

**International Conference on Gateways and Corridors  
Vancouver, British Columbia, May 2-4, 2007**

**Margaret Purdy – Speaking Notes**

**Gateways and Corridors: Assessing and Addressing Strategic Security  
Concerns**

**Opening**

As the discussion paper prepared by the conference organizers reminded us, gateways and corridors are not new in the context of international trade, travel and transportation. They pointed us to many examples from past centuries -- Alexandria, Marseilles, the Silk Road, and the fact that goods and people on the move have always gravitated to specific geographic gateways or hubs. Yet almost everything else about global trade and transportation has undergone dramatic change over the decades:

- principal commodities;
- the reach of supply chains;
- the look and capabilities of ships, planes, railcars and roadways;
- the dependence on information technology, and
- much more.

The most significant change in recent years has been the attention on security generated by the events of September 11 -- and subsequent fears about where terrorists might strike next. I am going to zero in on:

- contemporary security concerns, and
- what they mean for cities, regions and countries seeking to attract more international commerce by integrating a myriad of efforts under a gateway initiative or banner.

I want to explore four topics:

- First, the need to recognize that *form follows function*, and that the shape of the gateway influences security requirements.

- Second, the extent to which major gateways may be vulnerable to terrorism – but also to many other *dangers and hazards*.
- Third, the likelihood that a *sound security foundation* is already in place, thanks largely to the enhancements that September 11 generated.
- Finally, the need to accept that gateway security is *not security as usual*.

The modern gateway concept is still evolving, but I must say that I am surprised that security receives so little attention in the current dialogue and research. I read carefully the abstracts for all the presentations at this conference, and found the word “security” in only two – mine and that of my fellow panelist, Garland Chow.

- Is this because trade, economic development and transportation specialists tend to work independently of security specialists – in university, government and business settings?
- Is it because gateway players believe they “took care” of security in the wake of September 11 – by responding to new international standards, government regulations, and shareholder concerns?
- Or is it because we lack interdisciplinary research and strategic thinking about security in the gateway-corridor context?

I think all these factors contribute to the marginalization of security issues in the gateway dialogue – a situation that, in my view, makes neither business sense nor security sense.

### **Form Follows Function**

So, to start, what exactly is included in any specific gateway and corridor project? Is there consensus on what’s in and what’s out? And why does it matter in security terms?

Of course the gateway would include important infrastructure such as ports and associated road and rail connections -- as well as key intermodal exchange points. If the gateway is in one country, but final destinations in another, the project would also include international border crossings. That still leaves several questions about the dimensions of any one gateway:

- Is it only about the capacity of seaports and the adjacent road and rail connections?

- Is it just about attracting more market share of the commodities that move across oceans on container vessels -- or is it also about increasing the flow of tourists and business people?
- Does it include airports and the burgeoning air cargo business?
- Is it just about physical infrastructure -- or does it also include the computer systems and networks without which the gateway could not function?
- Who exactly are considered gateway players or partners? Just those who provide and receive special funding? Or does the team include suppliers, freight forwarders, brokers, shippers, and other logistics providers and supply chain players?

The answers to these questions have a direct impact on ensuring that the “right” security measures are in place. For example, goods and people present dramatically different security challenges, and protecting computer-based gateway management systems is not the same as protecting containers and trucks.

The overall objectives of the gateway project also influence security needs.

- Which countries and regions are being targeted for increased trade?
- Are there any indigenous security risks that might migrate to or through the gateway?
- Will goods and people travel directly from points of origin to the gateway, or will they pass through other countries en route?
- Will the extra hassle and the uncertainties associated with security re-screening at borders be the “tipping point” that drives business elsewhere – despite other advantages?

The transportation systems and supply chains that form the central architecture of gateways are complex and global. In my view, it would be ill advised to think narrowly and locally when designing programs to secure them.

### **Dangers and Hazards**

In setting the scene for this conference, Barry Prentice reminded us that there have always been security threats against transportation and freight gateways and corridors. Today, terrorism -- definitely not a new phenomenon -- is the threat that dominates the international security environment.

There is considerable debate around the extent to which the events of September 11 changed the world, but there is little doubt that those events raised the bar in terms of the nature, severity and brashness of terrorist attacks. Along with subsequent attacks in Madrid, London and elsewhere, September 11 also exposed the vulnerabilities of modern, open societies and economies.

Adherents of the extremist *al Qaeda* ideology will remain the pre-eminent threat over the medium term, and will continue to strike targets with symbolic value that offer the potential for mass casualties and major economic disruption. Major ports and other gateway infrastructure certainly meet these criteria.

While *al Qaeda* is front of mind today, over time other extremist phenomena with other motivations, tactics and targets will take its place. Thus, a gateway security program has to be flexible and forward-looking, not mired in getting ready for the last attack.

Nor should it be terrorism-centric. Many other threats could disrupt operations or tarnish the reputation of a gateway:

- organized crime, including fraud, piracy, the illicit trafficking of people, narcotics, vehicles, money and other commodities,
- natural disasters, including earthquakes and tsunamis,
- accidents and mishaps, such a prolonged telecommunications failure,
- SARS, pandemic flu, and other threats to human health,
- economic espionage, and
- cyber attacks.

This is a diverse, dynamic threat landscape -- some of these categories would have had little or no prominence as recently as ten years ago.

Importantly for international trade gateways, threat perceptions are not shared universally. Last year, Texas-based researchers conducted case studies of security initiatives in seven ports –in Brazil, France, Hong Kong, India, Mexico, the Netherlands and South Africa. Not a single port official interviewed for the study cited terrorist activities as a primary security concern. Instead, they said that smuggling, fraud and human trafficking were of far greater consequence.

Risk assessments – done properly – can help determine which scenarios present the highest risk for a specific gateway project, and why. By “done properly”, I mean:

- with the best available *expertise and information* applied objectively to assess the widest possible range of threats, vulnerabilities and consequences, and
- with a *clear purpose* in mind -- that is, to assign the highest priority to the highest risks.

A risk management approach is the only prudent approach in a risk-rich environment, but inevitably it will draw criticism. High-profile commentators will continue to point to what they perceive to be unacceptable vulnerabilities and gaps, and to demand corrective action on each and every one of them – with no assessment of the relative risks, benefits and costs. And elected officials will feel the pressure to act on plenty of non-risk-based reasons.

So, I have two main messages on the threat environment:

- *First, terrorism is but one of many threats that can disrupt or derail gateway initiatives.* All need to be assessed objectively and regularly.
- *Second, it is not enough to assess the risks relative to individual facilities, companies, border crossings, or transportation systems that make up a gateway and corridor project.* Rather, gateway teams must concentrate on scenarios that could affect the operations, performance and reputation of the gateway as a whole – as a composite entity. In this case, the sum really is greater than its component parts.

## **Sound Foundation in Place**

Thanks largely to the wave of activity following September 11, it is unlikely that any gateway project anywhere in the world will be starting from scratch when it comes to security. A sound foundation is probably already in place.

To start with, those managing supply chains and transportation systems were of course paying attention to security before September 11. But it was of secondary or sporadic interest, and most security programs were definitely not focused on terrorism, but rather on reducing shrinkage through theft or on preventing vandalism, the smuggling of people and contraband, and piracy.

Post September 11, counter-terrorism concerns moved to centre stage, and security measures proliferated. There was an almost immediate recognition that the global transportation network presented an array of attractive targets – as well as a wide selection of means for conveying terrorists and their weapons.

Over the past six years, many governments have invested heavily in aviation, marine, trucking, passenger rail and urban transit security. At the same time,

they have developed new security regimes at land, air and sea ports of entry, at border crossings, and for container shipments. They have reorganized the machinery of government, changed their legislative frameworks, and introduced new policies and regulations.

At the international level, organizations such as the International Maritime Organization have put aggressive new security codes in place.

And many owners and operators have gone well beyond meeting mandatory requirements by implementing additional security measures. Last weekend, I checked the web sites of most of the world's largest container ports. Each one had a detailed description of its security arrangements and achievements. I suspect that many – if not most -- of these sites would have been devoid of security content six years ago.

Gateway planners need to take stock of the wide array of post-September 11 security accomplishments and advances – and leverage them to the maximum. For programs still in development, they can propose pilot or demonstration projects or accelerated roll-out in their jurisdiction. They can also do much more in terms of taking advantage of measures put in place originally for safety and facilitation. Examples abound in such areas as intelligent transportation systems, the transportation of dangerous goods, and the provision of advance cargo and passenger information.

Turning the tables, gateway planners also can promote the multiplier effects of actions taken in the name of security. Will they make the task of dealing with other hazards easier? Will they enhance core business performance?

This last point is a critical one in terms of forging gateway alliances between security and economic interests and players – essential alliances, in my view. A growing body of research – most of it conducted by supply chain experts such as Dr. Chow – suggests that security should not be considered solely as an obstacle, an inconvenience, and a financial burden -- but rather as an investment that can simultaneously enhance business performance and profit margins.

A study by three Stanford University researchers concluded that security investments can help businesses improve on many fronts -- inventory control, customer service, visibility, efficiency – and profitability. Importantly, the Stanford team demonstrated that these benefits can be quantified.

Another study – this one by Hau Lee and Michael Wolfe -- examined how to implement “security without tears” – that is, how to improve security in ways that also enhance supply chain efficiency and effectiveness.

In light of this research and what we know about contemporary and future threats, it seems counter-intuitive to ignore robust security as a potential

advantage – or at least a playing field leveler -- in the highly competitive scramble to attract traders and shippers.

### **Not Security as Usual**

As I said, as a result of September 11, most gateway projects are starting from a sound foundation. On closer inspection, however, we discover that this foundation consists of many individual bricks lined up beside each other or on top of each other, with little or no mortar holding them together into a cohesive structure. Yet it seems clear that cohesion, integration and genuine collaboration are the keys to gateway security success.

Security players must find innovative ways to break down silos, avoid time-wasting turf battles, and align their work with the multi-modal, multi-jurisdictional complexion of the overall gateway.

I cannot stress enough that gateway security is not security as usual. It is not simply a matter of stitching together programs already in place at ports, border crossings, and other points along the supply chain. Nor does it replace the ongoing need for these programs. Rather, gateway security requires:

- a common operational picture that generates new insights about potential vulnerabilities
- a shared understanding of the threat and risk environment as it affects the entire gateway,
- a taking stock of security measures already in place,
- consensus around areas requiring new or different security attention to strengthen the gateway,
- recognition that the gateway's reputation depends on how well the entire entity – not its individual parts – manage security, and finally
- commitment to developing a coherent gateway security strategy.

In my view, information sharing best illustrates the scope of this challenge. It is not a matter of too little information, but rather of too much disparate, unconnected information that is never converted to knowledge and shared widely and wisely in the interests of both efficiency and security.

Gateway security planners should ask themselves questions such as:

- Is there an inventory and map of gateway critical infrastructure – both cyber and physical?
- Are the interdependencies among critical sectors well understood?
- Is information fused and shared in a way that enhances everyone's domain awareness?
- Do gateway security officials receive regular briefings and assessments – as a group -- from security and law enforcement officials?
- Is there a single protocol for reporting incidents?

A second area that illustrates the peculiar challenges of a gateway security is emergency management. Since September 11, the main thrust of security programs worldwide has been to prevent terrorism – with disproportionate attention on response, recovery and resilience. Gateways call for a more balanced approach. Even the best gateway security program in the world will not prevent all bad actors from doing all bad things all the time. Senior gateway executives should be interested in knowing:

- Can the gateway respond to disruptions and failures of isolated components without bringing the entire gateway to a grinding halt?
- Is there a consolidated response plan and an associated exercise program that draw in all key gateway players, facilities and jurisdictions?
- Are emergency operations centres within the gateway connected so they can respond in unison to an emergency, no matter what the cause?

Gateway leaders need assurance that both people and the processes across the entire network will perform well when attacks, incidents, and emergencies occur.

With respect to resilience, most gateway projects entail massive new funding for infrastructure projects – including new construction and upgrades. Are financial incentives provided to contract bidders who build in resilience to reduce the structural damage generated by powerful bombs or earthquakes?

Finally, it is critically important to have well-tested recovery and resumption plans -- to minimize disruptions following an incident, and to get goods and people moving again. This needs to be a well-calibrated, whole-of-gateway effort.

## Conclusion

Let me conclude by urging those of you who are engaged in research on gateways and corridors to consider including security in the scope of your future work. This panel is an encouraging sign. So too is the leadership that the Government of Canada has shown by including an assessment of security issues on the list of “immediate measures” announced last year as part of the Asia Pacific Gateway and Corridor Initiative.

My personal view is that smart gateway planners:

- will accept security as a essential element, not as an afterthought or an annoyance,
- will take a wide view – across the entire *network* of systems, processes, players and facilities that comprise the gateway,
- will develop a coherent, integrated security strategy to deal with all dangers and hazards, and
- will consider the many ways in which security can enhance efficiency and business performance.

Let me end by stating the obvious – this is much easier to say than to accomplish.