Canada-Asia Commentary

May 2008 www.asiapacific.ca Number 51

The Asia-Pacific Gateway and Corridor: Gaining a Competitive Edge by Doing Security Differently

By Margaret Purdy*

Executive Summary

The Asia-Pacific Gateway and Corridor Initiative[1] is a bold notion that calls for an equally bold security vision. Just as existing transportation, infrastructure and international trade programs cannot meet all the needs of this new national endeavour, neither can existing security programs respond adequately to such a complex, interconnected venture. The individuals, governments and businesses leading the Asia-Pacific Gateway and Corridor Initiative should take a wide view of security – across the entire network of systems, processes, players and facilities that comprise the Initiative. They should develop a coherent, integrated security strategy to deal collectively with all threats and hazards on the horizon, and focus on positioning security as a competitive asset, as well as a means to enhance efficiency and performance.

Canada occupies an enviable position as one of the world's safest and most secure countries. Indeed, this country's most aggressive domestic security actions since the terrorist attacks of September 11, 2001 have been in relation to two areas of central importance to shippers and traders – maritime, air and surface transportation systems and container movements along the global supply chain. These actions, along with enhancements to Canada's public safety, intelligence, public health, critical infrastructure protection and emergency management programs[2], provide a sound foundation for Gateway-Corridor security. But more is required. Gaps and deficiencies exist in both attitudes and capabilities. Missing is a holistic approach to Gateway-Corridor security that encompasses the myriad of security programs developed independently within public and private organizations. It is not enough to stitch together the fragmented programs already in place at ports, rail facilities, border crossings and other points along the supply chain. The current patchwork approach is not producing the necessary integration and cohesion of effort across sectors, jurisdictions and all modes of transportation.

This *Commentary* examines the evolving threat environment and how security is being designed and delivered in the context of the Gateway Initiative.

* Margaret Purdy is a Resident Scholar with the Centre of International Relations at the University of British Columbia in Vancouver, and a consultant specializing in national security, emergency management and public safety issues. From 1975 to 2006 she worked in policy, operational and senior management positions with various departments and agencies in Canada's security, policing and intelligence community.

Asia Pacific Foundation of Canada Fondation Asie Pacifique du Canada

ISSN 1481-0433

It identifies the missing elements, and recommends that participating governments, facilities and businesses assign high priority to:

- integrating and linking security programs, players and capabilities across the entire Gateway-Corridor;
- improving information sharing among Gateway-Corridor shareholders;
- ensuring that the Gateway-Corridor can respond seamlessly to incidents, accidents and attacks, no matter what their origin; and
- marketing the principal and collateral benefits of a robust Gateway-Corridor security program.

The *Commentary* ends with ten concrete steps for addressing these neglected elements over the next year.

Diverse, Dangerous and Dynamic Threats

For decades, the main security worries facing international trade and global transportation systems were smugglers, thieves, pirates, storms and plagues. While these threats persist, terrorism now dominates the threat landscape in North America and in many other parts of the world. Terrorist incidents over the past 35 years are very heavily focused on transportation systems.[3] Indeed, it is difficult to think of any major terrorist attack in recent years that has not included a transportation dimension – with trains, trucks, boats and planes serving as targets or as a means of conveying attackers and their weapons.

The most spectacular illustration of the persistent link between transportation and terrorism came on September 11, 2001, when terrorists transformed commercial aircraft into missiles aimed at the World Trade Centre in New York, and the Pentagon and other targets in Washington DC. Experts continue to debate the extent to which those events "changed the world," but terrorism crossed a significant threshold that day in tactics, targets and impacts. The 9/11 attacks exposed the vulnerabilities of modern, open societies and economies. The very attributes that enable successful trading and transportation networks – speed, reliability, visibility, predictability, interconnectedness – can work against them in stark, dramatic ways. Even the best security systems in the world cannot guarantee immunity from crippling events. It is impossible to protect everything all the time against all types of threats – or to eliminate all vulnerabilities.

Terrorism experts generally agree that, over the medium term, adherents of the extremist al-Qaeda ideology will continue to seek out targets with symbolic value that offer the potential for mass casualties and major economic disruption. Ports and other infrastructure at the core of the Asia-Pacific Gateway and Corridor certainly meet "the interrelated requirements of visibility, destruction and disruption" that terrorism expert Peter Chalk has described as the principal drivers of contemporary transnational terrorism.[4] Future terrorist attacks will likely have an economic focus, with transportation and information technology systems among the most attractive targets, according to Canadian academic Elinor Sloan, in a recent analysis of terrorism in 2025.[5] A 2006 Rand Corporation study contends that maritime terrorism – even though it accounts for less than 2% of international terrorist attacks – has specific pertinence to al-Qaeda "precisely because Osama bin Laden has emphasized that attacking key pillars of the Western commercial and trading system is integral to his self-defined war on the United States and its major allies."[6]

Fears of al-Qaeda-inspired attacks have dominated security agendas since late 2001. Yet 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 also have devastating impacts. Security programming for the Asia-Pacific Gateway and Corridor must therefore be flexible and forward-looking, rather than preparing against the last attack. Nor should it be terrorism-centric. Many other threats are just as likely – probably more likely – to disrupt operations or diminish the reputation of the Gateway-Corridor:

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

Incidents Illustrating the Linkages Between Terrorism and Transportation

- Aircraft hijackings that dominated the international terrorism landscape in the late 1960s and 1970s
- Hijacking of the cruise ship Achille Lauro off the coast of Egypt in 1985
- Bombing of Air India Flight 182 and Narita Airport in 1985
- Bombing of Pan Am Flight 103 over Lockerbie, Scotland in 1988
- Sarin gas attack on the Tokyo subway system in 1995
- Aborted bomb plot against Los Angeles Airport on the eve of the new Millennium
- Suicide bombing of the USS Cole harboured in the Yemeni port of Aden in 2000
- Attack against the M/V Limburg in the Gulf of Aden in 2002

▲ The French-owned supertanker Limburg on fire in the Arabian Sea off Yemen after being hit by an al-Qaeda suicide boat on October 6, 2002.

- Twin suicide bombing attacks on the Port of Ashdod in Israel in 2004
- Attacks on Madrid and London public transit systems in 2004 and 2005
- Foiled plans to use liquid explosives to destroy trans-Atlantic airliners in the summer of 2006.

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 are those in which terrorists or extremists cross new tactical thresholds – for example by deliberately introducing disease into a gateway city or disabling computer systems that control essential transportation operations.

The terrorism-transportation linkage is real – not theoretical – for Canada. Two of the most serious examples had origins in British Columbia. The bombing of Air India Flight 182 in 1985 was the most serious act of international terrorism – in terms of the number of casualties (329) – until the 9/11 attacks on the United States. On the eve of the new Millennium, an al-Qaeda supporter named Ahmed Ressam drove a rental car onto a ferry in British Columbia, transporting bomb-making material intended for an attack on the Los Angeles International Airport. Canada has also witnessed a steady series of non-terrorist emergencies over the past decade – SARS, floods, forest fires, hurricanes, landslides, prolonged power outages, to name a few[7] – and Canadian police and intelligence agencies have expressed serious concerns about transnational organized crime, economic espionage activities and cyber-based vulnerabilities.[8]

A Sound – but Patchwork – Foundation

The officials managing transportation systems and supply chains were attentive to security before September 11, but it was usually of secondary and sporadic interest – garnering attention after specific incidents, and ebbing thereafter. Many security programs, including in Gateway-Corridor facilities, 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.[9]

Counter-terrorism concerns moved to centre stage after September 11, 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. Successful 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.

The Asia-Pacific Gateway and Corridor benefits from the extraordinary attention accorded security over the past six years. Governments at all levels in Canada invested heavily in target-hardening measures in the aviation, marine, trucking, passenger rail and urban transit sectors. For its part, the federal government reorganized the security machinery of government, expanded legislative frameworks, introduced new policies and regulations and implemented new security regimes – at land, air and sea ports of entry, at border crossings and for container shipments.

Law enforcement, security and intelligence agencies responsible for monitoring and addressing terrorism and other threats to the security of Canada have received regular injections of new funding, as well as updated legislative mandates, since September 11. Organizational changes at the federal level have reflected the importance of horizontal cooperation on security. Dedicated centres focus on terrorism assessments and marine security and are staffed by experts from across government. Integrated Canadian law enforcement teams address national

Asia-Pacific Gateway and Corridor Benefits from Post-September 11 Security Enhancements*

Marine Security

- International Ship and Port Facility Security Code
- Marine Security Contribution Program
- Marine Security Operations Centres

Border Security and Facilitation

- Security and Prosperity Partnership of North America
- Free and Secure Trade (FAST) Program
- Partners in Protection Program

Container Security

- Container Security Initiative
- Advance Commercial Information Program
- Radiation Detection, Gamma-ray and other equipment

* For more details on these programs, see the websites of Transport Canada www.tc.gc.ca and the Canada Border Services Agency www.cbsa.gc.ca

security in major Canadian cities, and joint Canada-United States teams are tackling border enforcement challenges. A Government of Canada operations centre is now functioning around the clock in Ottawa.[10]

Private sector entities in Canada often exceed the minimum mandatory national and international security requirements, acting in response to local conditions, recent incidents, specific site assessments of potential risks, actions taken by competitors, or by a desire to reassure customers or clients. The websites of most of the world's largest ports – including the Port of Vancouver – include detailed descriptions of security arrangements and achievements.[11] Many – if not most – of these sites would have been devoid of security content six years ago. Several port authorities invested their own funds in new or enhanced security measures, such as perimeter fencing and other access controls, well before the federal government announced in 2004 that it would offer financial assistance under the Marine Security Contribution Program.[12]

Security is now on the agendas of all provinces, municipalities and cities. British Columbia, for example, has developed a four-level threat advisory system to disseminate information about the risk of terrorist activities and associated protective measures.[13] And the B.C. Provincial Emergency Program website provides advice on terrorism consequence management and preparedness.[14]

Security now appears regularly on the agendas of international organizations such as the G8, Asia-Pacific Economic Cooperation, the International Maritime Organization (IMO), the International Civil Aviation Organization and the World Customs Organization. In some cases, these discussions have generated tangible results. For example, the IMO influenced port and marine security around the world by putting an aggressive new security code in place and setting a firm deadline for compliance.[15] September 11 stimulated this activity, even though the attacks that day had no maritime links. Similarly, the International Organization for Standardization introduced a new suite of standards last year aimed at reducing security risks in global supply chains. In announcing the new 28000 series of standards, the ISO secretary-general commented, "Threats in the international market-place know no borders."[16]

Recent natural disasters, severe weather events and public health emergencies have had less dramatic impact on national and international security arrangements than the September 11 attacks. But they did stimulate a renewed interest in emergency management, critical infrastructure protection, disaster mitigation, business continuity and resumption planning in both the public and private sectors in Canada. More organizations are using simulation or tabletop exercises to test their responses to various types of crises. One of the most ambitious exercise programs in North America is managed by a partnership of government and business officials from five states in the northwestern US, as well as B.C., Alberta and the Yukon. The Pacific NorthWest Economic Region (PNWER) has organized four major exercises since 2002 using scenarios based on physical attacks on critical infrastructure, an earthquake, a major cyber disruption and a pandemic flu outbreak.[17]

Canada can be proud of its accomplishments over the past six years in enhancing security at ports, border crossings, airports and other points along global supply chains. And the Asia-Pacific Gateway and Corridor will continue to benefit from enhancements initiated by its constituent stakeholders. But almost every security program of direct relevance to the Gateway-Corridor was conceived and delivered in a security silo. Considering the pressures generated by the events of September 11, it is not surprising that the initial actions of governments, facilities and businesses have been in their narrow areas of principal responsibility. But the reputation and performance of the multi-dimensional Gateway-Corridor depend on how well the entire entity – not just its individual parts and players – manages security over the longer term. With a sound – albeit patchwork – security foundation in place, now is the time to consider security deficiencies that can be addressed only at the macro level and only by a coalition of stakeholders representing the entire Gateway-Corridor enterprise.

The Neglected Elements

From a Gateway-Corridor-wide perspective, three security elements need immediate attention:

- integration and cohesion of effort,
- information sharing and knowledge generation, and
- readiness and emergency management.

In Canada, as elsewhere, the post-September 11 work on new or enhanced security programs has taken place in a frenzied environment and largely within traditional silos – transportation security, border security, nuclear plant security, public health security, for example. It is impossible to find a single authoritative source of public information about

the full array of security measures and programs in place across the Asia-Pacific Gateway and Corridor Initiative. This information is available – but only by researching dozens of websites maintained by multiple government departments and agencies, as well as by specific ports, airports, rail operators and industry associations. A composite picture is a prerequisite to analyzing overall strengths, weaknesses and gaps – and to promoting the Gateway-Corridor as a destination that takes security seriously.

And there are silos within silos. Post-September 11 security enhancements emerged independently within the aviation, maritime and surface transportation sectors, with few signs of system-wide or multi-modal planning or collaboration. Stephen Flynn of the Council on Foreign Relations has characterized US efforts to secure global trade and transportation systems as "piecemeal, with each agency pursuing its signature program with little regard for other initiatives".[18]

The October 2006 document launching the Gateway-Corridor Initiative stressed the need for "an integrated gateway approach" and "a real partnership based on consensus and a shared vision".[19] Coordination, consultation and collaboration have characterized the investment, policy and regulatory aspects of the Gateway-Corridor endeavour – but not the security management of its many moving, interconnected parts. Assessing security issues related specifically to the reputation and performance of the Gateway-Corridor was part of the "fast-track" process announced by the federal government at the October 2006 launch. So far, according to a November 2007 update, only the "strategic context" for this security review has been completed.[20] The need to show progress on upgrading or building new physical infrastructure – rail lines, ports, roads and bridges – may explain the slow progress in relation to Gateway-Corridor security. Or it may reflect an attitude that security was taken care of in the years immediately following the terrorist attacks of 2001.

Integration and cohesion of effort across all jurisdictions, sectors and modes will be critical to safeguarding the Gateway-Corridor against the impacts of future hazards and dangers. It is not enough to stitch together the fragmented programs already in place at ports, border crossings and other points along the supply chain. It is equally important that all principal players and partners:

- have a shared understanding of the threat and risk environment as it affects the entire Gateway-Corridor;
- are aware of security measures, programs and capacities already in place across the Gateway-Corridor;
- understand how disruptions or failures in one Gateway-Corridor component can cascade immediately to other components;
- discuss and reach consensus on areas requiring new or different security attention; and
- commit to developing a coherent Gateway-Corridor security strategy.

Each Gateway-Corridor 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. Many excellent collaborative security efforts can be found within sectors, modes and major facilities, such as the regular multi-agency exercises hosted by the Port of Vancouver.[21] The missing piece is a forum or venue where all organizations with a vested interest in securing the Gateway-Corridor can meet, share and collaborate – a trusted environment for sharing information and ideas.

A dedicated security forum is needed to take stock of the wide array of recent security accomplishments and advances within the Gateway-Corridor, and leverage them to the maximum. Such a forum could identify situations where programs with a national, sector or modal focus are not meeting

overarching needs and priorities. For example, while risk assessments of individual ports, airports and rail systems yield valuable insights for the owners and operators of those specific facilities, they do not provide a pan-Gateway perspective of threats, vulnerabilities and areas of highest risk. In the case of new national programs, pilot or demonstration projects are needed to accelerate roll-out in the Gateway-Corridor. Ideas and technologies being developed for critical infrastructure mapping and air cargo security screening could be tested first in the Gateway-Corridor.

A Gateway-Corridor security forum could explore whether measures put in place originally for safety and facilitation – could also have security applications. By way of example, Canada is a world leader in intelligent transportation systems, and many of the technologies now serving efficiency, reliability or environmental objectives may also have valuable security-related applications.[22]

Generating Knowledge

Integration and cohesion on the security front will depend heavily on the willingness and enthusiasm of Gateway-Corridor players to share information. Collectively, the problem is not too little information – but the failure to connect the wealth of disparate information, to convert it to knowledge, and to share it widely and wisely in the interests of collective security. Gateway-Corridor security leaders should ask these types of questions about the current state of information sharing:

- Do we have a forum for the regular discussion of Gateway-Corridor security issues?
- Have we developed an inventory and/or map of critical infrastructure in the Gateway-Corridor?
- Do we agree on the key physical and cyber assets?
- Do we understand the type and extent of interdependencies among the critical elements of the Gateway-Corridor, and the likelihood of cascading impacts?
- Are we fusing and sharing information in a way that enhances everyone's awareness? For example, is there a continuous flow of information on cargo shipments as they move along the supply chain – by land, sea and air?
- Are Gateway-Corridor security officials attending regular briefings – as a group – and receiving regular threat assessments from security and law enforcement officials?
- Do employees across the Gateway-Corridor receive customized security awareness raising and training programs?

Reliable information about the threat environment is the starting point for any assessment of vulnerabilities, consequences, risks and mitigation strategies. In the case of transnational organized crime, terrorism and other significant threat categories, Gateway-Corridor stakeholders look to Canada's national security organizations for information and advice. But officials in those organizations are often uncomfortable sharing their information and assessments with "outsiders" – including with private sector officials who own or operate approximately 85% of Canada's critical infrastructure, including many assets within the Gateway-Corridor. Too much information remains classified and security organizations continue to accord low priority to sanitizing and declassifying reports for wider distribution. Too few officials in key industries and

sectors and in sub-national levels of government have security clearances or the associated capacity to safeguard classified information.

Governments need to find ways to share more threat-related information and assessments. But it is equally important for Gateway-Corridor stakeholders to make smarter use of publicly available information. Vast quantities of open source information relevant to Gateway-Corridor security are available but are not assessed and packaged for busy managers in either the public or private sectors. Opportunities to leverage information technology abound in the Gateway-Corridor setting. For example, a password-protected website could provide an electronic platform for Gateway-Corridor security officials to discuss specific questions or challenges, and to share information about trends, new technologies, incidents, workshops, publications, conferences and training programs.

Most critical infrastructure sectors in the US operate Information Sharing and Analysis Centers (ISACs) where security-cleared staff analyze reports on domestic and foreign threats from government and other sources, review information about possible security breaches from industry participants, and look for trends that could warn of a larger threat. For example, the rail-freight ISAC is credited with helping to avert a transportation slowdown in January 2008 by distributing an early warning of an Internet attack, as well as a patch to protect network computers.[23] A variation of this ISAC model could be piloted in the Gateway-Corridor before being rolled out at the national level or within specific critical infrastructure sectors in Canada.

Preparing for the Bad Days

The past decade has proven that the best security programs in the world cannot prevent all catastrophes. The Gateway-Corridor must be ready to deal with worst-case scenarios because it operates in a highly competitive environment, with many other North American choices available to shippers and travelers. An ineffective response to even a single incident could change minds rapidly and discourage business – at least temporarily.

Again, the whole is greater than the sum of its parts. Gateway-Corridor leaders need assurance that people and processes across the entire network will perform well when attacks or emergencies occur. Consider, for example, a scenario in which reliable intelligence reveals that a terrorist group has succeeded in placing a dirty bomb in an unknown location somewhere in downtown Vancouver, possibly at or near the Port of Vancouver.

- Is there a consolidated response plan that will draw in all key Gateway-Corridor players, facilities and jurisdictions?
- Has that plan been exercised regularly?
- How many emergency operations centres exist within the Gateway-Corridor? Are they connected? Can they respond in unison to this emergency?
- Is there a single protocol for reporting incidents that may be related to this threat scenario?
- Will a lessons-learned session take place after this major security incident, with the results shared broadly within the Gateway-Corridor?

The complex web of assets within the Gateway-Corridor depends on a myriad of externally-managed networks and systems for communications, information and other essential services. Anywhere along this chain, a single failure can cascade rapidly

and with devastating effects on the Gateway-Corridor, including to its reputation. In other words, the Gateway-Corridor is only as strong and secure as the weakest link in its chain of interdependencies. Actions need to be taken to ensure that overall operations are not crippled by a serious incident affecting one of its component parts.

Matt Morrison, the executive director of PNWER, argues that regions such as northwestern North America need to build "disaster resilience." Infrastructure and essential service providers are tightly interdependent and subject to cascading failures that can incapacitate entire communities. "What this means is that a utility or other service provider may have the best security possible and still have its operations or business practices damaged or disrupted."[24] Morrison's assessment applies to all highly interdependent entities – including the Gateway- Corridor. So too does his prescription for fostering disaster resilience:

- Protocols and procedures for information sharing must be worked out in advance of any incident.
- All key stakeholders need to work together to mitigate vulnerabilities and address shortfalls in a consistent framework.
- Cross-sector trust must be nurtured within a public-private partnership.[25]

Supply chain experts agree with Morrison's identification of information sharing as critical to mitigating the impact of security incidents. Hau L. Lee and Michael 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.[26]

Well-tested recovery and resumption plans are also critically important -- to minimize disruptions following an incident, and to get goods and people moving again. A 2006 Rand study concluded that the potential economic impact of a maritime terrorism incident could be reduced by improving procedures to reopen ports and restore container shipping systems that might be shut down following a terrorist attack or a natural disaster.[27]

Ensuring the readiness of the Gateway-Corridor needs to be a well-calibrated, whole-of-enterprise effort. A 2004 Deloitte report took stock of how global business should operate in the post-September 11 environment, characterized as it is by heightened threats and greater uncertainty. Entitled "Prospering in the Secure Economy," the report concluded:

> "The emerging secure economy is a lot like the old one, only faster and with more threats of disruption. Advances in information technology, telecommunications and transportation have enabled globalization to the point where no global organization in any sector is immune to events that occur halfway around the world. This new environment is one in which no single organization has the responsibility for success – but nonetheless may still be singled out for failure."[28]

Good for Business

Despite the shock of September 11, many business and government leaders continue to view security as an obstacle, an inconvenience and a financial burden. A growing body of research – most of it by supply chain experts – suggests that investments in security can enhance business performance and profits simultaneously, and can be a competitive asset and advantage.

A study by three Stanford University researchers[29] 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 team demonstrated that the direct business performance benefits of security investments can be quantified. 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; and enhanced shipment integrity resulting in reduced inspection costs.[30] Lee and Wolfe studied how to implement "security without tears", that is, how to improve security and simultaneously enhance supply chain efficiency and effectiveness.[31] They provided examples, including the use of information technology to automate the chain of custody and to increase transparency across the supply chain.

Despite the huge investments in transportation and supply chain security since September 11 and despite the continuing quest for efficiency gains, the research on links between security and efficiency is surprisingly sparse. Similarly, the Canadian information technology sector is not fully engaged in tackling the interoperability, information fusion and incident management challenges that can impede Gateway-Corridor performance.

Conclusion

The Asia-Pacific Gateway and Corridor is a multi-dimensional, multi-modal, multi-jurisdictional web of people, programs, assets, infrastructure and information. While all stakeholders have made significant security advances in recent years in their own spheres of activity, it is time to pay more attention to the overall Gateway-Corridor – to the shared threats and risks, the complex linkages and interdependencies, the need for the best-available security information and assessments, and the importance of seamless responses to emergencies.

Governments and businesses should continue to enhance security in areas critical to the functioning of the Gateway-Corridor – that is, in all modes of transportation, in border facilitation and security, and in the management of container cargo. At the same time, public and private sector stakeholders must also adopt a holistic approach to security and concentrate on those neglected elements that are critical to the overall performance and reputation of the Gateway-Corridor – integration, information sharing, and readiness. In other words, they must commit to doing security differently.

The kind of collaborative, holistic approach that is needed requires a public-private security partnership that would be unprecedented in Canada in terms of its orientation and national importance. The success of this pioneering security venture will depend on bold, innovative leaders who are motivated to move beyond their own institutional mandates to a joint security effort.

▲ Traffic held up for clearance into the US across the BC-Washington State border illustrates the need to coordinate security within the Gateway-Corridor as seamlessly as possible.

The Year Ahead – Ten Concrete Steps

The Year Ahead – Ten Concrete Steps

To move to a coherent security approach across the Asia-Pacific Gateway and Corridor, ten concrete actions are needed over the next 12 months.

1. Establish an **Asia-Pacific Gateway and Corridor Security Forum**, with broad public and private sector stakeholder representation. The Forum should focus its attention over the next year on specific actions to:

    - integrate and link security programs, players and capabilities;
    - improve pan-Gateway-Corridor information sharing;
    - ensure that the Gateway-Corridor can respond seamlessly to incidents, accidents and attacks, no matter what their origin; and
    - position and market the principal and collateral benefits of a robust Gateway-Corridor security program.

2. Launch a pilot project to identify and map the **critical infrastructure** (key physical and cyber assets, systems and networks) within the Gateway-Corridor.

3. Complete a **strategic risk assessment** of the Gateway-Corridor, using a range of scenarios to assess threats to the critical infrastructure, determine vulnerabilities, and analyze potential impacts and consequences.

4. Develop an **all-hazards security awareness program** for staff working in private and public sector facilities across the Gateway-Corridor.

5. Arrange for federal security and intelligence representatives to provide the Asia-Pacific Gateway and Corridor Security Forum with a **briefing on the all-hazards threat environment** and associated implications for the Gateway-Corridor on an annual basis, or more frequently if required.

6. Expand the **sharing of security-relevant information** between public and private sector stakeholders within the Gateway-Corridor by collaborating on the development of a password-protected website for dialogue and information sharing, by urging federal security and intelligence agencies to declassify assessments and reports for wider distribution, and to sponsor more security clearances for key officials.

7. Undertake a **survey of security or emergency operations centres** within the Gateway-Corridor, including information on their interconnectivity, incident reporting protocols, and alert advisory systems (both in-house and public).

8. Conduct a **tabletop exercise** involving broad public and private sector representation from across the Gateway-Corridor, using a realistic scenario to assess the processes and programs in place for coordination, information sharing, emergency response and business resumption.

9. Sponsor **research on security-related issues and questions** directly relevant to the Gateway-Corridor, including on the linkages between security and efficiency, the interdependencies within Gateway-Corridor critical infrastructure, the potential to leverage existing safety, facilitation and other measures and systems for security purposes, and strategies for engaging the Canadian information technology sector in tackling information sharing and fusion challenges within the Gateway-Corridor.

10. Provide more visibility to security aspects of the Asia-Pacific Gateway and Corridor in **marketing and promotion activities**.

The total cost of this package of 10 security actions would be in the vicinity of $1 million.

These actions should not be imposed by regulation, legislation, or by top-down orders. Nor should they be led by a single organization – although Transport Canada is best-placed to convene the initial meetings of the proposed Asia-Pacific Gateway and Corridor Security Forum, by inviting security, transportation and trade officials from federal, provincial and city governments, as well as owners, operators and users of principal Gateway-Corridor infrastructure and facilities, and industry associations. The key to the success of the Forum will be genuine collaboration, broad consensus and shared accountability. Willingness to share the costs of the ten action items would be a critical starting point.

Historically in Canada, major security initiatives have surfaced only as a result of one of three scenarios: a specific attack or disaster, an aborted security incident, or the imposition of new international standards. Asia-Pacific Gateway and Corridor stakeholders have the opportunity to break this cycle by taking action on the basis that doing so will enhance the reputation, performance and security of one of Canada's most ambitious national undertakings.

Notes

[1] This paper focuses on the Asia-Pacific Gateway and Corridor Initiative announced by the Government of Canada in 2006 and defined as "a network of transportation infrastructure including B.C. Lower Mainland and Prince Rupert ports, their principal road and rail connections stretching across western Canada and south to the United States, key border crossings, and major Canadian airports." Many of the observations and conclusions in the paper apply to other gateway-corridor projects in place or under development -- both in British Columbia and in other parts of Canada.
[2] For information on Canada's public safety programs, see <www.safecanada.ca>.
[3] For information on terrorism incidents, see the *Global Terrorism Database* maintained by the National Consortium for the Study of Terrorism and Responses to Terrorism at the University of Maryland <www.start.umd.edu/data/gtd/>.
[4] Rand Corporation, "Rand Study Warns Maritime Terrorism Risk Extends Beyond Dangers Posed to Container Shipping," news release, October 16, 2006.
[5] Elinor Sloan, "Terrorism in 2025: Likely Dimensions and Attributes," *Trends in Terrorism Series, Volume 2007-3,* Integrated Threat Assessment Centre, Government of Canada.
[6] Michael D. Greenberg, Peter Chalk, Henry H. Willis, Ivan Khilko, David S. Ortiz, "Maritime Terrorism: Risk and Liability," Rand Center for Terrorism Risk Management Policy, 2006, p.16.
[7] Public Safety Canada maintains a database of information on disasters affecting Canadians over the past century <www.publicsafety.gc.ca>.
[8] See, for example, the annual reports of the Criminal Intelligence Service of Canada <www.cisc.gc.ca> and the Canadian Security Intelligence Service <www.csis-scrs.gc.ca>.
[9] John DeGaspari, "Ports Look Outward," *Mechanical Engineering Magazine*, May 2005.
[10] For descriptions of these new organizations, see the websites of Public Safety Canada <www.ps-sp.gc.ca> and the Royal Canadian Mounted Police <www.rcmp-grc.gc.ca/security>.
[11] For example, the websites of the ports of Vancouver <www.portvancouver.com> , Hong Kong <http://marsec.mardep.gov.hk> , Hamburg <www.hamburg-port-authority.de> and Long Beach <www.polb.com> include descriptions of security measures taken since the 2001 terrorist attacks.
[12] Transport Canada, Marine Security Contribution Program <www.tc.gc.ca/marinesecurity>.
[13] British Columbia Threat Advisory System <www.pep.gov.bc.ca/hazard_preparedness>.
[14] British Columbia Provincial Emergency Program <www.pep.gov.bc.ca>.
[15] International Maritime Organization, "International Ship and Port Facility Security Code," adopted in 2002 for implementation by July 1, 2004.
[16] International Organization for Standardization, "New Suite of Supply Chain Management Standards to Reduce Risks of Terrorism, Piracy and Fraud," October 25, 2007 <www.iso.org>.
[17] Pacific NorthWest Economic Region, Blue Cascades exercise series <www.pnwer.org> and <www.regionalresilience.org >.
[18] Stephen Flynn, "Port Security is Still a House of Cards," *Far Eastern Economic Review*, January/February 2006.

[19] Government of Canada, *Canada's Asia-Pacific Gateway and Corridor Initiative*, 2006.
[20] Transport Canada, Departmental Performance Report 2006-2007, November 2007.
[21] For example, the Canadian Navy practiced protecting ship movements and related infrastructure in a 2007 exercise at the Port of Vancouver, and the Centre for Security Science managed a major biological terrorism exercise at the Port in 2008. For more information, see the Exercise Western Sentry backgrounder at <www.navy.forces.gc.ca/marpac> and the Exercise Initial Thunder backgrounder at <www.forces.gc.ca>.
[22] For more information on intelligent transportation systems in Canada, see <www.its-sti.gc.ca>.
[23] "Rail-freight Security Center Warned Early of Cyber Attack," Surface Transportation Information Sharing and Analysis Center, February 29, 2008 <www.surfacetransportationisac.org/news>.
[24] Matt Morrison, testimony before United States House of Representatives Committee on Homeland Security, Sub-committee on Intelligence, Information Sharing and Terrorism Risk Assessment, May 25, 2007, p.2.
[25] Matt Morrison, testimony, May 25, 2007, p.3.
[26] Hau L. Lee and Michael Wolfe, "Supply Chain Security Without Tears," *Supply Chain Management Review*, January 1, 2003, p.6.
[27] Rand Corporation, news release, October 16, 2006.
[28] "Prospering in the Secure Economy: A Deloitte Research Study," Deloitte Touche Tohmatsu, 2004, Foreword.
[29] Barchi Peleg-Gillai, Gauri Bhat and Lesley Sept, "Innovators in Supply Chain Security: Better Security Drives Business Value," paper prepared for The Manufacturing Institute, July 2006.
[30] Garland Chow, "A Total Logistics Cost Approach to Measuring Collateral Benefits of Security and Supply Chain Improvements," paper presented at Asia-Pacific Gateway and Corridor Round Table, Calgary, March 28-29, 2007.
[31] Lee and Wolfe, "Supply Chain Security Without Tears."

For general information on
APF Canada publications
Tel: 604-684-5986
Fax : 604-681-1370
email: info@asiapacific.ca
or visit our website:
www.asiapacific.ca