Gateways and Corridors: Assessing and Addressing Strategic Security Concerns

Margaret Purdy
University of British Columbia, Canada

Opening

Gateways and corridors are not new in the context of international trade, travel and transportation. Examples from past centuries include Alexandria and Marseilles, the Silk Road and the Orient Express. While goods and people on the move have always gravitated to specific geographic hubs, almost everything else about global trade and transportation has undergone dramatic change in recent decades: the principal commodities; the capabilities of ships, aircraft, railcars and roadways; the reach of supply chains; the containerization of ocean shipping; the dependence on information technology; the competition among service providers, and much more.

The most significant change in the past decade has been the attention on security generated by the attacks in the United States on September 11, 2001 and sustained by subsequent fears about where terrorists might strike next. The 2001 attacks prompted wholesale reviews of how security is provided at airports and sea ports, across rail and urban transit systems, and at border crossings. Stringent new rules, codes and regulations now govern advance information sharing about shipments and travelers, new no-fly and watch lists are in place, and more workers must undergo security background checks. In relation to both international trade and travel, security has moved over the past six years from the sidelines to centre stage. Governments have made unprecedented security investments, as have individual companies and sectors.

Yet security has received scant attention in the strategic thinking and research underpinning the modern gateway concept. The driving forces behind gateway initiatives are the stunning growth of Asian economies and the desire to gain competitive advantage over other trade routes and destinations - not security concerns. At the most strategic level, gateways and corridors are vehicles for enhancing a nation's prosperity. As a result, their development and promotion fall almost exclusively to government officials responsible for transportation,

---

1 Margaret Purdy is a Resident Scholar with the Centre of International Relations at the University of British Columbia (margaret.purdy@ubc.ca). She retired from the Canadian public service in 2006 after almost 30 years in the security and intelligence sector. This paper is based on a presentation at the International Conference on Gateways and Corridors held on May 2-4, 2007 in Vancouver. For more information on the conference, see www.gateway-corridor.com
international trade, business promotion, and regional economic development - collaborating with their private sector counterparts. Attracting traders and travelers is a competition - with success dependent on convincing them that a particular gateway-corridor combination offers the best answers to these types of questions:

- How long does it take to travel between origin and destination?
- How convenient are the gateway and associated corridors in terms of reaching end markets?
- How much does it cost to do business on arrival and departure?
- How reliable and modern are the local services, work force and infrastructure?
- How cumbersome is the regulatory environment?

Security is a consideration - but rarely the dominant one - as shippers and travelers choose the routes and destinations that best serve their requirements. Security is but one factor in their overall calculation of cost, convenience and reliability. That said, should a gateway facility or the surrounding community suffer a catastrophic event - be it a terrorist attack or a devastating earthquake - security would likely rise immediately to the top of the list of decision-making considerations.

The relationship between gateway players pursuing trade and economic goals and those focusing on security matters is often uneasy. To start with, these two groups of specialists almost always work independently of each other - whether in government or business settings. Furthermore, while one group may look at a particular company, country or region as a potential trading partner, the other may look at the same "target" through a threat lens.

Gateway players with an economic-trade orientation may believe they “took care” of security in the in the wake of September 11 - by complying with new international standards, government regulations, and shareholder concerns. Now they want to get back to “normal” - to generating more trade, courting new business, making more money. The absence of another September 11-type attack may have pushed security to the back of their minds and off their agendas.

On their part, security officials may not understand or appreciate the business and economic imperatives associated with a gateway initiative - predictability, speed and convenience - or the significant frustration, friction and costs that security requirements can create.

These factors contribute to the marginalization of security issues in the gateway dialogue - a situation that makes neither business sense nor security sense. This paper will explore contemporary security concerns, and what they mean for cities, regions and countries seeking to attract a larger share of international commerce by integrating a myriad of efforts under the banner of a gateway-corridor initiative. The paper is organized around four topics:

- First, the need to recognize that form follows function, and that the shape, objectives and orientation of the gateway have a strong influence on 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; and
• Finally, the need to accept that gateway security is not security as usual.

Form Follows Function

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

Of course, any gateway project would include important infrastructure such as ports and associated road and rail connections, as well as key inter-modal exchange points. If the gateway were in one country, but final destinations in another, the project would also include international border crossings. That still leaves many 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 gateway’s profile – in terms of its aspirations and its geographic location -- also influences security needs.

• Which countries and regions are being targeted for increased trade?
• Are there any indigenous security risks that might migrate from those points of origin to or through the gateway?
• Will increased trade and travel to and from a particular region exacerbate existing security concerns within the gateway, for example, in relation to smuggling and other types of organized crime?
• Will goods and people travel directly to the gateway, or will they pass through other countries en route?

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. If the gateway is an intermediate point in a longer supply chain that extends into another country, the extra hassle and the uncertainty associated with multiple border security screenings could be the “tipping point” that drives business elsewhere - despite geographic and other advantages. If there are serious concerns about the
security situation at points of origin, the gateway may advocate the posting of government security officers abroad to conduct pre-departure screening.

Security should be a central element of every gateway project, and security planners should take a broad view of what comprises the gateway-corridor system – a view that encompasses all relevant infrastructure, systems, commodities, locations, and players. The starting point for their work should be a solid understanding and assessment of the multiple dangers and hazards threatening the gateway.

**Dangers and Hazards**

There have always been threats against transportation and freight gateways and corridors; in the past, the main worries were about smugglers, thieves, pirates, hijackers, storms, and plagues. Today, it is terrorism that dominates the security environment in many countries. Terrorism is definitely not a new phenomenon; its origins can be traced back to revolutionary France and Tsarist Russia. Nor is terrorism a stranger to trading and transportation routes. Indeed, a review of terrorist incidents over the past 35 years reveals a preponderance of scenarios involving transportation – either as a target or as a means of conveying terrorists and their weapons. Consider, for example:

- the aircraft hijackings that dominated the international terrorism landscape in the late 1960s and 1970s
- the hijacking of the cruise ship Achille Lauro off the coast of Egypt in 1985
- the bombing of Pan Am Flight 103 over Lockerbie, Scotland in 1988
- the sarin gas attack on the Tokyo subway system in 1995
- the aborted bombing plot against the Los Angeles Airport on the eve of the last Millennium
- the attacks on the Madrid and London public transit systems in 2004 and 2005, and
- the reports that emerged in the summer of 2006 about plans to use liquid explosives to destroy trans-Atlantic airliners

Modern terrorism undeniably crossed a significant threshold on September 11, 2001 when commercial aircraft were transformed into missiles aimed at the World Trade Centre, the Pentagon, and other targets in the United States. It is debatable the extent to which those events “changed the world”, but there is little doubt that they raised the bar in terms of the nature, severity and brashness of terrorist attacks. At the same time, these attacks exposed in a dramatic way the vulnerabilities of modern, open societies and economies. The very attributes that make global networks successful – speed, reliability, visibility, predictability, interconnectedness – can work against them in the contemporary threat and risk environment. Additionally, not only does a modern gateway-corridor project constitute a sophisticated network on its own, but it also depends on many other networks to provide communications, information and other essential services.

Over the medium term, adherents of the extremist al Qaeda ideology will remain the pre-eminent threat - and will continue to seek out targets with symbolic value that offer the potential for mass casualties and major economic disruption. Major ports and other gateway infrastructure certainly meet “the interrelated
requirements of visibility, destruction and disruption” that Rand Corporation’s Peter Chalk has described as the principal drivers of transnational terrorism in the contemporary era.²

While fears of al Qaeda-inspired attacks have dominated most security agendas since 2001, a series of catastrophic natural disasters -- including the 2004 Asian tsunami and Hurricane Katrina in 2005 -- have reminded governments, businesses and populations that other phenomena can have equally devastating impacts. And, while al Qaeda is front of mind today, over time other movements with other tactics and targets will gain prominence and may even supplant al Qaeda at the top of the list of terrorism perpetrators. 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:

- extremism motivated by specific grievances or issues,
- organized crime, including fraud, piracy, the illicit trafficking of people, narcotics, vehicles, money and other commodities;
- natural disasters, such as earthquakes and tsunamis;
- serious accidents or mishaps, including technological disruptions and prolonged telecommunications failures;
- naturally occurring phenomena affecting human health, such as SARS and influenza pandemics;
- economic espionage, and
- cyber attacks on systems and networks controlling key operations

This is a dynamic threat landscape; not all of these categories would have made this list as recently as ten years ago. Some of the most troubling scenarios include a combination of threats -- for example, terrorists or extremists deliberately introducing disease into a city or disabling computer systems that control essential services. Former White House counter-terrorism coordinator Richard A. Clarke imagined some of these scenarios in a 2005 Atlantic Monthly article³

While fears of al Qaeda-inspired attacks have dominated most security agendas since 2001, a series of catastrophic natural disasters -- including the 2004 Asian tsunami and Hurricane Katrina in 2005 -- have reminded governments, businesses and populations that other phenomena can have equally devastating impacts.

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.⁴ Port officials interviewed for the study were in universal agreement on the importance of a secure global supply chain, but not one of them cited terrorist activities as a primary security concern. Instead, they

---

said that smuggling, fraud and human trafficking were security priorities of far greater consequence.

Because they operate in a complex threat environment, those responsible for securing gateways and corridors face difficult choices in deciding how and where to direct their security spending and attention. It is simply not possible for them to protect every potential target from every possible threat all the time. It is neither feasible nor smart for them to try to address all vulnerabilities – just in case something might happen. Not only would it prohibitively costly to aim for 100 per cent protection, it is impossible in such an unpredictable and dynamic threat environment.

Risk assessments – done properly – can help identify which scenarios present the highest risk for a specific gateway project, and why. Determining relative risk requires applying the best available expertise and information objectively to assess the widest possible range of threats, vulnerabilities and consequences. Carrying through requires a commitment to assign the highest priority (in terms of attention and investment) to the highest risks. Neither is easy or straightforward.

Risk assessment and mitigation are common in the financial and insurance sectors, but the methodologies are less mature in the security field. Indeed, some analysts contend that risk assessment cannot be applied easily to contemporary terrorism – because of its unpredictable and adaptable nature. Others argue that a risk-based approach helps avoid decisions and spending “motivated by political interests and knee-jerk reactions”.

Risk assessments come in a wide variety of forms and flavours. Most can be characterized as tactical in that they focus on one company, one facility, one location – or on one threat category. Some are more broadly based, for example, exploring all the risks relevant to an entire urban transit system or to all the land border crossings between two countries. While this type of work is critically important in a gateway context, it is not enough to assess only the risks to individual facilities, companies, border crossings, or transportation systems that make up a gateway and corridor project. Gateway teams must also conduct strategic risk assessments, by zeroing in on scenarios that could affect the operations, performance and reputation of the gateway as a whole – as a composite entity. In this case, the whole really is greater than the sum of its component parts.

Risk-based decision-making in a gateway-corridor operating environment should employ a three-step approach:

• First, planners should consider a range of scenarios that could have a major negative impact on the gateway and corridor, including scenarios that have not yet been experienced but are nevertheless realistic – a dirty bomb attack on a docked cruise ship, a tsunami that destroys a gateway airport, a pandemic outbreak that affects the gateway workforce, for example.

• Second, they should assess the relative likelihood of occurrence for each scenario, taking into account the history of similar events, the strengths/weaknesses of prevention and mitigation measures in place.

---

and, for deliberate attack scenarios, the track record and technical expertise of the potential perpetrators.

- Third, gateway officials should assess all the impacts, should the identified scenarios unfold. Impact analyses need to consider not only the direct economic and physical effects of large-scale disruptions or attacks, but also the secondary effects, such as public fear, loss of confidence, and personal safety concerns.

As Yossi Sheffi and James B. Rice of the Massachusetts Institute of Technology put it, three questions are at the core of security risk assessments: What can go wrong? What is the likelihood of that happening? What are the consequences if it does happen? They criticize organizations that leave risk management to security professionals, business continuity planners or insurance specialists. In their view, building a secure and resilient enterprise should be a strategic initiative that changes the way an entity operates and that increases its competitiveness. In other words, it is a topic for discussion in executive suites and boardrooms.

Objective, well-informed risk assessments can help determine priorities, but they cannot produce precise predictions. While risk management is the most prudent basis for security decision making in gateways and other risk-rich environments, inevitably it will draw criticism. Commentators will continue to point to what they perceive to be unacceptable vulnerabilities and gaps, and to demand corrective action. At the same time, elected officials may feel political pressure to increase security in situations not supported by risk assessments, or they may decide to take no action, especially if the risk scenarios have not yet transpired.

Any analysis of the evolution of counter-terrorism or homeland security programs will reveal that activity always peaks after major attacks or disasters, or after the discovery and thwarting of specific plots - not before. In the case of aviation security, for example, the 1985 Air India and Narita Airport bombings prompted a major rethinking about how to protect international air travel. Another round of air security enhancements followed the September 11 attacks, and yet another round followed the revelations out of the United Kingdom in 2006 about an alleged plot to use liquid explosives.

Richard A. Posner, an American judge and scholar, has cautioned that “people find it extraordinarily difficult to take novel risks seriously” and that “it is almost impossible to take effective action to prevent something that has not occurred previously”. Posner points to measures taken to reduce the likelihood of reoccurrence of September 11-type attacks. In his view, it was “psychologically and politically impossible” to take these measures before the attacks.

The experience since 2001 in the urban transit sector seems to confirm Posner’s conclusions about security decision-making. While September 11 generated some new measures to protect subway and passenger rail networks, the real push did not come until after two serious attacks -- on the Madrid train system in 2004, and on underground trains and a double-decker bus in London the following year.

---

The maritime sector, on the other hand, seems to illustrate that key gateway stakeholders are capable of allocating priority and investments to prevent and mitigate threats not yet experienced. A 2006 Rand Corporation study\(^8\) revealed that less than two per cent of international terrorist attacks over the past 30 years have hit maritime targets. Nevertheless, security has gained unprecedented prominence in the maritime sector over the past six years. The International Maritime Organization influenced port and marine security around the world by putting an aggressive new security code in place and setting a firm deadline for compliance.\(^9\) September 11 stimulated this activity, even although the attacks that day had absolutely no maritime links.

The Rand study noted that most of the post-September 11 activity in the maritime world has been directed to ports and container shipments, and to preparing for catastrophic terrorism scenarios, such as the detonation of a nuclear device smuggled through a port inside a shipping container. They urged more work on identifying and prioritizing all plausible 21st century risks – for example, conventional bombings of passenger ferries or the contamination of cruise ship food supplies.

### Sound Security Foundation

Thanks largely to the wave of activity and spending following the attacks on the United States on 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.

Those managing supply chains and transportation systems were of course paying attention to security before September 11, but security was usually of secondary and sporadic interest - taking a back seat to safety concerns, garnering attention only after specific incidents, and ebbing thereafter. Most security programs in these environments were not designed originally to counter terrorism, but rather to reduce shrinkage through theft or to prevent vandalism, the smuggling of people and contraband, or piracy.

Post September 11, counter-terrorism concerns moved to centre stage, and security measures aimed at preventing terrorism proliferated. There was an almost immediate recognition that global transportation and supply chain networks presented an array of attractive potential targets - as well as a wide selection of means for conveying terrorists and their weapons. Subsequent attacks and thwarted attacks - such as those against urban transit systems in Madrid and London and against trans-Atlantic airliners - have kept attention riveted on terrorism prevention. As a result, over the past six years, many governments have invested heavily in target-hardening measures in the aviation, marine, trucking, passenger rail and urban transit sectors. 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. Many nations have also reorganized the security

---


machinery of government, changed their legislative frameworks, and introduced new security policies and regulations.

Security has also moved – often for the first time ever – onto the agendas of states, provinces, municipalities and cities. These sub-national levels of government are often active in areas of direct relevance to gateway projects, such as critical infrastructure protection, emergency preparedness and incident response.

Security has appeared regularly on the agendas of international organizations such as the G8, Asia-Pacific Economic Cooperation, the International Maritime Organization, the International Civil Aviation Organization and the World Customs Organization since the September 11 terrorist attacks.

On their part, many owners and operators have gone beyond the minimum mandatory national and international requirements and have implemented additional security measures in their facilities. A check of the web sites of most of the world’s largest container ports will reveal detailed descriptions of security arrangements and achievements. Many – if not most – of these sites would have been devoid of security content six years ago.

It is not clear how many post-September 11 security initiatives have been grounded in objective, well-informed risk assessments. Many projects (such as cockpit door reinforcement and locking) appeared to respond directly to lessons learned from the September 11 hijackings. In the United States, the basis for Department of Homeland Security funding decisions has shifted over time. Initially, some monies were distributed according to population distribution. Later, the focus seemed to be on reducing vulnerabilities and gaps. More recently, Homeland Secretary Michael Chertoff has aggressively promoted risk-based decision-making.

Gateway planners need to take stock of the wide array of post-September 11 security accomplishments and advances – no matter what their origins -- and leverage them to the maximum. For programs still in development, it may be possible to propose pilot or demonstration projects or accelerated rollout in the gateway. Some existing security programs may need streamlining or reform in order to serve specific gateway needs. Two examples come to mind.

- Goods and people often face multiple screenings as they cross national borders en route to their final destinations, as countries exercise their right to determine who and what can enter their jurisdiction. This can create frustration and inconvenience, especially for frequent travelers and companies engaged in regular cross-border business, and may reduce a gateway’s attractiveness.

- The screening of workers provides a second example. Truckers and others who traverse an entire gateway often must undergo multiple – and different -- background checks in order to acquire the necessary credentials and the array of identification cards to enter gateway facilities and to transport shipments across borders. This practice is neither smart from a security perspective, nor efficient from a business point of view.

Security planners can also take advantage of measures put in place originally for safety and facilitation. Examples abound in such areas as intelligent transportation systems, the protection of chemical facilities, the transportation of dangerous goods, and the provision of advance cargo and passenger information. Turning the
tables, gateway planners can promote the multiplier and collateral effects of actions taken in the name of security. Will security measures make the task of dealing with other hazards easier? Will they facilitate movements and enhance core business performance? This latter point is a critical one in terms of forging gateway alliances between security and economic interests and players.

In the 21st century, choosing between competitiveness and security is not an option - for governments or for businesses. The challenge lies in providing adequate and appropriate security, while at the same time ensuring that the gateway remains competitive by moving goods and people quickly, efficiently and at the lowest possible cost. A growing body of research - most of it conducted by supply chain experts - suggests that security should not be considered an obstacle, an inconvenience, and a financial burden, but rather as an investment that can enhance business performance and profits simultaneously.

A study by three Stanford University researchers\(^\text{10}\) started from the premise that many supply chain companies find it difficult to construct a business case to justify security investments. They focused on manufacturers, logistics service providers and ocean carriers, and concluded that security investments can help these kinds of organizations improve their inventory control, customer service, visibility, efficiency, resilience - and profitability. Importantly, the Stanford team demonstrated that the direct business performance benefits of security investments can be quantified.

Another study - this one by Hau L. Lee and Michael Wolfe\(^\text{11}\) - examined how to implement “security without tears”, that is, how to improve security and simultaneously enhance supply chain efficiency and effectiveness. They provided many examples - inspecting products and containers at points of origin, using information technology to automate the chain of custody and to increase transparency and visibility across the supply chain.

Garland Chow of the University of British Columbia has compiled a list of collateral benefits of security initiatives from the perspective of an international shipper. They include enhanced asset utilization through greater visibility; improved lead times; increased efficiency and productivity; improved reliability and services; enhanced shipment integrity resulting in reduced inspection costs.\(^\text{12}\)

In light of this research and what we know about potential threats to transportation and supply chain systems, 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 to a specific gateway. Security should not be a “hard sell” in the boardrooms of key gateway organizations.


Not Security as Usual

As a result of the security scramble after September 11, most gateway projects are starting from a sound security foundation. On closer inspection, however, planners may discover that the foundation consists of 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. They may also discover that some key bricks are missing, broken, or ill fitting.

While some nations took the time to revamp their security and counter-terrorism strategies and to align specific activities to broad goals and objectives, much of the post-September 11 work on new programs and requirements took place in a frenzied environment and largely within traditional silos -- transportation security, border security, nuclear plant security, public health security, for example. And there were silos within silos. Security enhancements emerged independently within the aviation, maritime and surface transportation sectors, with few signs of system-wide planning or collaboration. Stephen Flynn of the Council on Foreign Relations has characterized United States efforts to secure global trade and transportation systems as “piecemeal, with each agency pursuing its signature program with little regard for other initiatives”.\(^\text{13}\)

Gateway security advocates must be prepared to cross traditional jurisdictional, modal and business lines of demarcation and to speak in unison. Presenting a single gateway security vision and a consolidated mitigation strategy calls for unprecedented levels of collaboration, as well as recognition that existing programs with a national, sectoral or modal focus may not fully meet the needs of a specific gateway. For example, some work may need higher priority or accelerated implementation within the gateway. And, in the same way as existing international trade, transportation and infrastructure programs cannot meet all the needs of a new gateway-corrider initiative; neither can existing security programs respond completely to the special requirements and integrated efforts associated with a gateway. In both cases, dedicated attention and innovative thinking are needed.

Each gateway stakeholder brings unique knowledge to the security equation. Governments know the threat and hazard environment; individual corporations have intimate knowledge of their own facilities and vulnerabilities; shippers know the door-to-door supply chain, and so on. The secret to success lies in finding innovative ways to break down information and institutional silos, abandon time-wasting turf battles, and align work with the multi-modal, multi-jurisdictional complexion of the overall gateway. While the terms “partnership” and “horizontal management” are in vogue, collaborative efforts in the security sector often get bogged down in concerns about mandates, secrecy and accountability. For example, attempts to forge public-private sector partnerships to address critical infrastructure protection have faltered in many jurisdictions, as have many cyber security endeavours.

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 shared understanding of the threat and risk environment as it affects the entire gateway,
- a common operational picture that may trigger new insights about potential vulnerabilities,
- a taking stock of security measures already in place,
- consensus around areas requiring new or different security attention to strengthen the gateway,
- acceptance that disruptions or failures in one gateway component can cascade immediately to other components,
- recognition that the gateway’s reputation depends on how well the entire entity - not its individual parts - manage security, and
- commitment to developing a coherent gateway security strategy

Perhaps most important, gateway security stakeholders need to collaborate in a trust-based environment that is neither too formal nor too legalistic.

Information sharing illustrates the scope of taking an integrated approach to gateway security. 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 a forum for the regular discussion of gateway security issues?
- Is there an inventory and map of gateway critical infrastructure - both physical and cyber?
- Are the interdependencies among critical sectors well understood?
- Is information fused and shared in a way that enhances everyone’s domain awareness?
- Is there a continuous flow of information on cargo as it moves along the supply chain - by land, sea and air?
- Can gateway security officials attend regular briefings and assessments - as a group -- from security and law enforcement officials?
- Do they have access to a password-protected web site dedicated to sharing information relevant to securing the gateway?
- Do employees within the gateway have access to customized security awareness raising and training programs?

In countries such as Canada and the United States, somewhere in the order of 85 per cent of critical infrastructure is owned and operated by the private sector. This is certainly the case with many ports, airports and other key gateway-corridor facilities. Outdated attitudes on the part of government security officials can hinder robust information sharing with private sector officials who have legitimate prevention, mitigation and response roles in the gateway context. Too much information remains classified, and security organizations continue to accord low priority to sanitizing and declassifying reports for wider distribution. Too many national security organizations still operate in isolation and secrecy, and are uncomfortable sharing their information and assessments with “outsiders”. Too
few security clearances are sponsored for officials in key industries and sectors and in sub-national levels of government.

While governments need to find ways to share more threat-related information obtained from secret sources using clandestine methods, it is equally important for gateway stakeholders to make smarter use of open information. Vast quantities of open source information relevant to gateway security are available -- but are not assessed and packaged for busy managers in both the public and private sectors. Password-protected websites could provide venues for dialogue around specific questions or challenges, and for sharing information about trends, new technology, incidents, workshops, publications, conferences, and training programs.

A second area that illustrates the peculiar challenges of a gateway security is emergency management. Since September 11, the main thrust of security programs has been to prevent terrorism, especially catastrophic terrorism -- with disproportionate attention on other threat categories and on response, recovery and resilience activities. Gateways call for a more balanced approach.

Even the best gateway security program in the world will not prevent all catastrophic occurrences, and it should not be difficult to make a strong business case for gateway emergency preparedness. Yossi Sheffi of MIT has pointed out that supply chains can be thrown into disarray for many reasons. “The tornado hits, the bomb explodes, a supplier goes out of business or the union begins a wildcat strike.”

Gateway leaders need assurance that people and processes across the entire network will perform well when attacks, incidents, and emergencies occur. They need to prepare not only for serious incidents affecting their own assets and facilities, but also for those affecting networks and systems on which they depend -- those providing energy and communications, for example. They should be interested in knowing:

- Can the gateway respond to disruptions and failures of isolated components without crippling the entire gateway?
- Is there a consolidated response plan and 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?
- Is there a single protocol for reporting incidents?
- Are lessons-learned sessions scheduled after every major security incident, with the results shared broadly within the gateway?

Current, accurate information is critical to managing gateway emergencies of all types. The high levels of interconnectedness in gateway systems and networks mean that a single failure can cascade rapidly. Lee and Wolfe have observed that “a tight integration of information systems across suppliers, manufacturers, logistics providers and customers” can help organizations respond more effectively when a security breach develops in one part of the supply chain.

---

14 Sheffi, “Building the Resilient Enterprise”, page 42.
Infrastructure resilience is also critical in the gateway-corridor context. Gateway projects often entail major public sector investments in massive infrastructure projects—either new builds or upgrades. Governments could consider offering financial and other incentives to bidders who build in resilience to the kind of major trauma associated with 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. A 2006 Rand study of maritime security concluded that improving procedures to reopen ports and restore container-shipping systems that might be shut down following a terrorist attack or a natural disaster could reduce the potential economic impact of a maritime terrorism incident.16

Emergency management and resumption planning need to be well-calibrated, whole-of-gateway efforts. Furthermore, since most gateway infrastructure is located in or near major urban areas, this work needs to merge seamlessly with that of the surrounding communities and their governments.

**Conclusion**

Smart gateway planners will accept security as an essential element, not as an afterthought or an annoyance. They will take a wide view—across the entire network of systems, processes, players and facilities that comprise the gateway. They will develop a coherent, integrated security strategy to deal with all hazards, and they will market their gateways as being both secure and efficient. They will take advantage of the many ways in which security can enhance efficiency and business performance.

This paper has argued that gateway security is not security as usual, and it has identified a myriad of issues that require further exploration and analysis. To date, security has been of peripheral interest in the dialogue around gateways and corridors—not only among gateway proponents and stakeholders, but also among academics and scholars. As a result, independent research and writing on gateway-corridor security are almost non-existent. For the reasons set out in this paper, security may be destined to be ignored or marginalized in the design and management of many gateways and corridors. Collaborative research by experts in supply chain logistics and economics, transportation, information management, security and emergency management could help ensure that security receives the attention it deserves.

---