A few years back, an article appeared in the online al Qaeda journal, *Al-Ansar*. Entitled: "A Lesson in War," its author wrote the following words: "Aborting the American economy is not an unattainable dream."

The statement, as vague as it is threatening, is a serious warning. We live in an era, in which bides a new arena of conflict. In this post 9/11 Cold War epoch the enemy is not conventional, less identifiable, not as easy to anticipate, but more immediate and very likely to strike. Chaos, rather than conquest, is its primary objective. Therefore, the above quote posits its assumption, not just on the direct material costs of an attack, but also on the cascading economic effects of security expenditures, business disruption, and market shock.

In addition to the transformation in warfare, another pattern of change has been taking place. Global commerce was been undergoing the impact of free trade policies, financial liberalization, and the internationalization of production. The result is a new commercial environment of high volume, unfettered trade. As the global economy expanded, the supply chain became a fragile lifeline. A lifeline upon which, commerce's dependency intensely grew. The greatest and most exposed piece of this supply chain is maritime trade. It is global commerce's circulatory system.

Between 80%-90% of world trade is sea-born. Maritime trade, therefore, may be the single, most exposed link in the transportation system. Among world governments and global corporations the maritime trade transport system is a major source of concern. Particularly serious is the matter of container transport. The uniformity, velocity, and anonymity of containerized traffic offer terrorists ample opportunity to inflict catastrophic damage to the commercial infrastructure. By the time of the September 11 attacks, the United Nations Conference on Trade and Development (UNCTAD) estimated 5.8 billion tons of goods, hulled by 46,000 vessels, passed through 4000 ports in 2001. The volume of trade increased by nearly 40% between the years 1995 and 2001 alone.

These figures represent a transport system that lies at the heart of the global economy. It is also a system vulnerable to an array of corruption, from documentary fraud and illicit money raising operations to physical violation and attack. The system has already been the target of pirates and criminal organizations, which regularly traffic in contraband materials, weapons, illegal drugs and bulk quantities of dangerous material. Due largely to the accessibility of opaque ownership and disclosure requirements, terrorist have the logistics to move material, funds and human beings freely around the globe while using legitimate commercial operations as a front for their sinister motives and activity.

According to a 2003 report by the Organization for Economic Cooperation and Development, the U.S. intelligence community believes that al' Qaeda controls a fleet of 15-18 bulk/general cargo vessels. These vessels have been used for revenue support and to assist in these groups' logistical activity. However, it is obvious that these ships would have utility in paramilitary operations and suicide missions. According to a same report,

statements emerging from al Qaeda sources make no secret of their intentions: “to inflict massive economic losses on the United States and its allies.”

Fortunately, an important trait of the system is the fact that 70% of the containers shipped to the U.S. come through only a few major port operators. The entire network is concentrated in a handful of extreme pressure points. In an attempt to turn this reality into an advantage, the U.S. government has instituted a number of programs. The U.S. Customs and Border Protection agency has initiated a layered approach to securing the supply chain while facilitating trade.

CBP uses a pattern of programs to screen, select, and inspect oceangoing cargo containers. As a primary tool of this strategy, CBP employs an Automated Targeting System (ATS) to automatically flag the highest risk shipments. ATS is a rules-based computer system, which sorts and screens each ship's electronic records to determine cargo risk status. Because most importing companies are legitimate, CBP simply sorts shipments into one of two categories: trusted or untrusted. Using the database of the National Targeting Center, officials can waive through cargos they consider safe while holding suspicious shipments they deem at risk. NTC’s database contains detailed information on every shipment that has entered the United States over the past 10 years. Combined with manifest records, U.S. intelligence reports, and information from foreign governments, ATS matches its targeting rules against the data to assign to each container its level of risk.

Another tier in this layered approach to supply chain security is the Container Security Initiative (CSI) program. The Customs Border Protection Agency launched CSI in January 2002. Under this program, the largest world ports host CSI teams of customs agents, which identify and inspect high-risk containers bound for the U.S. before they load onto vessels. Host countries, which have significant trade traffic with the U.S. ports sign bilateral agreements to assure cooperation between Customs and local officials. By participating, CSI partner countries agree to exchange information, deploy non-intrusive inspection equipment, and commit to establishing an automated risk management system.

.

Complementing CSI is the Customs-Trade Partnership Against Terrorism, or C-TPAT Program. This is a joint government-business initiative. The aim of C-TPAT is to build a collaborative effort with the owners of the supply chain. Importers, carriers, brokers, warehouse operators and manufacturers are requested to conduct a security audit of their operations. C-TPAT members then develop, implement and submit a program to U.S. customs addressing their operation’s vulnerabilities. Additionally, a “24 hour rule” demands that carriers electronically submit a cargo declaration twenty-four hours prior to the cargo’s loading on to any vessel destined for the U.S. This requirement links with the CSI program and offers participants an opportunity for self-policing and reduced inspection time.

Despite these programs, the maritime transportation system still represents our greatest exposure. It has the greatest number of breach points and the potential for the most serious damage. Because ports are located at the intersection of transportation,

communication, and human traffic flows, they are prime targets for terrorist groups. It has been estimated that an attack on the Port of New York/New Jersey could have an economic impact of USD $1 trillion in losses. Any group seeking to "abort the American economy" will have to consider a strike at a major container port.

Yet, the material elements for the defense of our sea-born supply chain are in place. New regimes and regulatory frameworks, for the most part, need not be reinvented. The required technology, too, is available. RFID, biometrics, and computer security technologies are already benefiting from the demand for security goods and services. What seems to be missing is the sense of urgency and a willingness to reconsider our previous notions about national security. With these admissions comes the acknowledgment that we are extremely vulnerable, and that defending these assets will require strategic shifts in defense policies and business plans. This new view of the world raises another dilemma; who should rightly bear the financial, operational, and legal onus for the protection of the maritime transportation system. As important they are to the above theme, however, these topics will have to keep for another discussion.