Supply chains and terrorism

Yossi Sheffi
Professor of Civil and Environmental Engineering

Abstract

On the morning of September 11th, 2001 the United States and the Western world entered a new era – one in which indiscriminate terrorist acts of all kinds must be expected. Many, if not most, of the expected consequences of the new era will be reflected in supply chain management challenges: relations with suppliers and customers, transportation difficulties and revised inventory management strategies.

This article looks at the twin corporate challenges of preparing for new terrorist attacks, and of operating under heightened security resulting in less reliable lead times and less certain demand scenarios. In addition it looks at how companies should organize to meet those challenges efficiently and the new role that public-private partnerships are likely to play.

To prepare for terrorist attacks, firms should revise their inventory management posture and keep strategic inventory on hand. This does not mean that they should abandon just-in-time principles since JIT brought about better quality, higher accountability and better productivity, in addition to reduction in inventory carrying cots. Instead, firms should manage the strategic inventory in a JIT fashion. Similarly, firms should not abandon offshore procurement. Instead, they should organize to run dual procurement systems where the bulk of the material is bought from inexpensive and innovative offshore suppliers, and at the same time, a portion of the business is given to a local supplier who can pick up the slack in case an attack disrupts transportation lanes. Both of these examples can be analyzed in the context of real options where the dual supplier or the extra inventory buys the firm the ability to continue manufacturing after an attack.

To keep operating in an environment where security measures mean less reliable lead times, supply chain managers should focus on methods that they have always used to deal with uncertain supply chain. These include investments in better visibility measures, configuration of manufacturing systems for postponement and make-to-order, and the use of risk pooling strategies.

In preparation for another attack and as part of the effort to foil it, companies should redesign their systems with security in mind. Thus this article calls for the establishment of a Chief Security Officer and for the creating of a security culture similar to the sales culture of the 1970-s and the quality culture of the 1980-s and 1990-s. In addition the article calls for a public-private partnership focused on sharing data and knowledge at all levels.

1 The challenge

Shortly after the September 11th 2001 terrorist attack, many manufacturers experienced disruptions to the flow of raw material and parts into manufacturing plants. For example, Ford had to idle several of its assembly lines intermittently in the days following the attack, as trucks loaded with parts destined to these production plants were delayed at the Canadian and Mexican borders. As a result, Ford lost 12,000 units of production. And as reported by the wall Street Journal (Ip 2001), Toyota came within 15 hours of halting production at its Sequoia SUV plant in Princeton, IN, since one of its suppliers was waiting for steering sensors, normally imported by plane from Germany, and air travel was shut down.

The reason that Ford, Toyota, and other leading manufacturers were vulnerable to transportation disruptions is that they operate a "Just-in-Time" (JIT) inventory discipline, keeping just enough material on hand for only a few days and sometimes only a few hours of operation. The system requires frequent deliveries of material and a reliable transportation system.

It is instructive to note that these disruptions were not caused by the attack itself but by the US Government response to the attack: closing borders, shutting down air travel, and evacuating buildings all over the country. The US Government is now in the process of getting its thinking, its institutions, its communications strategy, its military response, and its domestic defense strategy ready for a challenge that is likely to last a long time. Thus, we have entered a new era during which there are likely to be continuous hostilities between the US and its allies on the one side, and various terrorist group and governments who support them, on the other. A "win" will be a long period of unsuccessful terrorist activity and one will never know whether the US has achieved it or not, since the "win" can be reversed in a single act by a small number of people.

This article focuses on how corporations should prepare and change so they can continue operating in the face of the new realities, since "living well is the best revenge" and getting back to economic growth is the job of the private sector.

As companies organize to face the new world order, manufacturers, distributors, retailers and other entities involved in the handling of physical goods are faced with four challenges:

1. How to be prepared for another attack? Assuming that some attacks will be successful, companies have to prepare to operate in the aftermath. It should be noted that companies are vulnerable not only to attacks on their own assets, but also to attacks on their suppliers, customers, transportation, and communication lines and other elements in their eco-system.
2. How to manage supply chains under increased uncertainty? The measures taken by the US and other governments aimed at better homeland defense and higher scrutiny of international movements have burdened the world's transportation system, thus creating longer and less reliable lead times. In addition, even small terrorist events, which have little economic consequences, can have unexpected effects on demand.
3. How to manage the relationship with the government. The war on terrorism will bring about a new era of public-private cooperation in which companies will rethink their relationships with the government. Unlike any prior wars, all US citizens and US institutions, in particular private enterprises, will have to be part of this war.
4. How to manage the increased costs of security measures?, Taking precautions to defend employees, physical assets and intellectual property, will take resources. Companies need to determine what has to be done, and how to do it in the most efficient manner, balancing the need for security against other corporate goals.

Sections 2, 3, 4 and 5 of this article, respectively, describe the steps companies should undertake to position themselves for success in the new environment.

2 Getting ready

The analysis of preparedness and the extent that companies should invest in it, maybe best conducted in the context of real options theory.[1]

An option represents an opportunity—the right but not the obligation— to take action in the future. In the financial markets, options are contracts representing the right to buy or sell an asset at a given price under certain conditions (such as on a given date, or when a certain event takes place). Option contracts are, therefore, a mechanism for handling risk,[2] since they can be activated (or not) if a certain outcome takes place.[3] Since options represent a right that can be exercised (or not) at the discretion of the option holder, their value is higher when the range of underlying possible outcomes is wider. In other words, the option holder should not mind if a bad outcome is very bad, especially if a good outcome may be very good – since the option would not be exercised in case of a bad outcome regardless of its magnitude. The option price is the amount a buyer will have to pay for the option (i.e., for the opportunity represented by the option).[4]

Unlike financial options, real options deal with physical entities. Since any investment that a company may undertake entails risk, and it may open for the company a range of investment opportunities that will not be otherwise available, option theory provides a natural framework for analyzing capital investments; and as many authors argue, it leads to better decisions than traditional methods.

While traditional investment criteria are based on the Net Present Value (NPV) rule, in many cases they fail to take into account the value of creating opportunities or *options* for future actions. An investment that appears uneconomical when subtracting its discounted costs from its discounted benefits, as the NPV rule prescribes, may be viewed differently if the company can take into account other investments and projects that will be open to it (but it will not be obliged to undertake) if the first investment is made. For example, Dixit and Pindyck (1996) make the point that by not accounting properly for the options that research and development (R&D) may open up, naïve NPV analysis may lead companies to under-invest in R&D.

One of the main tenants of preparedness is the investment in redundancy, which can hardly be justified on the basis its positive NPV. Instead, we use real options framework to

[1] For more detailed explanation of real option analysis, see, for example, Luenberger, (1998); and Amran and Kulatilaka, (1999).

[2] Note that people use option in everyday life to manage risk – DeNeufville (2001) make the point that insurance is a form of option. The insurance premium gives an automobile owner the right to "sell" the car to the insurance company at a certain price (its market value) regardless of its actual shape (say, following an accident). In practice, the automobile owner does not really sell the car but simply receives payment for the losses.

[3] Most high technology employees are familiar with company stock options, which give the holder the right to buy the underlying stock at a certain ("exercise") price. The value of the option stems from the fact that the employee may be able to "exercise the option" (i.e. buy the underlying stock) when the market price of the stock is higher than the exercise price (i.e., the option is "in the money"), pocketing the difference between the market price and the exercise price. If the stock price is not above the exercise price, the employee does not have to exercise and thus does not have to take a loss.

[4] Note that the option price is different from the exercise price. The former is the (usually upfront) price that a buyer pays to purchase the option, while the latter is part of the contract represented by the option.

analyze these investment which fall into three main categories: (i) supplier relationships and awards, and (ii) inventory management criteria, and (iii) knowledge and process backup.

2.1 Supplier relationships

In the last decade many companies have moved to limit 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. New procurement tools and services have enabled companies to conduct on-line auctions and participate in commodity exchanges.

Security considerations are likely to push more companies to abandon public Internet 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. The latter types of relationships are more prevalent in Europe and the Far East and in some cases were viewed suspiciously in the US.[5] In the new environment, however, companies may worry that their suppliers might start rationing their products in case of difficulties due to a local terrorist attack, a problem with one of their own suppliers, transportation difficulty, or another disruption. Clearly suppliers are likely to allocate products first to their long-term customers, with whom they have stronger relationships, giving more impetus to this type of relationships.

Following the September 11 attack, many US companies started re-considering the wisdom of using overseas suppliers. The choice is between a close-by US suppliers and international (mostly but not exclusively third world) suppliers. Offshore suppliers may be less expensive but require longer lead-time and may be susceptible to disruptions in the international transportation system. Local suppliers may be more expensive but closer (and, arguably, less vulnerable) and therefore able to respond faster.

Instead of choosing one alternative over another, the 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.

Thinking in terms of real options - the incremental cost of using the local supplier for the fraction of the business is the price of the option. Consider the following example: a high technology company sells medical devices made by a contract manufacturer in Malaysia. The Malaysian supplier is contracted to deliver the devices at $100 a piece and the devices are sold by the US company at $400 each. The fixed costs involved in 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, however, that there is a 1% probability that the Malaysian supplier will be disrupted and will not be able to deliver for an extended period. Taking this into account, the expected profit when using the Malaysian supplier is:

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

[5] Clearly, many US companies -- for example, Chrysler -- have developed deep relationships with key suppliers – looking for low costs through stable relationships and joint product development, while others (such as General motors under "Procurement Czar" I. Lopez) looked for low costs through whip-sawing suppliers against each other to get the lowest bids.

since in case of a disruption the company will have no sales but he fixed costs will still be there. A local supplier can deliver the same devices for $150 a piece. Under a dual supply arrangement the local supplier may be given, say 20% of the business so it will have the capability 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 vendor will supply all the devices and the company's profit will be:

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

Taking into account both eventualities, the expected profit when operating with dual suppliers is:

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

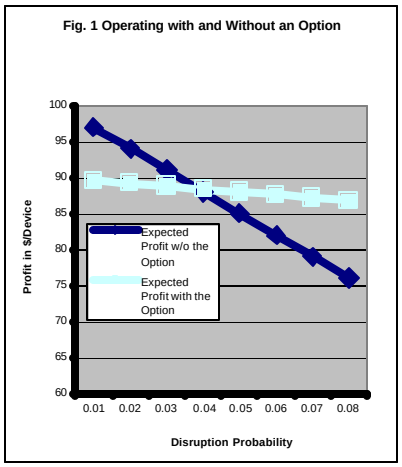
Thus, the price of the option that the company bought, looking at the expected value of the lost profit, is:

$$P_6 = P_2 – P_5 = \$97 - \$89.6 = \$7.4 \text{ per device}$$

Naturally, if there is no disruption, the company has spent $P_1 – P_3 = \$10$ to be able to call upon the local supplier and avoid a loss of $200 per device when no supply is available.

Clearly this simplistic example ignores the time value of money, possible penalties for not delivering and many other aspects of reality. It demonstrates, however, the value of creating a real option. By establishing the relationships with the local supplier, the company has the right to procure the devices from it. It has no obligation to procure the devices from it (beyond the 20% required to keep the supplier's capability). And it will use its right in case of a disruption to the main supply flows.

Note that as DeNeufville (2001) points out, such an option is more valuable the more uncertain the reliability of the supply chain becomes. As Figure 1, the difference between the expected profits when using the option to the expected profit when operating without using an option grows as the probability of disruption grows.



Thus, one can expect some jobs to be moving back into the US as companies trade off lower parts costs against delivery reliability and adding local sources to their mix. This, however, is likely to be neither a large shift nor an immediate one. It is not going to be large since it is not likely that companies will forgo the benefits of low cost, high quality offshore manufacturing altogether, but rather only hedge their bets with local suppliers. It will also take time since companies sourcing decisions are made, in many cases, 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 high traditional reliance on offshore contract manufacturing.

Dual supply sources are not a new idea and they have general merits beyond responding to terror. For example, Billington and Johnson (2000) describe how Hewlett Packard has used "dual response manufacturing" to supply inkjet printers to North America for several years. Initially this was done using a combination of high volume, low cost production resources in Singapore and higher cost, shorter lead-time production resources in Vancouver, Washington. It used the Vancouver supplier to launch the product and deal with demand peaks, while the Singaporean supplier handled most of the stable production.

Another example is the Pentagon's concern about the availability of high quality design and manufacturing of weapon systems in the US. This concern has been used to justify many weapons contracts by the need to keep design and manufacturing capacity alive, even when the need for a specific weapon system is not clearly justified by the services' immediate needs.[6]

2.2 Inventory

Following the terrorist attack of September 11th, many companies started questioning the wisdom of "lean operations" using just-in-time" (JIT) processes. The temptation is to start accumulating inventories "just-in-case" something happens again. Some companies are looking to ordering parts in larger quantities and creating new safety stocks to keep their assembly lines moving in case their inbound transportation is disrupted. In addition, they plan to keep more finished goods on hand so their customers can be supplied even when the manufacturing process is disrupted.

The benefits of JIT manufacturing, however, have been immense – manufacturers who adopted the system saw not only their inventory carrying costs go down -- even more importantly, they saw their *product quality* improve dramatically. The reason is that having large inventories on hand creates complacency, which masks quality problems in the manufacturing, procurement, and other processes. Rather than fix these problems, it used to be easy and tempting to discard defective parts and replace them with parts from stock. With a JIT system, such quality difficulties are apparent and lead to fixing the problem at its source. This discipline is one of the underlying principles of the Toyota Manufacturing System, which propelled the company to its current leadership position, and was adopted, in one form or another, by leading manufacturers in every industry.

The challenge, then, is to ensure that supply lines are intact while not incurring the high costs of extra inventory. A possible solution, which can again be analyzed by using the notion of real options, 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, normal forecasting discrepancies and business fluctuations should be covered by safety stock, which should be set using existing methods, based on the lead time and required service levels (see section 3 for a discussion of mitigating forecast challenges).

To create a dual inventory system logistics managers should designate a certain amount of inventory as "Strategic Emergency Stock." This stock should not be used to buffer the day-to-day fluctuations of the processes it feeds. Instead, it should be managed using an

[6] Even the 2002 controversial tariffs on imported steel were justified, in part, by the need to keep steel production capabilities in the US in case of war (Will, 2002).

inventory discipline that can be summarized as: "Sell-One-Store-One" ("SoSo.") With this discipline the reorder quantity of the items in the strategic emergency stock is raised by the number of item required in this inventory. Then this inventory is managed in JIT fashion – when an item is drawn upon, it is replenished immediately regardless of changing daily needs. Furthermore, this inventory can be drawn upon only in case of an extreme disruption, possibly requiring approval at a high level of authority within the organization.

Using the real option terminology, the costs of the extra inventory represent the price of the option, or insurance policy, that the organization invests in.

Clearly, it is difficult to expect managers to ignore this inventory when a service failure is about to take place in normal times. To make sure, however, that the organization will not simply get used to the higher level of inventory, reaching the strategic inventory level should be treated as a stock-out situation. In other words, such occurrences should get top management attention and the root causes fixed at the source.

Such a discipline is difficult to implement since the temptation will be to always draw on existing inventory, especially since it is physically indistinguishable from any other inventory the company may keep and the separation between the two types of inventory takes place in the database and not on the floor. However, this discipline, while increasing inventory carrying costs some, may save manufacturers the considerable costs of low quality associated with "Just-in-Case" inventory management.

The concept of Strategic Emergency Stock is similar to the philosophy that led the US to keep Strategic Oil Reserves. Such reserves are intended to buffer the US in case of a sever disruption in the flow of oil. When these reserves were dipped into occasionally due to price fluctuations, they were replenished immediately.

Manufacturers and distributors of medical supplies keep a similar "strategic inventory" for military needs. In the early 1990-s, the Department of Defense (DOD) discontinued the practice of holding emergency medical supply inventory in special depots (where they would get outdated) in favor of two cooperative industry programs:

- Corporate Exigency Contracts (CEC). Established in the early 1990-s, this program requires manufacturers to keep certain amount of inventory, which the DOD has already paid for, as part of their regular safety stock.[7] Thus, if the re-order point of a certain item is say, 100 units and the DOD requires 50 units in its emergency inventory, the re-order point would be raised to 150 units. Furthermore, a stock level of 50 units is treated as a "stock out" where shipments to all commercial customers are canceled. In consultation with DOD, however, this inventory can be released.[8]
- Prime Vendor Contracts (PVC) with distributors. Established in 2001, this program is similar but is based on the inventory kept by distributors near urban areas. This is usually the first line of response as distributors are required to ship supplies to hospitals within 12 hours (while manufacturers have to be ready to ship their emergency inventory in 24 to 48 hours, depending on the item).

The medical supply industry is, naturally, more attuned to emergency response considerations than other industries, but the philosophy behind the handling of their emergency inventory is applicable to all industries.

---

[7] The DOD also pays the manufacturers inventory carrying coats and handling costs for this inventory.

[8] For example, the DOD approved shipments of emergency inventory from Johnson and Johnson plants to New York in the aftermath of September 11th, even though the inventory was originally slated for the use of the military.

2.3 Knowledge

The preparations involved in protecting companies' knowledge involve three main efforts:

1. Developing backup processes
2. Backing up the company's knowledge
3. Backing up the company's relationships

Process documentation and backup

Many companies have long understood their total reliance on their information technology infrastructure. Consequently, they have set up backup sites for the information technology infrastructure of each enterprise, ensuring appropriate backup of critical applications and data.

Consider, for example Solomon Smith Barney. The giant financial services firm had 7,000 workers in one of the towers of the Word trade center. Luckily, they all got out in time. What was not due to luck but to massive preparations, was that the firm had its trading desks backed up by complete information technology infrastructure, ready to operate on the afternoon of September 11. As it turns out the company kept a set of back up systems in a New jersey site and was able to be up and running in very little time. The company was able to move very quickly because in addition to *systems*, it also had emergency backup processes in place.

Fewer companies, however, had worried about the development of such backup emergency business processes. Such process should spell out communications protocols, authority, and decision-making procedures in case of a breakdown in communication as a result of another terrorist attack.

Knowledge backup

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

Interestingly, many companies document business process when such processes are designed. They fail to keep up, however, with the ever-changing nature of such processes in the business world. This need may be the nucleus of a much better set of software applications, which support both processes and their continuous documentation.

Relationships backup

In addition to business processes, companies need to be able to salvage customer and supplier relationships. These can be salvaged if all interactions with customers have been documented in a Customer Relationships Management (CRM) system. Relationships should be thought of as just as important as data and processes. Documenting all customer interactions can help companies pick up after a disaster a lot faster than otherwise.

* * *

All these backup activities are a form of insurance premium or the price of a real option that companies should pay in order to be able to exercise them when the need arises.

Not every preparedness action, however, involves 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, several incompatible manufacturing and financial systems, are much more vulnerable than companies who standardized their operations and can move personnel and processes between locations if a single location goes down.

Standardization, in effect creates the option of letting managers from different places to move around the enterprise and use their expertise elsewhere in case part of the enterprise is inoperable.

3 The basics: better supply chain management

For many nations and peoples, terrorism is not a new phenomenon – the people of Belfast, Jerusalem, Spain's Basque region, Kashmir, and elsewhere had to endure terrorist actions for many years. And they had to keep operating their enterprises under these conditions, putting the proper security measures in place as well as making contingency plans.

The supply chain of any manufactured good involves the network of enterprises and processes which take a combination of raw materials and turn them into a finished product at the consumer's hands. Most of the expected impact of the new security measures will be reflected in supply chain management challenges, which are likely to be less reliable.

Longer supply lines and uncertain deliveries are not new for supply chain managers. The globalization of manufacturing, the explosion of new products, and the short life cycle of many products have burdened logistics managers with long supply lines and significant uncertainty in forecasting of demand. In that sense the new world order does not represent a fundamentally new challenge and thus the basic problem can be tackled by refocusing on known solutions, and adopting new technology to this end as it become available. Some of the most basic strategies include (i) improvements in-shipment visibility, (ii) improved collaboration between trading partners and across enterprises, and (iii) better forecasting through risk pooling methods.

3.1 Shipment visibility

Many logistics managers are still describing the transportation system they are dealing with 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 carries and 'hand-offs," and it requires integration with manufacturing, inventory and purchasing -- since logistic managers need to know not only what is in-transit, but also what is available in stock and what is on-order, and when orders will be available from suppliers. And they deal with thousands of items every day.

Lack of visibility can aggravate the well-known "bullwhip" phenomenon in supply chains (see, for example, Lee *et al*, 1997).[9] This phenomenon describes how demand information becomes increasingly distorted as it moves away from the actual consumers; from retailers to distributors, wholesalers, manufacturers and suppliers along the supply chain. Such distortion leads to forecasting errors, excessive inventory, erratic order patterns, and unavailable products to fill orders – all leading to higher costs and poor customer service.[10] One of the principal ways of mitigating the bullwhip effect is by sharing data about actual end-consumer demand, inventory levels and incoming shipments throughout the supply chain. In other words, by providing visibility to all participants in the supply chain.

Thus 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 both the demand pattern they experience will be more stable and their suppliers will be more consistent.[11] The costs 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 better their own conveyance movements, while others are available from software providers who are attempting to aggregate the information from many carriers and present it to shippers in integrated fashion.[12]

To date, most of the shipment tracking information is based on tracking the conveyance that a shipment is using or the environment it is in. Thus, it depends on timely reporting from the carriers hauling the shipment, the warehousemen storing it, or the distributors handling it. New technology using tags which can communicate directly with low-earth-orbiting-satellite (LEOS) systems offers the promise of freeing shippers from their

---

[9] The first model characterizing the bullwhip effect was built by Forrester (1958). His model consisted of a four stage supply chain, where each stage ordered on its immediate upstream neighbor who only ship those orders (plus those in backlog).

[10] The information distortion gets more pronounced as one moves "upstream" in the supply chain due to "system dynamic" effects – see Sterman (1989a, 1989b), who conducted human-subject experiments to demonstrate that the sources of oscillation and increase in variability were managers' misperceptions of feedback and their inability to account for the supply line of orders as suggested by Forrester

[11] Note that there are other factors that contribute to the bullwhip effect, including long and uncertain lead times, promotions, order and shipment batching, and order inflation during shortage periods. All these factors should be addressed when striving for better supply chain operations, as mentioned in Sec 3.2.

[12] Many of the impediments to full visibility for shippers are not technological. Some leading carrier refuse to let shippers "see" where their trucks are, even though the carriers have the information. To understand the reason, consider, for example, a large truckload carrier who may have at any point in time 10,000 trucks on the road. The carrier's own tracking system may indicate that as many as 1,000 of those are behind schedule. The carrier knows, however, that through a combination of mitigation techniques (driver switching, assigning tractors with team drivers, etc.), only 50 or so will end up actually late. It does not know which 50, though. Opening the tracking system to customers is likely to generate an avalanche of frantic phone calls, which may hamper the work of dispatchers and the relationships with the customers. Instead, carriers usually notify customers that something is late only when they are convinced that they cannot fix the problem. In many cases this notification comes too late for the shipper to avoid service failure to its customer or a disruption to a production line.

reliance on carriers and other suppliers by allowing direct communications with the shipment.[13]

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

3.2 Collaboration

The term "supply chain" describes the movement of material from raw material to finished good at the end-consumer's hands.[14] Thus, while the logistics function within the enterprise is concerned with the inbound and outbound movements to and from manufacturing and storage facilities and the accompanying movements of information and cash, supply chain management is focus on such movement between enterprises. Thus, collaboration among different enterprises is what binds supply chains to make them integrated systems.

In general, one can distinguish between two types of business collaboration:

- Horizontal collaboration – between firms at the same stage of the supply chain. For example, among different retailers or different OEMs. Sometimes the collaborating companies are competitors in certain parts of their business. In the past such cooperation involved working together on the development of standards for commercial transactions, lobbying the government on industry issues, cross selling, and other forms. The new environment will require companies to share knowledge with other enterprises in their industry, including competitors, to develop secure processes.
- Vertical collaboration – between suppliers and their customers and the third parties involved in commercial transactions: transportation carriers, financial institutions, infrastructure operators, etc. This type of collaboration is aimed directly at improving visibility and reducing lead times by letting suppliers and customer collaborate in a structured fashion, which is standard across all industry participants. This is what industry initiatives such as co-managed inventory (CMI),[15] Collaborative Planning, Forecasting and Replenishment (CPFR)[16] processes are currently attempting to accomplish.

Vertical collaboration is aimed square at mitigating the bullwhip effect. By creating mechanisms for trading partners to work together on reconciling their forecasts of sales and

[13] An intermediate step between bar code identification systems and satellite-based system are radio frequency tags, which allow more remote and automatics readings of shipment identification, thus aiding carriers, warehouse operators and distributors to keep better tabs on items under their control. These systems, however, still rely on supplier reporting.

[14] Some authors also include the "reverse logistics" (dealing with returns) and "green logistics' (the disposal of packaging material and discarded products).

[15] CMI grew out of the practice of vendor-managed inventory which many retailers adopted

[16] CPFR is a process by which retailers and their suppliers are sharing data regarding future sales and promotions, allowing retailers to keep less inventory and provide higher availability of products to consumers, while allowing manufacturers to tailor their production schedules to the exact needs of the retailers, leading to lower inventories and higher availability at the manufacturing echelon.

orders, they are much less likely to over-react, independently, to demand signals and order too much or too little, thereby magnifying the demand signal, leading to the bullwhip effect.

Since the middle of the 1980-s, American companies have devised many cooperative schemes to improve supply chain operations. 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, JIT II in procurement and lately, Collaborative Planning, Forecasting and Replenishment (CPFR) in the consumer packaged goods industry and Collaborative Transportation Management (CTM) in the transportation industry. These and dozens of other such initiatives are aimed at ensuring that trading partners coordinate their forecasts, orders, thus avoiding the bullwhip effects.

The Internet and electronic commerce in particular have enabled new collaboration methods between companies with the development of new standards (such as XML[17]), which allow more flexible and general computer-to-computer communications than older electronic data interchange (EDI) standards. The new technologies also gave rise to new breeds of application software that are housed by third party providers and allow many trading partners to access them simultaneously (rather than having one trading partner using an application developed by another).

As lead times are becoming more variable, companies should counter this by redoubling their collaboration efforts. The basic reason is that if the consignee knows about a problem early enough, it can take corrective measures (such as expedite shipment, go to an alternative source, adjust its own customer's expectations, etc.)

Security collaboration

In addition to working on collaboration in order to improve supply chain operations, companies should work both with trading partners (vertical collaboration) and with industry groups (horizontal collaboration) to develop best practices and share relevant knowledge. More than ever, corporations should realize that their long-term fate is intertwined with that of their suppliers, customers, corporations in other sectors of the economy, and even their competitors. Such collaboration has many precedents and is not limited to collaboration among US companies or any other nation's enterprises. For example, when the Japanese figured out the lean manufacturing and Just-in-Time system, leading Japanese manufacturers, such as Toyota, not only allowed researchers from the world over to study their methods, they allowed other companies, including other automobile companies to visit their plants and study their manufacturing system, including their system of collaborating (vertically) with their suppliers. This is an example of collaboration that will be required in the coming era.

Both types of collaboration are important in allowing supply chains to function better. A new type of collaboration – with government is discussed in section 4.

3.3 Risk pooling

One of the fundamentals of forecasting is that it is always easier to forecast more aggregate phenomena.[18] For example, it is easier to forecast the number of Ralph Loren's men's blue blazers size 44R that will be sold nationwide, than the number that will be sold in a particular

[17] Extended markup language

[18] The reason for this, in simplified terms, is that when the number of items one is dealing with is large and varied, it is likely that errors will cancel each other – thus if the forecast is too high for a particular store, or item, or day, it may be lower for another store, or item, or day. And thus the larger the universe of units one is dealing with, the smaller the forecast error is likely to be.

store. And it is easy to forecast the monthly sales than the sales during a particular day.[19] To take advantage of this, companies can employ a variety of strategies such as:

- Postponement. By delaying the time that product have to be committed to a particular destination (customer, location, etc), companies can reduce the forecasting error. For example, Billinton and Johnson (2000) report that Hewlett-Packard cut printer supply costs by 25 percent with modular design and postponement. Generic printers are shipped to local distribution centers worldwide, where local customization (involving local transformers, power cords, and instruction manual in local language) take place once firm orders are at hand.[20] Thus HP has to forecast the aggregate demand for the generic printers, while requiring a disaggregate forecast only for the local parts. These parts are not only less expensive to stock, but can also be manufactured with short lead-time (as compared to the whole printer).
- 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 built cars waiting for customers in dealers' showrooms.[21]
- Product variability reduction. Some manufacturers have combated forecasting difficulties by reducing the number of options and items they are producing. For example, many automobile manufacturers stopped long ago offering all possible combinations of features on their products and offer "packages" of features instead, thus reducing the number of options, reducing costs, and improving the forecasts of the packages desired by customers. This improvement is possible since the smaller number of option allows for better risk pooling, lower variability and thus better forecasts.
- 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 (in this case - geographical aggregation). Thus the trend towards reducing the number of warehouses and other inventory stocking location may accelerate as part of companies' learning to operate in even more uncertain times.[22]

4 Public-private partnership

Most executives in US corporations look at the government as a hindrance to the smooth functioning of the economy. Defense, however, is one of the few roles that even Libertarians

[19] More accurately, the *coefficient of variation (the ratio of the standard deviation to the mean forecast)* of an aggregate forecast is never higher than the coefficient of variation for a disaggregate forecast. In other words, the relative accuracy of an aggregate forecast is always at least equivalent and in most cases higher.

[20] Using postponement, HP has become number one worldwide in Q3, 2001 in inkjet printer market share, in photo-quality inkjet printers, in all-in-one products, and in large-format inkjet printers

[21] Over 80% of the cars VW sells in Germany are built to order rather than to dealers' stock.

[22] Note that increasingly stringent level of service requirements may limit the use of centralized physical inventory.

believe is the proper role of government. 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 many related agencies. The challenge facing the US government is enormous, but the government is slowly rising to this challenge. Protecting private interests, however vital to the nation, is still the purview of the owners of those private assets.

4.1 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 adjust their thinking and start considering the government, both Federal and local, as a partner in certain aspects of corporate life. Some possible collaborative avenue 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 who are in particularly sensitive businesses, such as Nuclear power generation and chemical manufacturing are already subject to laws that require them to do so, but in the new era, corporate executives should think about new possible threats and work with local authorities over and above the legal obligations.[23]
- 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.

4.2 Taking on certain security tasks

Immediately following the September 11 attack the US had a somewhat uncoordinated response, marked by closed airports and borders. Conflicting government calls to be on the alert, while leading normal life, followed this. In the months following the attack The US has started to settle into the long-term reality. This reality is marked by added security costs, added administrative costs, and longer, as well as less certain transportation times due to security checks. Currently, however, the nation has not yet developed the new long-term procedures that will be necessary to deal with the threats efficiently. The delays shippers and carriers experience in the months following September 11 will be reduced as the US develop a more sustainable security system.[24] Thus, firms should not yet over-react to current transportation delays and added administrative costs.

[23] One area of possible coordination is the transportation of hazardous materials, which is described in section 4.3.

[24] Clearly, short-term government responses to specific attack may still disrupt product flows, but even these may be tempered if the threat of terrorist attacks becomes a way of life. For example, immediately after American Airlines flight 587 crashed into the neighborhood of Belle Harbor, Queens, NY, on November 12, 2001, the city closed all bridges and tunnels in and out of Manhattan for several hours. The economic costs of such disruptions are very large and in the future such actions might be avoided.

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. By 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.[25]

Similarly, many of the current processes used to insure the security of freight flows are inefficient and do not "scale" up. This will become more and more evident as the economy will start to get out of the current recession. For example – checking every truck getting into Manhattan or crossing the Mexican border is impractical – the cost it imposes on the economy is too high. Furthermore, such security regime is less effective; it means that security checks become more "routine" and checkers tend to become more complacent when every vehicle is examined.

The freight equivalent of "profiling" is the use of "known shippers" and "certified carriers." In other words, a new certification program will have to be put in place – this will probably be a government certification of carriers, based on training and a prescribed set of security processes. An important part of such certification will be the need to create a class of "known shippers" who have done business with the carrier for a long time and have their own security measures in place. Thus, for example, trucks owned by "certified carriers" hauling shipments from "known shippers" coming into Manhattan, may be waved through (or just spot-checked).

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.

This means that corporations will have to take upon themselves some of the burdens of security provision. Shippers will have the responsibility to check and seal trailers at the origin, as well as to check the background of their transportation managers and warehouse and dockworkers. Transportation carriers will have to develop security procedures for routing and scheduling sensitive cargo as well as to check the background of all their employees. In addition, certified carriers will have the ability to track their vehicles at any point through its journey[26] and to be automatically alerted if the journey pattern changes.

Leading carriers and shippers should work with the government on the creation of the certification programs and the guidelines for who is a "known shipper." 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.[27]

---

[25] The US is using such profiling only to check the luggage of "flagged" passengers.

[26] Most trucking companies can track shipments from origin to destination using satellite communications systems such as Qualcomm's OmniTrack. The system is still vulnerable, however, when cargo has to change hands, as it is transfered between modes of transportation, and in local pickup and delivery operations. The software applications that companies use to track their equipment will have to be augmented in order to detect suspicious patterns.

[27] In a speech at an importers conference on November 27, 2001, Customer Commissioner Robert Bonner laid out a vision of exactly such system. He even 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 custom service in a timely fashion, if they use electronic seals on their containers, etc.

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. (see O'Reiley, 2001).

4.3 Hazardous materials

More than 800,000 hazardous materials shipments are transported every day in the US alone, 94% of which are moved by truck.[28] While many transportation movements may be subject to terrorist threats, the transportation of hazardous materials deserves special attention. Not only is it important to strengthen the security of hazardous material transportation and handling, but also the infrastructure that was already put in place to deal with hazardous materials (especially if it is strengthened) can be the basis for a more comprehensive security program. The main elements of the existing system are:

- The Emergency Planning and Community Right-to-Know Act requires 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 of this legislation 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 drive 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 have to file a "flight plan" and then tracked to that plan throughout their journey. Any deviations from the plan will be checked.

---

[28] About 5% of the shipments are moved by air, and the rest by rail and pipeline. Note, however, that rail and pipelines move a much larger share of the tonnage of hazardous materials (O'Reilly, 2001).

Food supplies

The nation's food supply may also be a target of a terrorist act and, as with hazardous materials, food inspection services can also be used as part of the model and the infrastructure for creating a secure distribution system. In that case there are many Federal and State agencies involved, including the Federal Drug Administration (FDA), the Food Safety and Inspection Service (FSIS), the Environmental Protection Agency (EPA) and the National Marine Fisheries Services (NMFS). In addition, every state has several agencies responsible for public health, agricultural products and meat and poultry inspections.

In refocusing many of these agencies on the threat of terrorism, the main challenge is to coordinate the work of these agencies and make sure that information keeps flowing freely among all the agencies involved.

* * *

In both of these instances – hazardous materials handling and transportation, and food processing and transportation – there is an infrastructure and a tradition of public-private partnerships to ensure safety. In both cases there are many Federal, state and local agencies involved with private industry. And both cases can serve as a basis for a more comprehensive system that will deal with security threats.

4.4 Direct emergency assistance

Modern, large corporations have been in existence only since the second part of the 18th century, with the emergence of the American railroads and Germany's Deutsche Bank. Since then they have developed resources, which in many cases rival public resources and are used in case of war.

For example, US strategy for sea lift in case of war includes the use of The Merchant Marine, which is the fleet of ships that carries imports and exports during peacetime and becomes a naval auxiliary during wartime to deliver troops and war materiel. According to the Merchant Marine Act of 1936: "It is necessary for the national defense... that the United States shall have a merchant marine of the best equipped and most suitable types of vessels sufficient to carry the greater portion of its commerce and serve as a naval or military auxiliary in time of war or national emergency..." The Civil Reserve Air Fleet (CRAF) was similarly established to organize civilian airliners to augment regular military airlift capability in a military emergency.

The specter of continued terrorist attacks means that corporations should get ready to join in the national defense and in the rescue and recovery efforts, which will follow. And the corporate function, which can most likely provide help, is logistics and transportation management. Logistics professional should organize in every area on the US to prepare and help FEMA, the Red Cross and the many other agencies that may be working to alleviate emergencies and rebuild 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.

Interestingly, during the meeting of the World Economic Forum in New York in 2002, several construction and logistics enterprises have come together to create an informal

network for disaster relief. Their objective is to help governments worldwide to mitigate the effects of disasters, whether they are natural or man-made.[29]

5 Organizing to meet the challenge

The demands of the new world reality will require enterprises to add another dimension to the set of objectives and criteria by which they manage their operations: *security*. Many of the actions required for security and preparedness, however, 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 are getting good at it, it is easy to measure and "perfect," it is easy to cost, and easy to manage. In fact, when processes differ from the norm, companies generate another process to deal with exception – this is an attempt to standardize even the outliers. Many aspects of security, however, require that companies will be less predictable. For example, daily changes 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. Section 2.1 mentioned that companies may choose to deal with fewer suppliers on a long-term basis. One should not forget, however, that there might be substantial costs involved. Not only can new suppliers be more competitive price-wise, but also they may bring with them new ideas and processes that may help innovation. The same rationale applies to the choice of local vs. overseas suppliers discussed in that section.
- Centralization vs. dispersion. One of the points argued in Section 2.2 is that in order to pool the forecasting risk, companies should manage inventory centrally. Indeed, many corporate activities, from the provision of information technology, to office work, are conducted better in central location. Security considerations, however, call for dispersion of both assets and personnel in order to mitigate the effect of any local terrorist attack.
- Redundancy vs. efficiency (or security vs. value delivery). Another way to look at the same point mentioned above. All the preparatory steps that corporations may be taking regarding procurement policies, inventory management and knowledge backup (see section 2), 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 the concept "lean operations." The latter calls for "just in case" mentality of preparations while modern operations are organized around "just in time" systems. As argued in section 2.2, the challenge in creating the required redundancies (which can be looked upon as insurance or real options) is to minimize their adverse effects and possibly, use them to create value.
- Collaboration vs. secrecy. Section 3.2 argued for increased collaboration among enterprises as a way to manage supply chains more efficiently and avoid some of the increased costs of longer and less certain lead times and demand patterns. One of the

[29] The effort is coordinated by the Fritz Institute in San Francisco.

tenants of security, however, is secrecy. Thus, while corporations maybe exposing more of their data and internal workings to others and even sharing information about security measures with other corporations, they have to do it in a way that does not compromise security.

- Government cooperation vs. direct shareholder value. US executives are conditioned to put shareholders value, above all other considerations. The new environment may create situation where cooperation with government and the companies, including competitors, may be required, even at the expense of short term profit and therefore shareholder value.

To organize for dealing with the threats, companies will need to create a new function headed by a "Chief security Officer" (CSO) that may join the executive team. The CSO will have to be, first and foremost, a *businessperson* who is familiar with the enterprise and in getting things done in a corporate environment. The reason is that every person and organization is subject to a strong temptation to return to normalcy; 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 daily basis, and will have to create the constituency to follow through with the required investments and changes to corporate life. By and large, military or other security agency background may not be enough for CSO candidates since they will be quickly marginalized in a corporate environment, unless they can understand the business trade-offs and argue for just the required measures and no more, while taking into account the normal business mission and objectives..

In addition, the CSO office is likely to be the only place in the organization where the various security schemes will be coordinated and tested. This is the function that will not only have to make sure that the enterprise can continue after an attack, but that the emergency processes complement each other. For example, while it is clear that dispersion of work and personnel is a reasonable strategy to avoid a large damage due to physical terrorist attack, this strategy makes the enterprise more vulnerable to an Internet virus or worm attack that will slow down and even shut down sections of the Internet. The CSO will also have to be part of the team that will determine not only the priorities under various scenarios but also the procedures to set such priorities when the unexpected happens.

The CSO task, however, is much bigger. In the 1970-s and 1980-s corporations tried to instill in their employees that "everyone is a salesperson." In other words, every employee has to worry about sales and the customers, not only the marketing and sales people. In the 1980 and the 1990-s corporations realized that every employee had to be quality-conscious. It was not enough to add an executive in charge of quality; high quality was the result of entire organizations changing the way they do business to "get it right the first time." The security challenge is similar. 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 where employees have internalized both a set of intelligent applications of security measures and the need backup emergency processes.

Another reason for the CSO to be a businessperson is that many of the 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. Participation in community-wide efforts can also help the image of many corporations as good citizens. 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.

6 Summary and conclusions

Terror is not a new phenomenon and the US itself was no stranger to either suicide bombing or terrorist plots or attacks even before September 11th, 2001:

- On February 26, 1993 a minibus containing 1,100 pounds of explosives detonated in the garage beneath the World Trade Center complex, killing six people. (Investigation of the WTC bombing reveals that it was only a small part of a massive attack plan that included hijacking a plan and crashing it into the CIA headquarters.)
- On August 7th, 1998 the US embassies in Kenya and Tanzania were bombed (killing 224, including 12 Americans).
- In December 1999, authorities arrested an Algerian trying to enter the U.S. from Canada and foiled a plot to detonate a bomb at Los Angeles International Airport in the days before January 1, 2000.

The September 2001 attack highlights a fundamental difference between past and future terrorist acts, which should be looked upon in a historical context.[30] Violent battles for control of people by one group over others have characterized the human race since it began forming societies. Entire populace possessed by a collective anger and hatred, threatening their neighbors and demanding hegemony are as ancient as Biblical histories and as modern as the late 20th century. They always had justification for violence – be it economic conquest, religious domination, righting ancient wrongs, cultural threat, whatever.

Never before, however, has the risk arising from violent social confrontation been as large for a greater number of people. The increased risks cropped up out of the confluence of increased destructive power of weapons and the rise of cheap, instant communications. Together these factors allow, for the first time, ordinary people to gain access to tools of mass destruction and to spawn well coordinated, geographically distributed networks of soldiers ready to use those tools.

The scope of the risk may be nothing less than the survival of humanity. Based on several thousand years of human history, the likelihood that some number of the world's six billion people will from time to time want to spread their influence through violence is 100%. The likelihood that some group will do so in a way that adversely affects a significant portion of the world's population depends only on the vigilance with which the rest of the world (i) defends against the possible violence and (ii) seeks out its roots and cleans away the intolerance of those groups seeking to control others through violence. The United States, with the help of a few other nations, notable Great Britain, may have started to face the threat.

The upcoming period of struggle, however, will challenge not only the US armed forces and its intelligence and police institutions. It will lead to a change in the way US citizens lead their lives and in the way US corporations conduct their business. This article had focused on the last point – getting back to business in the new environment: creating redundancies do that enterprises can withstand new attacks; cooperating with the government and adding security measure in order to prevent such attacks from taking place; and changing corporate processes to cope with the heightened security environment.

[30] The following three paragraphs are taken from a private communication from D. Dolgin to the author.

7 References

Amran,M. and N. Kulatilaka, (1999) **Real Options, managing Strategic Investment in an uncertain World**. Harvard Business School Press, Boston, MA

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

DeNeufville, R., (2001) Real Options: *Dealing with uncertainty in Systems Planning and Design*, 5th International Conference on Technology and policy innovations, Delft, Netherlands, June 29, 2001

Forrester, J.W. (1958). *Industrial Dynamics A Major Breakthrough for Decision Makers.* **Harvard Business Review**. 36(4), pp. 37-66.

Ip, G. (2001) As Security Worries Intensify, Companies See Efficiencies Erode, **WSJ** Sep 24,

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

Luenberger, D. (2000) **Investment Science**, Oxford University Press, Oxford, UK and NY, New York

O'Reilly, J. (2001) *Under Pressure*, **Inbound Logistics** October 2001, pp. 62 - 65

Sterman, J.D. (1989a). *Modeling Managerial Behavior: Misperceptions of Feedback in a Dynamic Decision Making Experiment*. **Management Science**. **35**(3): pp. 321-339.

Sterman, J.D. (1989b). *Misperceptions of Feedback in Dynamic Decision making*." **Organizational Behavior and Human Decision Sciences**, 43(3): pp 301-335.

Will, G. (2002). *New Bush Steel Policy is Driven by Politics*, **Boston Globe** March 7.