

*“The perception of the world has changed remarkably in the last several months”*

*Capt. D. M. Egan PE*

*14 January 2002*

The world seems to be a much more dangerous place.

I would like to suggest to you today that the world has not changed; only our perceptions of the world have changed.

Rather than a conventional belligerent nation, we are confronting a more ancient foe.

The nature of the beast is global and supra national in scope (outside the construct of the nation state) with a dangerous unifying doctrine of hate, intolerance and violence.

Not since the days of the anarchists has the world experienced such a threat, and the important difference today is these terrorists have access to weapons of mass destruction.

Starting with the Persian Gulf War of 1990-1991, the United States ushered in a new type of war with a focus on destroying critical infrastructure of the enemy using both conventional and somewhat revolutionary means. This was a war that ushered in the use of stealth fighters and bombers, cruise missiles, and a satellite controlled battlefield with a particular emphasis upon destroying the enemy's command, control and communication systems including the ability to control and distribute electricity and fuel and water. This was the introduction of “nodal” warfare, destroying the enemy's ability to use critical infrastructure.

During the decade that followed, we started to realize that our own nation, by becoming increasingly complex, tightly coupled and heavily dependent upon computerized control and communications, was becoming more vulnerable to cyber attack and cyber disruption. Considerable emphasis was placed upon introducing continuity of operation plans that ensured redundant and appropriately isolated systems. This effort peaked during Y2K which, being a non-event, convinced most of the public that our vulnerabilities were not as bad as they might have seemed at first. As almost an afterthought, the press reported on a foiled terrorist plot to destroy the

Seattle Space Needle by Algerian terrorists linked to the Osama Bin Laden organization. Few understood the nature of this linkage, however some understood that there was some indirect linkage to terrorists who had blown up two US Embassies in Africa, destroyed American soldiers' barracks in Saudi Arabia, and carried out an abortive attempt to destroy the World Trade Towers.

Following the attacks on the World Trade Towers and the Pentagon on the 11<sup>th</sup> of September, we realized that these terrorists did not have to bring their weapons to the party, they used an inside-out strategy which turned the risks of our own transportation systems against us. One should never forget that the most effective weapon against the might of the US Navy, was the suicidal-manned aerial bomb, the kamikaze. Indeed, much of our critical infrastructure is subjected daily to risks from the hazardous cargos of our nation's transportation systems. The public accepts the risks because the carriers have employed very safe practices in transport operations that prevent accidents from happening. This risk-tolerance on the part of government and the public has resulted in some adverse linkages of hazards that in an unfortunate sequence can change the occurrence of a number of unrelated accidents into a tightly coupled chain reaction, with disastrous consequences. For instance, some ports employ the practice of segregating ships carrying explosive cargoes into a common anchorage, sometimes with little recognition of adjacent shore handling facilities that have large quantities of toxic materials stored on site. The fact of the matter is that if one ship is exploded by a terrorist, perhaps by the crash of an airplane, several other ships and toxics ashore can be ignited with dire consequences to the coastal population.

The USCG Commandant, in a recent speech to the International Maritime Organization, emphasized the need for security plans that address vulnerabilities of individual facilities, offshore terminals and ships. Had the IMO been a multi-modal, all-hazard organization, he could have gone further in recognizing the close coupling among hazards, including transportation systems that provide incentives for exploitation by terrorists, because they amplify the consequences of a terrorist attack into a much larger complex disaster. Despite the creation of many individual security plans that emphasize preparedness and rapid reaction or response, unless they are correlated into a larger regional or area infrastructure security plan, that recognizes the potential linkages among hazards, terrorists will maintain an advantage of choosing the weakest or most vulnerable link with greatest systematic consequences.

Terrorists use our own transportation systems against us exploiting our freedom of movement that creates significant economic advantages of free markets in the "Developed world". Such a concept greatly influenced the Asian Pacific Economic Conference "Economic Leader's Statement On Counter-Terrorism" 21 October 2000 in Shanghai, China. It emphasized the need to coordinate plans and preparedness to enhance airport, aircraft, and port security. It recognized key linkages between transportation system disruptions and temporary supply disruptions and longer-term challenges facing the region's energy supply. It recognized the need for a coordinated effort in critical sector protection including telecommunications, transportation, health and energy. It called for the enhancement of international communications networks

and accelerated sharing of information among Customs and Border police organizations. It called for new response initiatives to strengthen capacity building and economic and technical cooperation to help member economies to put in place and enforce effective counter-terrorism measures. Finally, it called for greater cooperation to limit the fallout or secondary effects of the attacks and the importance of recovering economic confidence in the region through growth-building coordinated policies as well as providing a secure environment for recovery of trade, investment, travel and tourism.

Note the much broader considerations of the APEC Economic Leaders' Statement. They are calling for much more than a simple initiative on improving reactive forces or more completely sharing police intelligence about terrorists. They are calling for an integrative approach with improved coordination in the four pillars of disaster management that are Prevention, Preparedness, Response and Recovery.

The economic leaders used the language "coordination". What is really needed is more collaboration than coordination. We find ourselves in much better shape to coordinate safety than security. Security is quite different than safety. It is highly sensitive and it requires a great deal of trust to divulge one's vulnerabilities even to a partner. Consequently, coordinating one common, unified security approach is uncommon. Safety, everyone can subscribe to and leads towards both standards and international protocols. Because resources are limited, security requires that certain national decisions be made about protecting some things more than others. Because a terrorist will probe a potential target and select targets of lower resistance that still meet the terrorist's objectives, it is unwise for a nation to openly set patterns of security protection and procedures "in concrete". Security demands a degree of covertness while safety is an open discussion. Security requires collaboration over secure communications while safety can be openly communicated and coordinated.

Collaboration is essential to enhance and share security technology that provides such initiatives as integrated surveillance and detection systems, alert and warning systems, secure communication systems – both wide bandwidth and wireless, and decision support capabilities such as hazard simulation and consequence modeling, pattern recognition, and rapid identity authentication. Collaborating to establish common approaches to analyze vulnerabilities and understand the relationships among various linked hazards, can lead to very productive initiatives to mitigate the consequences of terrorism when it occurs. Often this kind of analysis can establish a potential causal chain of events and heighten the awareness and pattern recognition should a terrorist organization conduct a "dry-run" or the initial stages of an attack. This kind of analysis can also suggest productive strategies to break the causal chain by reducing or eliminating coupling of hazards. Such mitigating approaches are also beneficial in the recovery phase to ensure that communities and their economies become more capable of sustaining and recovering from terrorist attacks.

The Multi-Sector Crisis Response Consortium (MSCRC) is positioned in an extraordinary manner to enhance the collaboration needed for combating and mitigating terrorism from international organizations. It provides a wide bandwidth, common meeting ground to discuss and evaluate key technologies such as Geographic Information Systems which effectively communicate the distribution of critical infrastructure and sensitive areas of the economy, modeling and simulation of hazards to establish coupling and consequence footprints and development of econometric models to establish the real costs both immediate from the terrorist attacks as well as that self-imposed reactive cost of initiating alternative counter-terrorism strategies.

We have the challenges of moving such discussions increasingly behind encrypted means. I enjoin this organization with this imperative.

During the recent APEC Transportation Security Experts Working Group session in Singapore, I submitted a potential project proposal that drew heavily upon the capabilities of enhanced collaboration offered by the MSCRC. This proposal would lead to both team to team direct collaboration as well as video-teleconferenced collaboration in development of a toolbox of mutually accessible models and simulations of hazards (transportation hazards with potential danger to critical infrastructure) that might be unleashed by terrorists. The nations of Russia, China (including Hong Kong), Singapore, Canada, Australia and New Zealand, were not in favor of divulging their own appraisals of their nations' vulnerabilities. However, they were strongly in favor of developing common techniques of analysis of the consequences of terrorist attack and a community's capability to survive such an attack. Using a notional nation, the proposal would have a multi-national team set up the GIS clearly demonstrating typical vulnerabilities and coupling of hazards and critical infrastructure. It would then design a tabletop exercise that would engage the power of collaborating over wide-bandwidth video teleconferencing and streaming video. Participants would demonstrate using the toolbox as decision support for response to simulated terrorist attacks as well as a means for improved prevention, preparedness, and community recovery. The tabletop exercise could feature a "red" terrorist cell as well as defenders or terrorist attacks could be pre-scripted. Discussion would draw on the predictions of the consequence assessment tools used as decision support as participants would submit their proposed response and mitigation strategies. A basic and relatively simple econometric tool could be used as a decision support aid by participants to demonstrate the necessity of seeking a balance between security imperatives and the economic benefits derived from free flow of trade.

This conceptual proposal was selected as one of the top four by the APEC Security Experts Group from among 12 proposals submitted by various nations. It is being redefined this week as a proposal for a Phase 1 feasibility study and is to be considered by the APEC Transportation Security Committee during its meeting in Manila 4 March 2002. Russia, China, Singapore, New Zealand and the US strongly supported it at the Working Group level.

To conclude, the current focus on international counter-terrorism really demands a more comprehensive approach to the four pillars of disaster management – Prevention, Preparedness, Response and Recovery. While traditional approaches are used to coordinate international safety initiatives, approaches towards strengthening our collective counter-terrorism capabilities require a different sort of collaboration, more akin with traditional disaster management considerations but with some important differences in secure communications and respect for national sensitivities. Key technologies are those that can enhance collaboration and visual communication in a secure environment. New insight may be gained through creating a notional geographic information system model and conducting team-based, collaborative consequence assessment analysis. This would engage a common set of hazard simulation tools and an econometric tool for more effective decision support. Table top exercises and follow-on discussions would emphasize the need for strategies that enhance the ability for communities to both survive and recover economically from terrorist attacks.