



CONTENTS OF THE G-8 SUMMIT ISSUE

The Dynamics of Supply Chain Security.....15

Michael Wolfe¹
North River Consulting Group

There are two themes to this article. First, the rules of the game in international trade are deceptively unstable, hiding the risk of catastrophic economic impacts from the defensive countermeasures taken to ward off terrorist events. Risk management is deficient, both on the public/private and on the macro/micro scales. Most firms are doing too little to prepare themselves to protect their supply chains and their stockholders. Most governments are having a hard time moving beyond business-as-usual in preparing for and mitigating threats.

Second, we are failing to bring market dynamics and incentives to bear in ways that support and enhance supply chain security. By focusing too closely on the security aspects of new technologies and new practices, the security community is undercutting its own goals. Similarly, by trying to force governments to focus on security and stay away from enhancing operating efficiency – which they see as a private responsibility – private firms and their industry associations are increasing the odds that governments will compel them to apply security countermeasures that represent a net drag on productivity and prosperity.

Linking these themes is my conviction that the careful and successful application of new technologies and processes can simultaneously enhance supply chain security, efficiency, and effectiveness – delivering net business benefits that induce shippers and their supply chains to adopt even better security against theft, contraband, and terrorism. As it turns out, the Group of Eight industrialized nations (G-8) can play a role in supply chain security in both the public and private sectors.

Approach

This article focuses primarily on freight and global supply chains, especially ocean freight. Security is not a new concern to supply chain managers. It became an issue even before the

time of the Phoenicians – as soon as human beings began to trade goods beyond the next village or camp. Since September 11, 2001, however, the perception of the stakes has changed. A lot has been done since September 11 to bolster security, more

Unfortunately, the measures taken thus far come nowhere near what is needed to decisively reduce risk and vulnerability in global transportation networks.

in terms of air transportation than surface transportation, and more in terms of passengers than freight. Clearly, though, there have been useful and important moves in terms of global supply chains. Unfortunately, the measures taken thus far come nowhere near what is needed to decisively reduce risk and vulnerability in global transportation networks.

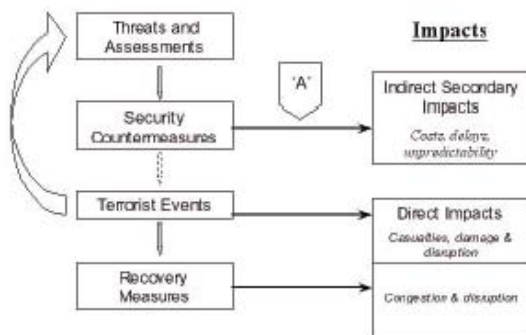
Section I of this article addresses the impacts of security countermeasures in terms of costs and operating practices. It considers factors that compound the economic risks and contribute to supply chain overconfidence. Section II addresses ways to prevent and mitigate the effects of both terrorist attacks and security countermeasures. Section III weighs how the G-8 can at once contribute to the efficacy of security preparations, limit the economic fallout of these preparations, and promote efficiency in global trade.

**Section I:
Impacts and Dynamics of Supply Chain Security²**

Terrorism and the threat of weapons of mass destruction (WMD) have transformed perceptions of supply chain security. Intermodal containers, the ubiquitous facilitators of international commerce, are a potential weapon delivery system, a "poor man's cruise missile." Weapons delivered by freight systems would put at risk large numbers of lives, significant infrastructure, public and business confidence, and ultimately trade and prosperity.

Figure 1 describes the security planning cycle and the impacts of terrorism-related policies and events. In the left-hand column, governments and firms analyze threats and make decisions about countermeasures, some aimed at prevention, some at mitigation. The dotted arrow under "Security Countermeasures" indicates that some terrorist events may happen despite any countermeasures taken beforehand. Successful terrorist attacks should trigger both recovery measures and a classic iterative planning cycle that uses new information to revise assessments, plans, resource allocations, and countermeasures. The feedback loop from successful "Terrorist Events" to "Threats and Assessments" in Figure 1 implies a considered, careful process.

Figure 1: Threats, Countermeasures, and Impacts



Security policies and events produce direct and indirect impacts. Direct impacts arise from terrorist events and recovery measures, including casualties, damage, congestion, and disruption to business and daily life. Direct impacts may be profound, as they were after September 11; but in economic terms, the indirect effects of terrorism dwarf the direct effects.

Security countermeasures produce indirect or secondary impacts that will have important implications because of their geographic breadth, functional scope, and potentially long duration. In addition to negative impacts such as added costs, delays, and unpredictability, positive impacts could follow from countermeasures that both improve security and improve the efficiency or effectiveness of the supply chain. In either case, defenders against terrorism – not the terrorists themselves – generate indirect secondary impacts. Initiators of these secondary effects may be public, private, for-profit, or even volunteer organizations. The actions taken by these initiators could be reactive, as they were when the Bush administration shut down the U.S. aviation system for several days after September 11. They could also be proactive, as in the case of the 24-hour rule that requires detailed cargo data to be submitted to the U.S. Customs Service at least 24 hours before containers are loaded onto a ship bound for a U.S. port.

A phenomenon known as "Wolfe's Paradox" suggests that complex logistics systems incorporating advanced information technology are at once "more robust and more fragile" than their less sophisticated, less efficient forbears. Well-tuned supply chain management systems excel at handling supply or

demand fluctuations within their competence and design capacity. What they cannot do is respond effectively to conditions that far outstrip their normal operating circumstances, such as major spikes in demand – perhaps created by large military deployments – or plunges in supply created by external agents such as significantly tighter, government-imposed security measures. Few if any logistics systems are designed to cope with massive failures of the Internet, telecommunications, GPS, or power supplies. Wolfe's Paradox is a potent factor because most firms operate in several independent yet interwoven supply chains.

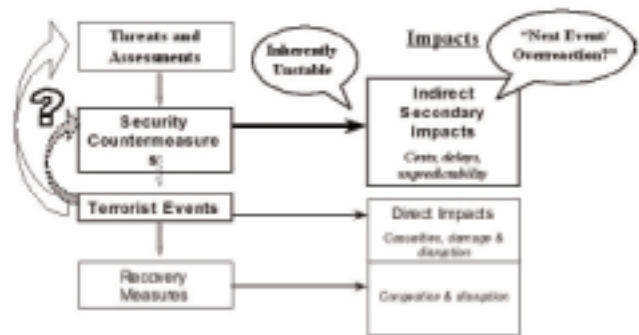
Interdependencies between these supply chains – some of which may not become apparent until a time of crisis – may result in a cascade effect that affects other supply chains and, with surprising speed, leads to widening circles of factories forced to shut down.³

One class of indirect impacts is the cost of traditional security measures – items such as guards, gates, fences, and closed circuit cameras, which simply add costs on top of the normal costs associated with supply chain operation. Such costs represent a burden on productivity.

A second and more interesting class of indirect impacts includes changes to operating practices. These shifts may arise from government actions as well as the strategic decisions taken by firms. These changes include regulatory practices, such as the 24-hour Advanced Manifest Reporting rule mentioned previously or new cargo inspection regimes. In Figure 1, such mandatory security practices are the essence of line "A," the horizontal arrow leading from "Security Countermeasures" to "Indirect Secondary Impacts." These practices are among the rules of the game established by governments for trade, and they are pregnant with potential for self-inflicted wounds.

Figure 2 addresses what may – indeed, what I believe is likely – to happen after a subsequent terrorist attack connected with containers and freight supply chains. The distortion begins on the left, with the gray dotted loop back from "Terrorist Events" directly to the "Security Countermeasures" box. One may ask

Figure 2: Potential for Self-Inflicted Wounds



how rational political leaders from the United States or other nations would be in the aftermath of such an attack. Raw emotion, public demands for action, and political overreaction

could well short-circuit the plan/re-plan cycle, leading to a visceral leap from a terrorist event to draconian security measures intended to ensure such an event "never happens again."

The political essence of the rules of the game renders them inherently unstable. The political culture in the United States tilts toward avoiding the political discomfort associated with proactive measures that could preclude errors ahead of time – and thus toward correcting errors after they happen. We can almost count on political leadership to intervene and stiffen the rules afterward. It is also a safe bet that any new rules imposed in the aftermath of an attack will involve economic impacts far beyond that of a particular terrorist event. There is a risk of disproportionate overreaction – a "next event/overreaction" hypothesis. To take one example, devastating economic impact would result if the government ordered ports and border crossings closed for any meaningful time after a major terrorist attack delivered via the freight transportation system.⁴ To take another, there have already been periodic calls in the U.S. Congress for increasing the level of container security inspection to 100 percent, a 25-fold increase that would seriously disrupt trade. We could inflict economic costs and wounds upon ourselves that far outdo the impact of the terrorists themselves.

Section II: Framework to Address Security Problems

The two classic and complementary approaches to disaster preparedness are prevention and mitigation. In addition to preparing for terrorist events, prevention and mitigation strategies can apply to negative indirect impacts – that is, the negative economic consequences – of security countermeasures. Further, both strategies apply on the macro (public sector) level and the micro (firm and supply chain) level. Figure 3 illustrates this. Cells T-1 to T-4 depict the macro and micro actions we usually think about to preclude terrorist attacks and minimize the effects of attacks that do occur. Cells E-1 to E-4 depict corresponding actions to avoid and reduce the negative economic effects of security countermeasures.

Preventing and Mitigating Attacks

Macro attempts to prevent attacks (T-1) include military, financial, and diplomatic attempts to disrupt if not eliminate terrorist threats. They also include trade-related policies such as the Container Security Initiative (CSI) and the Customs-Trade Partnership Against Terrorism (C-TPAT). Cell T-1 also includes regulatory actions, such as the 24-hour rule, and public R&D projects intended to develop more effective sensors and detection devices.

Micro attempts to prevent attacks (T-2) include actions taken by firms to reduce the vulnerability of the supply chain to attack. Examples include improved fences around facilities, tighter controls over access, protection of information systems, and compliance with regulations requiring (for instance) the use of high-security cargo seals. Firms may take such actions at their own initiative, at the insistence of critical

supply chain partners, or from government mandates.

Figure 3: Approaches to Security Preparedness

		Macro	Micro
Terrorist Events (T)	Prevention	<i>T1</i>	<i>T2</i>
	Mitigation	<i>T3</i>	<i>T4</i>
Indirect Economic Impacts (E)	Prevention	<i>E1</i>	<i>E2</i>
	Mitigation	<i>E3</i>	<i>E4</i>

Macro efforts to mitigate the effect of attacks that do take place (T-3) cover a wide range. They include furnishing state and local emergency response agencies with financial and technical assistance, improving intra-governmental coordination, and helping fund development projects to ease critical infrastructure bottlenecks, such as with the mid-Atlantic railroad network in the United States.

Micro efforts to mitigate attacks (T-4) overlap partially with T-2. For example, attempts to harden facilities usually improve survivability in case of an attack while improving defenses to foil attempted attacks. Other T-4 examples include adding emergency power supplies and generators at important facilities, creating redundant operations centers, and cross training personnel.⁵ Cells T-2 and T-4 are home to what we generally think of as the "added costs of security."

Assurance and control activities are embedded in each of these four cells. Specific activities vary from cell to cell, but both government agencies and firms must monitor activities and supply chain processes to assure that performance remains within acceptable bounds.

Preventing and Mitigating Impacts of Countermeasures

Public-sector activities can simultaneously address preventing and mitigating the negative economic effects of countermeasures (E-1 and E-3). U.S. government policy is clear, since the president and others have explicitly affirmed the importance of maintaining trade and commerce in the face of terrorist threats. More concretely, the C-TPAT program aims to reduce border processing delays and unpredictability for shippers and carriers that certify the use of best security practices. The U.S. Departments of Homeland Security and Transportation sponsor dual-goal demonstrations of new technology electronic seals and satellite monitoring technologies. While their primary purpose is to accelerate progress toward more effective security, these projects also test tools that could improve supply chain visibility and control – offsetting security costs with improved efficiency and customer service.

Micro activities to prevent negative impacts from

countermeasures (E-2) tend to be educational and representational. Most of these activities are directed at government security mandates being developed in T-1. Individual firms and their industry associations do – and should – work actively with government officials and use the media to help officials understand how to achieve better security without impeding commerce.

Micro activities to mitigate impacts of countermeasures (E-4) involve a rich array of supply chain strategies, including the application of lessons from the Total Quality movement. The highest level of activity under E-4 is supply chain redesign to reduce variability and improve security throughout the supply chain, from manufacturing through final distribution. One approach is to enhance redundancy within corporations and supply chains, for example by adjusting material and product sourcing strategies to reduce firms' vulnerability to disruption. Another approach is to apply new technology for automatic identification, monitoring, and control of items and to construct reusable assets such as totes and pallets and transportation conveyances. Risk management and hedging approaches may also be used to protect profitability.

E-4 is the most important arena for those who are concerned with managing supply chains in a business environment that has been distorted by the threat of terrorism. Supply chain managers can take E-4 actions within their firms and together with their supply chain partners. E-4 is the centroid for managing the economic implications of security.

A theme running through all four cells in Figure 3 that are concerned with moderating the economic impacts of countermeasures is that it is crucial to identify and promote security alternatives that enhance supply chain efficiency – or, phrased another way, to identify and promote supply chain productivity alternatives that enhance security. Although there are significant costs to security, the right strategies and tactics can reduce security risks while contributing to productivity and effectiveness. Such strategies include the application of Total Quality Management philosophy and the refinement and adoption of new technologies to improve supply chain visibility and control.

It is in the direct interest of security professionals to promote security solutions that yield traditional business benefits. When this happens, market incentives operate on the side of good security. For example, firms adopt better cargo visibility and control systems because they can increase profits. On the other hand, it is somewhat self-defeating if security professionals concentrate on their regulatory powers to mandate security solutions that produce net costs to shippers and carriers. Such actions engage market incentives against security: The tendency is to oppose, question, and delay the mandates, and even to cheat once they are imposed. For an example, one need only look at the long history of "misdeclarations" on customs forms.⁶

Section III: The Role of the G-8

Leaders of the G-8 nations can help enhance supply chain security both directly and indirectly. They can work to educate their citizens and their governments about the risks reviewed

in this article. They can implement policies and practices that mitigate the tendency towards political overreaction when terrorist attacks do occur. They can address both the E and T cells from Figure 3, by sponsoring policies that enhance the efficiency of the supply chain while cutting down on the threat of terrorism and limiting the ill economic effects of security countermeasures. They can work towards a stable set of rules of the game that strikes a balance between reducing risk and protecting commerce. These measures are all a function of political leadership and will require both vision and stamina on behalf of G-8 leaders.

Some encouraging signs have already come out of various G-8 summits and meetings. At its 2002 summit, for example, the G-8 approved a document outlining "Cooperative G8 Action on Transport Security." The document called on G-8 members to work together on a variety of projects, including:

- Developing and implementing "an improved global container security regime to identify and examine high-risk containers and ensure their intransit integrity."
- Implementing "common standards for electronic customs reporting" and encouraging non-G-8 countries to do the same.
- Supporting the installation of automatic identification systems in certain cargo vessels, and beginning to require ships and ports to upgrade their security plans and personnel.⁷

If adopted and implemented expeditiously, these measures will contribute both to security and to the smooth flow of commercial traffic. A global container security regime would involve better screening and inspecting of containers before they are loaded onto merchant ships – minimizing the risk of security disruptions during and after the voyage. Electronic customs reporting would likewise reduce delays that impair efficiency. While automatic identification systems would add modestly to the transaction costs of global trade, they would also reduce the likelihood that a vessel would be stopped at sea for inspection, and – if done right – could actually yield efficiency benefits. These are the kinds of imaginative solutions that the G-8 nations ought to be pushing at the Sea Island summit and beyond.

1. Michael Wolfe is a Principal of the North River Consulting Group. His main interest is the interplay between supply chain security, intermodal freight system productivity, and tracking technologies. His clients include government agencies, international organizations, private firms, and not-for-profit agencies. He is currently completing a market forecast for smart container technologies. The author appreciates the collaboration of Stanford's Hau Lee in developing some of the ideas in this article, and of the University of Georgia's James Holmes in pulling together the piece with a focus on the G-8.
2. Much of the material in this section is drawn from Michael Wolfe, "Freight Transportation Security and Productivity," U.S. Department of Transportation Website, April 2002, <<http://www.ops.fhwa.dot.gov/freight/intermodal/index.htm>>.
3. Michael Wolfe, "Defense Logistics: From Stovepipes to Focused Logistics, Including a Post-September 11 Epilog," U.S. Department of Transportation Website, December 2001, <<http://www.ops.fhwa.dot.gov/freight/adfrmwrk/index.htm>>.
4. One attendee at a brainstorming session on maritime security held by the Organization for Economic Co-operation and Development estimated that the detonation of a containerized WMD would halt world liner traffic for up to four months because of public demand for more security inspections. "Brainstorming Security," *Traffic World* online, March 18, 2002, <<http://www.trafficworld.com/search/index.asp>>.
5. The Council of Logistics Management published a research report designed to help firms and supply chains prepare for and cope with disasters: Omar Keith Helferich and Robert L. Cook, *Securing the Supply Chain* (Oakbrook, IL: CLM, 2002).
6. For more on these strategies, see Hau Lee and Michael Wolfe, "Supply Chain Security Without Tears," *Supply Chain Management Review*, January 1, 2003, <<http://www.manufacturing.net/scm/index.asp?layout=articleWebzine&articleid=CA278114>>; Michael Wolfe, "Technology to Enhance Freight Transportation Security and Productivity," U.S. Department of Transportation Website, <http://ops.fhwa.dot.gov/freight/publications/security_tech_appx.htm>; Michael Wolfe and Homeland Security Research Corp., "Maritime Smart Container Market Report," forthcoming June 2004; and Michael Wolfe, "Security Must Yield an Economic Benefit," *Journal of Commerce*, December 1, 2003, <<http://www.joc.com>>.
7. Government of Canada, "Cooperative G8 Action on Transport Security," <<http://www.sars.gov.za/csi/docs/G8%20Action%20on%20Transport%20Security.pdf>>. See also "G8 Foreign Ministers Meeting in Paris, May 22-23, 2003," University of Toronto G8 Information Centre Website, <<http://www.g8.utoronto.ca/foreign/fm230503.htm>>.