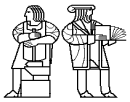

*Massachusetts Institute of Technology*
*Engineering Systems Division*

**Working Paper Series**

**ESD-WP-2003-01.27-*ESD Internal Symposium***

# SUPPLY CHAIN MANAGEMENT UNDER THE THREAT OF INTERNATIONAL TERRORISM

**Yossi Sheffi**
Professor of Engineering Systems
Professor of Civil and Environmental Engineering
Massachusetts Institute of Technology

**MAY 29-30, 2002**

# Supply Chain Management under the Threat of International Terrorism

**Yossi Sheffi**
Professor of Engineering Systems
Professor of Civil and Environmental Engineering
**Massachusetts Institute of Technology**

MIT Center for Transportation and Logistics
Rm 1-235
77 Massachusetts Avenue
Cambridge, MA 02139

This paper was published in the April 2002 issue of the
International Journal of Logistics Management

# Supply Chain Management under the Threat of International Terrorism


## Abstract

On the morning of September 11th, 2001, the United States and the Western world entered into a new era – one in which large scale terrorist acts are to be expected. The impacts of the new era will challenge supply chain managers to adjust relations with suppliers and customers, contend with transportation difficulties and amend inventory management strategies.

This paper looks at the twin corporate challenges of (i) preparing to deal with the aftermath of terrorist attacks and (ii) operating under heightened security. The first challenge involves setting certain operational redundancies. The second means less reliable lead times and less certain demand scenarios. In addition, the paper looks at how companies should organize to meet those challenges efficiently and suggests a new public-private partnership. While the paper is focused on the US, it has worldwide implications.



## Acknowledgements

The author is indebted to Dr. Jim Masters and Mr. Dan Dolgin who provided invaluable insights and detailed comments, including extensive editing. Three anonymous referees also provided helpful comments.

## The Challenge

Within days of the September 11, 2001 terrorist attack, manufacturers began to experience disruptions to the flow of materials into assembly plants. For example, Ford had to idle several of its assembly lines intermittently as trucks loaded with components were delayed at the Canadian and Mexican borders. Toyota came within hours of halting production at its Sequoia SUV plant in Indiana, since a supplier was waiting for steering sensors shipped by air from Germany, but air traffic was shut [1]. Ford, Toyota, and other manufacturers were vulnerable to transportation disruptions because they operate a "Just-in-Time" (JIT) inventory discipline, keeping material on hand for only a few days and sometimes only a few hours of operation.

It is instructive to note that these disruptions were not caused by the attack itself, but rather by the government's response to the attack: closing borders, shutting down air traffic, and evacuating buildings throughout the country. The federal government is now readying its thinking, its institutions, its communications strategy, its military response, and its domestic defense strategy for a challenge of fighting terrorism, that is likely to last a long time.

Popular wisdom repeatedly recites that the war on terrorism is unlike any past war. But popular wisdom has not yet adapted to the most fundamental way in which this "war" is different. In fact, it is not so much a war as it is a new era of continuous danger. In addition, the defensive aspects of this war will be fought on the home front, not by a professional army but by business organizations and ordinary citizens endeavoring to make the interdependencies of our economy function for their own benefit, not as the weapons of the enemy.

As companies organize to face this new era, manufacturers, distributors, retailers and other firms involved in the handling of physical goods face four challenges:

1. Preparing for another attack. Assuming that some future attack will be successful, companies must prepare to operate in its aftermath. Firms are vulnerable not only to attacks on their own assets, but also to attacks on their suppliers, customers, transportation providers, communication lines, and other elements in their eco-system.

2. Managing supply chains under increased uncertainty. Measures taken by the US and other governments to improve homeland defense have burdened the global transportation system, creating longer and less reliable lead times. In addition, even small terrorist events, which have negligible economic consequences in themselves, can have disproportionate effects on demand.

3. Managing relationships with the government. The war on terrorism will bring about a new era of public-private cooperation in which companies will reform

their relationships with the government. All US citizens and business organizations will have a part to play in this war.

4. Organizing to meet the challenge. Actions taken to defend employees, physical assets, and intellectual property will consume resources. Companies must determine what to do, and how to do it in the most efficient manner, balancing the costs and benefits of security needs against other corporate goals.

## Preparing for Another Attack

One of the main tenets of military preparedness is the investment in redundancy, which can hardly be justified on the basis of its positive net present value. Preparedness is best viewed as insurance. We use this framework to analyze investments in three main categories: (i) supplier relationships and awards, (ii) inventory management criteria, and (iii) knowledge and process backup.

### *Supplier relationships*

During the last decade many companies reduced the number of their suppliers, developing "core supplier" programs in order to create stronger relationships with fewer, key suppliers. A counter trend took hold in the late 1990's with the Internet boom. E-procurement tools and services enable companies to conduct on-line auctions and participate in commodity exchanges, expanding the number of firms with whom they do business and decreasing costs.

Security considerations are likely to push more companies to abandon public exchanges in favor of private auctions (where only known and pre-screened suppliers are allowed to participate), or to abandon auctions altogether in favor of long-term relationships with suppliers. In the new era companies may worry that their suppliers will ration their output in case of a disruption. Clearly, suppliers are likely to allocate products first to customers with whom they have long-term relationships, giving this type of relationships added value in the new environment.

Since September 11, many US (as well as European) companies are reconsidering the wisdom of using overseas suppliers. Offshore suppliers may be less expensive, but require longer lead-time and may be more susceptible to disruptions in the transportation system. Local suppliers may be more expensive but are closer and therefore able to respond faster.

Instead of choosing one alternative over another, the best solution may include both – using offshore suppliers for the bulk of the procurement volume while making sure that a local supplier has the capability to fill the needs, by giving it a fraction of the business. In the terminology of insurance, the incremental cost of using the local supplier is the premium paid for the reduced risk of supply-chain disruption.

Consider the following example: a high technology company sells medical devices made by a contract manufacturer in Malaysia. The Malaysian supplier delivers the devices at $100 a piece and the devices are sold by the US company at $400 each. Fixed costs, including marketing and channel setup, have been estimated at $200 per device. Thus, the company expects a profit of:

$$P_1 = \$400 - \$100 - \$200 = \$100 \text{ per device.}$$

The company estimates that there is a 1% probability that the Malaysian supplier will be disrupted and will not be able to deliver for an extended period. This will expose the company to $200 loss per device since in case of a disruption the company will have no sales but will still be burdened with the fixed costs. Taking this into account, the expected profit when using the Malaysian supplier is:

$$P_2 = 0.99*(\$400 - \$100) - \$200 = \$97 \text{ per device,}$$

A local supplier can deliver the same devices for $150 each. Under a dual supply arrangement the local supplier may be given a portion, say 20% of the business if it guarantees to supply all of the company's requirements should the need arise. If there is no disruption, then, the expected profit when using dual manufacturing will be:

$$P_3 = \$400 - (0.8*\$100 + 0.2*\$150) - \$200 = \$90 \text{ per device}$$

If there is a disruption, the local manufacturer will supply the devices and the company's profit will be:

$$P_4 = \$400 - \$150 - \$200 = \$50 \text{ per device}$$

Taking into account, however, that in case of a disruption the company will be able to use the local supplier, the expected profit when operating with dual suppliers is:

$$P_5 = 0.99* P_3 + 0.01* P_4 = \$89.6 \text{ per device}$$

Dual manufacturing will cost the company $7.4 per device ($P_2 - P_5$) in expected profit. This is the insurance premium. The value of the insurance is that if a disruption does occur, the company will experience a profit of $50 instead of a loss of $200 per device.

This simple example ignores the time value of money, possible penalties for not delivering and many other aspects of reality. It demonstrates, however, the value of purchasing the insurance.

Thus, one can expect some jobs to be moving back into the US, as companies trade off lower parts costs against delivery reliability. This shift, however, is likely to be neither large nor immediate. It is unlikely that companies will forgo the benefits of low cost, high quality offshore manufacturing altogether, but rather will only hedge their bets with local suppliers. Calculation of the insurance value depends largely on assessment of the

probability of a disruptive event. Even after a decision to dual-source is made, it will take time since sourcing decisions are often made several years in advance of product launch. The first signs of such strategies should be seen in the high technology sector with its short product life cycle and traditionally high reliance on offshore contract manufacturing.

Note that dual supply sources are not a new idea and they have general merits beyond responding to terror. For example, Billington and Johnson [2] describe how Hewlett Packard has used "dual response manufacturing" to supply inkjet printers to North America for several years. It used a Vancouver, Washington supplier to launch the product and deal with demand peaks, while a low cost Singaporean supplier handled most of the stable production.

## *Inventory*

In response to the terrorist attack of September 11, companies began to question the wisdom of "lean operations" using JIT processes. Some companies are ordering parts in larger quantities, increasing safety stocks to keep their assembly lines moving "just in case" their inbound transportation is disrupted. In addition, they plan to keep more finished goods on hand so customers can be supplied even when the manufacturing process is disrupted.

The benefits of JIT manufacturing, however, have been immense. Manufacturers not only have seen their inventory carrying costs go down -- even more importantly, they have seen their *product quality* improve dramatically. With a JIT system, component quality problems are apparent and must be resolved. This discipline is one of the underlying principles of the Toyota Manufacturing System, which has been adopted, in one form or another, by leading manufacturers in every industry.

The challenge then is to ensure that supply lines are maintained while not incurring the high costs of extra inventory. A possible solution, which can again be analyzed by using the insurance framework, is to separate the normal business uncertainties from the risk associated with another possible terrorist attack, creating, in fact, a "dual inventory" system. Under this system, typical forecasting discrepancies and business fluctuations should be covered by conventional safety stock.

To mitigate the effect of another terrorist attack, however, manufacturers should maintain an additional inventory designated "Strategic Emergency Stock." This stock is not used to buffer day-to-day fluctuations. It can only be used in the case of an extreme disruption. The costs of carrying this extra inventory represent the price of the premium for the insurance it buys.

It is unreasonable to expect managers to ignore this inventory when a service failure takes place in normal times. To make sure that the organization will not simply become accustomed to the higher level of inventory, two policies should be adopted: First, the strategic inventory should be replenished immediately in a "Sell-One-Store-One (SoSo)"

discipline regardless of daily forecasts. Second, usage of the strategic inventory should be treated in the same way that assembly line shutdowns are treated. In other words, it should get top management attention and the root causes fixed at the source.

The concept of Strategic Emergency Stock is similar to the philosophy that led the US to keep Strategic Oil Reserves, which are intended to buffer the US against a severe disruption in the flow of oil. When these reserves have been used to moderate oil price spikes, they have been promptly replenished in order to maintain their availability for their primary purpose. A similar "strategic inventory" of certain key medicines is kept by hospitals for use in crisis situations.

## *Knowledge Backup*

The preparations involved in protecting companies' knowledge involve three main efforts: (i) developing backup processes (ii) backing up the company's knowledge, and (iii) backing up the company's relationships.

Many companies have long understood their total reliance on their information technology infrastructure and have established backup sites for their critical hardware, software applications, and data

Consider, for example Solomon Smith Barney. The financial services firm had 7,000 workers in the World Trade Center, all of whom, fortunately, got out in time. The company was up and running within twelve hours using a backup New Jersey site and invoking a set of emergency backup processes.

Few companies, however, have backup emergency business processes. Such processes spell out communications protocols, chains of authority, and decision-making procedures in case of damage to systems, losses in personnel and breakdown in communications.

More generally, the most precious resource of nearly every company is the knowledge of its workers. Since companies cannot afford to maintain redundant employees around "just in case," companies should insure that their knowledge is backed up. This means that critical processes should be documented and that these documents are available. When appropriate, cross training should be part of any preparedness effort.

Many companies document business processes when they are designed, but fail to keep up with their ever-changing nature as these processes mutate in actual use. This failure may be the impetus for a much better set of software applications, which support both the processes and their continuous documentation.

In addition to business processes, companies need to be able to salvage customer and supplier relationships. These can be protected if all interactions with customers have been documented in a Customer Relationship Management (CRM) system. Relationships should be deemed just as important as data and processes. Documenting all customer interactions can help companies pick up after a disaster much quicker.

* * *

All of these backup activities are a form of insurance premium. Not every preparedness action, however, imposes a premium. Some strategies are beneficial to the business at any time but take on extra significance when looked upon from the perspective of preparedness. One such notion is standardization. One of the most important tools in creating redundancy and the ability to recover quickly is standardization of business processes and practices across the enterprise. To this end, corporations with several warehouse management systems, multiple order entry systems, or several incompatible manufacturing and financial systems, are more vulnerable than companies who standardized their operations and can move personnel and processes between locations if a single location goes down.

## Managing Supply Chains Under Increased Uncertainty

Manufacturing supply chains involve a network of enterprises and processes, which turn a combination of raw materials into finished products delivered to the consumer. Most anti-terrorist measures will reduce the reliability of the network, challenging supply chain management processes.

Longer supply lines and system uncertainties are not new problems for supply chain managers. The globalization of manufacturing, the explosion of new products, and shortened product life cycles have burdened logistics managers with long supply lines and significant demand uncertainty. In that sense, the new era does not represent a fundamentally new challenge. Thus, the basic problem can be tackled by refocusing on known solutions, including (i) improvements in shipment visibility, (ii) improved collaboration between trading partners and across enterprises, and (iii) better forecasting through risk pooling methods.

### *Shipment Visibility*

Many logistics managers still describe their transportation system as a “black hole” – shipments disappear when tendered to the carrier and no information is available to either shipper or consignee until the shipment is delivered. Shipment visibility tools allow shippers to track the progress of their shipments in the same way that consumers can track the flow of their UPS or FedEx shipments. Tracking industrial shipments has proved to be a significantly more challenging problem – it involves multiple carriers and “hand-offs,” and it requires integration with manufacturing, inventory and purchasing. Furthermore logistics managers deal with thousands of items every day and they need to know not only what is in-transit, but also what is available in stock, what is on-order, and when orders will be available from suppliers.

Shipment data visibility allows manufacturers to avoid plant shutdown due to part shortages and allows retailers to avoid turning customers away due to unavailability of goods. At the same time, good visibility also allows all the players in the supply chain to keep lower safety stocks since the demand pattern they experience will be more stable and their suppliers will be more consistent. The cost savings associated with better forecasting and smoother operations include not only lower inventory carrying costs, and the avoidance of expedited shipments; it also means that warehousing facilities can be downsized and a significant amount of administrative overhead associated with unscheduled activities can be avoided.

There are several partial technology solutions available today for helping shippers find out where their shipments are, as well as helping them decide what action to take in case a shipment is late, misrouted, damaged, or otherwise in trouble. Some of these solutions are available from carriers who are tracking their own conveyance movements, while others are available from software providers who are attempting to aggregate the information from many carriers, suppliers and their own warehouses and present it to shippers in an integrated fashion.

To date, most shipment tracking information is based on following the conveyance that a shipment is using or the shipment's location and status. Accurate tracking depends on timely reporting from the carriers hauling the shipment, the warehouseman storing it, or the distributor handling it. This is true for all short-range technologies (including all bar codes and RF devices). New technology using tags which can communicate directly with low-earth-orbiting-satellite (LEOS) systems offers the promise of freeing consignees from their reliance on carriers and other suppliers by allowing direct communications with the shipment.

As lead times are becoming longer and less consistent, shippers should mitigate the problem by investing in visibility tools. Even in cases in which these tools provide only a partial coverage, they help moderate the problems by allowing timely responses.

## *Improved Collaboration*

The focus of supply chain management is on interactions between enterprises in the chain. Collaboration among enterprises is what integrates the supply chain.

Since the mid 1980s, American companies have devised many cooperative schemes to improve supply chain coordination. These include vendor-managed-inventory (VMI) and co-managed inventory (CMI) in the retail industry, efficient consumer response (ECR) in the grocery industry, quick response (QR) in the textile industry, just-in-time (JIT) in manufacturing, and JIT II in high-technology procurement. Lately, collaborative planning, forecasting and replenishment (CPFR) is taking hold in the consumer packaged goods industry and collaborative transportation management (CTM) is under development for the transportation industry. These and dozens of other such initiatives are aimed at ensuring that trading partners share information and coordinate forecasts and

replenishment orders, thus avoiding the unnecessary inventory fluctuations, often referred to as the "bullwhip" effect, which arise from uncoordinated channel decisions. (The bullwhip effect is described by Lee et al [3], based on Sterman [4] and [5] and on Forrester [6].)

The Internet and electronic commerce in particular have enabled new collaborative processes between companies with the development of new standards, which allow more flexible and general computer-to-computer communications. New application software hosted by third party providers allows many trading partners to access their collaborative data simultaneously.

As lead times are becoming more variable and forecasts less certain, companies should redouble their collaboration efforts. When the consignee knows about a problem early enough, it can take corrective measures (expedite shipment, go to an alternative source, adjust its own customer's expectations, etc.)

In addition to collaborating to improve supply chain performance, companies should work both with trading partners and with industry groups to develop best security practices and share growing expertise. More than ever, corporations should realize that their long-term fate is intertwined with that of their suppliers, customers, and even their competitors. Such collaboration has many precedents and is not limited to collaboration among US companies. For example, when the supremacy of the lean manufacturing and JIT became apparent, leading Japanese manufacturers, such as Toyota, allowed researchers from the world over to study their methods. In addition, they allowed other companies, including competitors, to visit their plants and study their manufacturing systems. (See, for example, Womack et al [7].) This is an example of the level of collaboration that will be required in the coming era.

## *Risk Pooling*

One of the fundamentals of forecasting is that forecasts of more aggregate phenomena are more accurate. For example, forecasts of nationwide sales figures are more accurate than store level forecasts and monthly forecasts are more accurate than daily forecasts. To take advantage of this, firms employ a variety of strategies such as:

- Postponement. By delaying the decision to make, configure, label, or ship a product to a particular destination, companies can reduce their forecasting error.

  For example, Billington and Johnson (2000) report that Hewlett-Packard cut printer supply costs by 25 percent with modular design and postponement. Generic printers are shipped to distribution centers worldwide, where local customization (involving local transformers, power cords, and instruction manuals in local language) takes place once firm orders are at hand. Thus, HP forecasts the aggregate demand for the generic printer, while requiring a disaggregate forecast

only for the local parts which are less expensive to stock and can be acquired with short lead-times.

- Build-to-order. The ultimate postponement strategy is to build items only after customer orders are known. Dell Computer has used this strategy to become the world's dominant PC maker. But even automobile manufacturers are embracing the strategy. For example, VW now delivers many of its models to German customers within two weeks of ordering. This means that VW has very few cars waiting for sale in dealers' showrooms.

- Product variability reduction. Some manufacturers have combated forecasting difficulties by reducing the number of options and items they offer. For example, many automobile manufacturers stopped offering all possible combination of features on their products and put forward "packages" of features instead. The smaller number of options allows for better risk pooling, lower variability and thus better forecasts and lower overall costs.

- Centralized inventory management. By managing inventory centrally, companies can use surpluses in one area of the country to cover for deficits in others. This is another example of risk pooling by geographical aggregation. Thus the trend towards reducing the number of warehouses and other inventory stocking locations may accelerate as part of companies' learning to operate in even more uncertain times.

## Public-Private partnership

US executives often look at many government functions as hindrance to the smooth operation of the economy. Defense, however, is one of the few roles virtually no one wants the government to leave undone. In fact, the creation of an Army and a Navy were contemplated in the US constitution itself.

The US government has taken the first step in organizing for the new environment by establishing the Office of Homeland Defense. At this point, the office is charged with coordinating the efforts of the various defense, intelligence, emergency response, health services and related agencies. The challenge is enormous, but the government is slowly rising to meet it. Protecting private interests, however vital to the nation, is still the purview of the owners of those private assets.

### *Sharing information*

Recognizing the important role that government will play in the new era, and recognizing that government cannot do it alone, corporate executives need to start considering the government, both federal and local, as a partner in corporate life. Some possible collaborative avenues include the following:

- Use of the vast government know-how on the nature of threats and ways to deal with them. At the same time, corporations who may be subject to attacks have an obligation to inform local law enforcement and rescue agencies about their vulnerabilities. Companies in particularly sensitive businesses, such as nuclear power generation and chemical manufacturing are already subject to laws that require them to do so. In the new era, corporate executives should consider possible threats and work with local authorities even when they are not legally obligated to do so.

- Many American corporations have operations all over the world and may possess information that is important to the national defense. Following the Cold War tradition, many corporations and individual executives may increase the level of information sharing with the US government.

## *Assuming security roles and responsibilities*

The US has started to settle into a new long-term reality. This reality is marked by added security costs, added administrative costs, and longer, as well as less certain transportation times. Currently, however, the nation has not yet developed new long-term procedures that will be necessary to deal with the threats efficiently. The delays shippers and carriers experience today will be reduced as the US develops a more sustainable security system. Thus, firms should not yet over react to current transportation delays and added administrative costs.

At this point, the philosophy behind cargo security checks mirrors airport checks in the US – inefficient and not very effective. By and large, US checkers at airports give the same level of attention to every passenger who goes through the system. In contrast, leading airports in Europe and Israel have always used an advanced “profiling” system to pre-screen, conduct quick interviews and then check more thoroughly certain passengers, while letting others go through.

Similarly, many of the current processes used to insure the security of freight flows are inefficient and do not “scale” up. The cost of stopping and checking all trucks at the Mexican or Canadian border or at a city's limits is unsustainably high.

The freight equivalent of “profiling” is the use of certified carriers and shippers. Current government efforts are aimed at carriers with whom cargo liability lies. These carriers will have to be certified, based on training and a prescribed set of security processes. In addition, shippers should be certified as well for having approved security processes in place. Thus, for example, trucks owned by “certified carriers” hauling shipments from “certified shippers” may be waved through check-points (or just spot-checked). The idea of certifying the source (warehouse, plant, etc.) where a shipment is packaged is foreign to current regulations, which are aimed at carriers. As US businesses have learned from the quality movement, however, acting at the source can be both more efficient and more effective.

A version of this idea is included in FAA Directive 108-01-10 and its more recent "Cargo Revised Emergence Amendment." The FAA attempts to distinguish between "known shippers" and "unknown shippers" in setting up procedures for acceptance of cargo by air carriers. The FAA does not address carrier certification since it is already familiar with all the air carriers. The problem of certifying carriers is most acute in the trucking industry.

Corporations will take upon themselves some of the burdens of providing security. Shippers will be responsible for checking and sealing trailers at the origin, as well as checking the background of their transportation managers and warehouse and dockworkers. Carriers will develop security procedures for routing and scheduling sensitive cargo and check the background of all their employees. In addition, certified carriers will have the ability to track each of their vehicles at any point in its journey and be automatically alerted if the journey pattern changes.

Leading carriers and shippers should work with the government on the creation of the certification program. Such certification programs are similar in nature to the ISO 9000 programs used to certify quality. In fact, the government may choose to relegate the certification to private organizations, creating a structure similar to the quality programs.

Interestingly, US Customs Commissioner Robert Bonner laid out a vision of a similar system in a speech at an importers conference on November 27, 2001. He suggested a government security certification program similar to the ISO 9000 quality certification process. Companies will be able to use a "fast lane" to enter the US if, for example, they will have certifiably secure processes at their loading docks and their offshore suppliers plants, if they share the cargo information with the customs service in a timely fashion, if they use electronic seals on their containers, etc. [8].

## *Hazardous materials*

More than 800,000 hazardous materials shipments move every day in the US alone, 94% of which are moved by truck. The transportation of hazardous materials deserves special attention in the fight against terror. The main elements of the existing system are:

- The Emergency Planning and Community Right-to-Know Act require that detailed information about hazardous substances in or near communities be available at the public's request.

- The U.S. Department of Transportation employs a labeling and placarding system for identifying the types of hazardous materials that are transported along the nation's highways, railways, and waterways. This system enables local emergency officials to identify the nature and potential health threat of chemicals being transported.

- In 1986, Congress passed the Superfund Amendments and Reauthorization Act (SARA) of 1986. Title III requires that each community establish a Local Emergency

Planning Committee (LEPC) to be responsible for developing an emergency plan for preparing for and responding to chemical emergencies in that community. The LEPC is required to review, test, and update the plan each year.

The systems that are in place are aimed at efficient response to an accident involving hazardous material. Proposed new legislation increases fines for non-compliance and strengthens the US Department of Transportation inspectors' authority to inspect cargo in transit. Separate legislation is aimed at tightening the rules for obtaining commercial drivers' licenses.

These legislative moves are appropriate and timely. The threat of terrorism calls for further control of the movements of hazardous materials so that the authorities can react after a trailer-load or a rail car loaded with hazardous materials is reported missing but before it is used in a terrorist attack. To this end the US may create a "HazMat Transportation Control System" similar to the air traffic control. Before trucks or rail cars will be allowed to depart they will file a "flight plan" and then be tracked to that plan throughout their journey. Deviations from the plan can be checked.

### *Direct Emergency Assistance*

Modern, large corporations have access to extensive resources, which in many cases rival public resources. Some of these resources may have to be used as part of the homeland defense effort during wartime.

This idea is not new; for example, US sealift strategy includes the use of the Merchant Marine fleet in case of war according to the Merchant Marine Act of 1936. The Civil Reserve Air Fleet (CRAF) was similarly established to organize civilian airliners to augment regular military airlift capability in a military emergency.

Corporations should get ready to join in the national defense and in the rescue and recovery efforts that will follow. The corporate function that can provide the most help is logistics and transportation management. Logistics professionals should organize in every area of the US to prepare and help FEMA, the Red Cross and other agencies charged with alleviating emergencies and rebuilding affected communities. Most of these preparedness efforts involve the creation of local databases regarding the availability of transportation capacity to haul people and materiel; heavy earth moving and construction equipment; warehouse space and shipping and handling equipment; computers and communication hardware; etc.

## Organizing to meet the Challenge

Many of the actions required for security and preparedness are in conflict with traditional corporate goals and processes. Consider, for example, the following trade-offs:

- Repeatability vs. unpredictability. In order to be successful and reduce the cost of performing their everyday activities, companies establish repeatable processes. Doing the same task over and over again means that workers get good at it, it is easy to measure and "perfect," and easy to manage. In fact, when processes differ from the norm, companies generate another process to deal with exceptions – in an attempt to standardize even the outliers.

  Many aspects of security, however, require that companies be less predictable. For example, daily changes to the route that a truck carrying hazardous material is using, or frequent changes to password systems and other entry control systems to computers and facilities increases security.

- The lowest bidder vs. the known supplier. To enhance security, companies may choose to deal with fewer suppliers on a long-term basis (as mentioned in the section Supplier relationships), but there might be substantial costs incurred in doing so. New suppliers often offer more competitive prices and they may bring with them new ideas and innovative processes. The same rationale applies to the choice of local vs. overseas suppliers discussed in that section.

- Centralization vs. dispersion. In order to pool the forecasting risk, companies should manage inventory centrally (see the Inventory section). Indeed, many corporate activities, from the provision of information technology to office work, are conducted better in a central location. Security considerations, however, call for dispersion of both assets and personnel in order to mitigate the effect of any local terrorist attack.

- Managing risk vs. delivering value. The costs associated with new security measures are likely to be significant. The success of such measures cannot be measured by the value they deliver to customers, employees or shareholders day in and day out. Instead, these measures will be most successful if they are never actually tested. Consequently, it will be difficult to keep vigilant and keep investing in assets, personnel, inventory and processes that do not deliver value in the short term.

- Collaboration vs. secrecy. Increased collaboration among enterprises makes supply chain management more efficient and avoids some of the increased costs of longer and less certain lead times and demand patterns (see the section *Improved Collaboration*). One of the tenets of security, however, is secrecy. While corporations may be exposing more of their data and internal workings to others and even sharing information about security measures with other corporations, they have to do so without compromising security.

- Redundancy vs. efficiency. The preparatory steps that corporations may be taking regarding procurement policies, inventory management and knowledge backup (see the section *Preparing for Another Attack*), involve the creation of

redundancies in the system – be it extra supplier capacity, extra inventory, backup equipment and processes, etc. Such redundancies are, by their very nature, in direct conflict with "lean operations." Redundancy calls for a "just in case" mentality while modern operations are organized around "just in time" systems. As argued in at the end of this section, the challenge in creating the required redundancies is to minimize their adverse effects and possibly, use them to create value.

- Government cooperation vs. direct shareholder value. Many US executives are conditioned to put near-term shareholder value above all other considerations. The new environment may require cooperation with government and other companies, including competitors, even at the expense of short-term profit and near-term shareholder value.

Just as the US has created an Office of Homeland Security, companies will often find it necessary to create a new office headed by a "Chief Security Officer" (CSO). The CSO must be, first and foremost, a *businessperson* who is familiar with the enterprise and in getting things done in a corporate environment. Organizations, perhaps like individuals, are subject to a strong temptation to return to normalcy. They gravitate toward return to the days when nobody had to worry about terrorism and bio-attacks. The CSO and the security organization will have to continuously fight this temptation. They will face many of the trade-offs mentioned above on a daily basis, and will have to create the constituency to follow through with the required investments and changes to corporate life. Military or law enforcement background may not be the right mix for CSO candidates. Outsiders may be quickly marginalized in a corporate environment, unless they can understand the business itself and the trade-offs it routinely makes and argue for just the required measures and no more, while taking into account the normal business mission and objectives.

The CSO should be the place in the organization where the various security schemes will be coordinated and tested, making sure that the enterprise can continue after an attack and that the emergency processes complement each other. For example, while it is clear that dispersion of work and personnel is a reasonable strategy to contain damage from physical terrorist attack, this strategy makes the enterprise more vulnerable to an Internet virus or worm attack that will impede communications and distributed applications.

Another major business-preparedness role, which the CSO office should coordinate, is the use of simulation and optimization models to test various scenarios. Such models are readily available and can be adapted to contingency planning in terms of operating partial networks, using different ports of entry, responding to massively different demand scenarios, and adapting warehousing strategies to changing conditions.

The CSO's task, however, is much bigger than establishing and testing contingency plans. No Chief Security Officer or security organization will be successful unless the culture of the enterprise adds security consciousness to its daily life. Thus, companies

that will best survive terrorist attacks will be those whose employees have internalized a set of intelligent applications of security measures and the needed backup emergency processes. In that sense, the security challenge is similar to the drive to create a sales culture during the 1970s and the quality challenge of the 1980s.

Efforts aimed at security can actually improve corporate performance and the preparation should be put in place with an eye towards reaping such "collateral benefits." For example, better security measures can help reduce theft, embezzlement, and loss of intellectual property. They can help cement relationships with trading partners and accelerate the work of standard-setting organizations. Participation in community-wide efforts can also help the corporate image. Beyond the image, however, such efforts can empower employees and inject new meaning to their jobs, as strong corporations will be seen not only as a source of economic security to individuals but also as contributors to the greater good of the nation.

## Summary and Conclusions

Terror is not a new world phenomenon and the US itself was no stranger to either suicide bombing or terrorist plots or attacks, especially in the last decade. The September 11 attack demonstrated, however, the magnitude of the struggle in the new era and its far-reaching dimensions.

While European governments are in support of the US war on terrorism, it is the US that is the target of the current wave of terrorism and it is the US who is leading the charge against it, thereby exposing itself to retaliations.

This struggle will challenge not only the armed forces of the US and its intelligence and law enforcement institutions, but it will change the way citizens in the Western world lead their lives and the way corporations conduct their business. This paper had focused on the last point – getting back to business in the new environment: cooperating with the government and adding security measures in order to prevent new attacks from taking place; creating redundancies so that enterprises can withstand such attacks; and changing corporate processes to cope with the heightened security environment.

## References:

[1] Wall Street Journal "As Security Worries Intensify, Companies See Efficiencies Erode,", Ip, G., ***WSJ*** p. 1, Sep 24 (2001)

[2] Billington, C. and B. Johnson "Creating and Leveraging Options in the High Technology Supply Chain," ***Journal of Applied Corporate Finance***, Forthcoming

[3] Lee, H., P. Padmanabhan, and S. Whang, "The Paralyzing Curse of the Bullwhip Effect in a Supply Chain," ***Sloan Management Review***, Spring (1997), pp. 93-102.

[4] Sterman, J.D. "Modeling Managerial Behavior: Misperceptions of Feedback in a Dynamic Decision Making Experiment," ***Management Science***, Vol. 35, No. 3, (1989), pp. 321-339.

[5] Sterman, J.D., "Misperceptions of Feedback in Dynamic Decision Making," ***Organizational Behavior and Human Decision Sciences***, Vol. 43, No. 3, (1989b), pp.301-335.

[6] Forrester, J.W., "Industrial Dynamics: A Major Breakthrough for Decision Makers," ***Harvard Business Review***, Vol. 36, No. 4, (1958), pp. 37-66.

[7] Womack J., D. Jones and D. Roos ***The Machine that Changed the World: The Story of Lean Production***, Rawson Associates Press, (1990).

[8] O'Reiley, J., "Under Pressure," ***Inbound Logistics*** October 2001, (2001), pp. 62 - 65