.gov/serialset/creports/pdf/108-796/108-796_intel_reform.pdf.
[60] Ibid. Sec. 4001: "National Strategy for Transportation Security."
[61] U.S. National Security Council, "NSC-68: United States Objectives and Programs for National Security," http://www.fas.org/irp/offdocs/nsc-hst/nsc-68.htm.
[62] Ibid.
[63] Please note discussion below.
[64] ***Point #1: There are Increased Wait Times at the Canada-U.S. Border***
Many shippers and carriers report increased wait times at the Canada-U.S. border since September 11. This factor is now part of conventional planning in managing supply chains between our two countries. For instance, the operations head of a leading third-party automotive logistics firm in the Ontario-Michigan market now recommends keeping additional inventory on both sides of the border to make up for increased wait times. John Taylor, professor of marketing and logistics at Grand Valley State University in Michigan, contends that some trucks previously running four round-trips per day across the Canada-U.S. border now can only do two.

Underscoring this point, a recent Fraser Institute study sought out Canadian exporters with questions of impediments to cross-border trade with the United States. Not surprisingly, 79 percent of survey respondents said export delays increased after September 11. As of mid-2003, 60 percent said that such delays had been increasing over the past 12 months. See Fred McMahon, Matthew Curtis, and Adeola O. Adegoke, *The Unseen Wall: The Fraser Institute's 2003 Trade Survey*, Public Policy Sources (Vancouver: The Fraser Institute, 2003).

Recent anecdotal indications suggest that such border slowdowns continue.

Point #2: Increased Documentation Burdens
Operators cite documentation processing as a major impediment. This is a perennial complaint in trade circles since September 11, 2001. See Bernard Simon, "Wheels of Trade Seize Up at Busiet Border: Bernard Simon on the Problems of Shipping Goods across the US-Canada Frontier, Where Delays are Threatening Competitiveness," *Financial Times*, August 3, 2004.

For instance, in describing Labatt Brewing Co.'s difficulties in maintaining cross-border deliveries, their spokesman said "You see drivers spending time on pre-arrival, where they have to fax documentation about the load. That can translate into missed handoffs, when they are scheduled to meet another truck and problems with terminal operations…."

A Deloitte Touche study released in October 2003 cited border delays as a material setback to the Canadian auto industry.

To compound the documentation burden, by year-end 2003—later extended into 2004—new, additional information submissions entered the picture. The U.S. CBP now requires specific advance manifest information by specified times in advance of imports or exports crossing the border under the Trade Security Act of 2002. Failure to comply risks cargo being blocked at ports and border crossings.

Finally, in regard to documentation processing, the advance manifest rules cited above provide for considerable additional paperwork. While the enabling legislation (the Trade Security Act of 2002) provides that advance manifest data be sent electronically, proposed U.S. CBP rules implementing the statute make an exception for certain truck firms. Specifically, those firms using the "BRASS" and "CAFE" systems may submit written forms and fax them ahead of truck arrivals at border checkpoints. CBP allows papers and faxes because the needed electronic systems are not yet ready. Imagine a significant percentage Canada-U.S. crossings (the rule applies in each direction) each resulting in a separate fax.
[65] United States District Court, Southern District of New York, In RE September 11 Litigation: Opinion and Order Denying Defendant's Motion to Dismiss, Alvin K. Hellerstein, 21 MC 97 (AKH).

[66] International Organization for Standardization, "About ISO: Introduction," http://www.iso.org/iso/en/aboutiso/introduction/index.html.

[67] This private organization was formed in the 1990s by businesses in the electronics and high-technology components industries to develop and audit supply chain security standards. The Technology Asset Protection Association (TAPA) has set forth a security protocol for theft and pilferage purposes. Initially spearheaded by Intel and a handful of electronics components firms, TAPA publishes a detailed protocol of security measures to which TAPA-certified firms must agree to adhere.

The standards relate to perimeter security—circumstances where guards are required and surveillance technology and other issues pertaining to the conditions under which electronics and other high-technology components are shipped and stored en route to customers are monitored. To do business with Intel and other TAPA members, a supplier must agree to adhere to these standards and receive periodic validation by TAPA-certified independent auditors who visit such members' operations, inspect their supply chains, and provide a passing grade.

The TAPA membership list is composed of approximately 50 leading firms in the electronics and high-technology component industry (e.g., HP, Motorola, Lucent, and Gateway).

Finally, establishment of these standards and auditing criteria are transparent to member firms. Changes in such standards or auditing criteria may be suggested and made only through established governance mechanisms, which assure other members are made aware.

[68] Businesses formed this private organization in the late 1990s to develop and then conduct certification and compliance testing for low-cost radio frequency identification devices (RFID) whose placement in or on pallets, boxes, and individual goods provides identification for their tracking, tracing, and inventory management.

Standing for "Electronic Product Code," EPCglobal grew out of a 100-company effort under the aegis of the MIT Auto-ID Center to develop and apply standards in the RFID field (www.epcglobalinc.org). Its practical application is varied. Prominent examples include consumer goods, high-technology components, pharmaceuticals and healthcare products, and government procurement shipments. Typically, RFID "tags"—tiny and relatively inexpensive radio transmitters—can be attached to a pallet, box, or individual good (on either a reusable or disposable basis) and reply passively (there are active variants available as well) to a "reader" that sends out a radio signal.

The sending of a radio signal to such a passive RFID tag elicits a return transmission with the desired data—such as the contents of a case of goods (or a pallet of the same or of a single item). The point is to avoid the need to read labels manually, inspect the containers for their contents, or run a barcode scanner over a barcode marking. If the RFID tag is within the specified footage of the reader, the contents of the pallet, case, or item are automatically transmitted.

As with TAPA, this private organization both sets standards and provides for validation. Also as with TAPA, changes in standards or certification criteria may be made only through governance mechanisms focused on EPCglobal's board of directors.

[69] A growing handful of significant buying entities have issued RFID mandates for their supplier bases in the area of real-time supply chain data provision.

First, Wal-Mart announced requirements that its top specified suppliers be RFID compliant by 2005. This began with its 30 top pharmaceutical suppliers in March 2004 and will extend to all suppliers by the end of 2006. Wal-Mart's total supplier base numbers about 10,000.

Second, in summer 2003, the U.S. Department of Defense announced that it would require RFID compliance for some of its suppliers (the announcement was vague on how many this covered). This was to begin in January 2005 and cover pallets, boxes (cases), and packaging for items requiring a "Unique Identification" (UID). Such RFID tags must be "EPC-compliant." Analysts at Bear, Stearns & Co., Inc. note that the eventual impact of this mandate may exceed that of Wal-Mart. The U.S. Department of Defense has about 43,000 suppliers that may eventually be affected by this.

Third, Metro AG (the large German retailer) announced in January 2004 a wireless inventory-tracking system based on RFID for rollout in November 2004 at 250 stores and 10 warehouses. This will require compliance for 100 of its suppliers, and the names in this category overlap to

some degree with those cited in connection with the Wal-Mart mandate (e.g., Procter & Gamble, Kraft, Gillette, etc.).
[70] Huffmaster, "Huffmaster Introduces: RED Team Services," http://www.huffmaster.com/Redteam.
[71] National Commission on Terrorist Attacks Upon the United States, "The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States: Executive Summary," http://www.9-11commission.gov/report/911Report_Exec.pdf.
[72] Jack Welch, "Five Questions to Ask Before You Pull that Lever," *Wall Street Journal*, October 30, 2004.
[73] Robert C. Bonner, "Remarks by Commissioner Robert C. Bonner, Trade Support Network, Manhattan Beach, California" (speech, Trade Support Network meeting, Manhattan Beach, CA, February 1, 2005).
[74] United States Customs and Border Protection, "C-TPAT Revision: Final Draft: February 11, 2005," http://www.nitl.org/ (available to members only).
[75] R.G. Edmonson, "With James Loy, deputy secretary of homeland security," *Journal of Commerce* (January 24, 2005).

About the Author

Joel Webber is a transportation lawyer with the Chicago-area firm of Couri and Couri. Previously, he spent 12 years in transactional work with aircraft, rail rolling stock, and trucking equipment, followed by investment in businesses involved in logistics software and wireless technology at GE. He was an assistant district attorney in the Manhattan Major Offense Bureau under Robert Morgenthau. He holds a B.A. in philosophy from Wheaton (Illinois) College and a J.D. from the University of Pennsylvania.