# Ports and Shipping Security

Michael C. Ircha, Professor Emeritus
The Transportation Group
University of New Brunswick

## Introduction

Increasingly efficient international maritime transportation underlies the global economy's phenomenal growth. Reduced freight rates stemming from economies of scale inherent in containerization and other forms of specialized maritime transport have enabled major companies to internationalize their activities. Economic globalization has allowed international firms to source raw materials and assemble components to produce finished goods in various low cost countries throughout the world. The minimum cost of maritime transportation, primarily focused on containerization, coupled with reductions in national tariffs and trade barriers through international trade liberalization policies has fueled the growth of global economic activities.[1]

Global trade growth has been reflected in the continued expansion of the world's shipping fleet – both in terms of numbers and vessel size. By 2010, the fleet size was 1,276 million dead weight tones, representing an increase of 60 percent since 2000. The most significant growth was in specialized container ships representing an astounding increase of 264 percent during this decade.[2] This growth in the world container ship fleet reflects the continued expansion of the global economy and its dependence on international trade of manufactured commodities.

Despite the recent downturn in container traffic due to the economic recession, this maritime trading sector continues to grow. In 2000,

world ports handled 231,689 TEUs (twenty-foot equivalent units). This rose to 524,945 in 2008, a remarkable 127 percent.[3] The economic recession resulted in a downturn in container throughputs in many ports due to a decrease in world exports in the latter part of 2008 and 2009. In 2010, there was a noticeable recovery in container throughput rates, reaching about 7 percent below the 2007 peak. It is expected that the 2007 levels will be surpassed in 2011.[4]

The remarkable growth in containerization around the globe has led shipping companies to order larger vessels to handle increased volumes and achieve economies of scale in this highly competitive market. Post-Panamax sized 6,000+ TEU vessels are now commonplace in the major trade routes serving Asia. At present, the largest container ship afloat is the *Emma Maersk*, the first of a series of eight "PS-class" ships christened in September 2006. The *Emma Maersk*, at nearly 400 meters long, 56 meters wide and with a draft of 15.5 meters can carry 14,800 TEU (twenty-foot equivalent units). Larger ships mean fewer ports that can serve them. From a security perspective this implies a concentration of targets for terrorists.[5]

Ports and marine terminals provide an essential link in the intermodal interchange of consumer goods exports/imports between ocean carriers and land-based transportation such as trucks and railroads. Marine terminal operators, who manage cargo-handling operations of ocean carriers, trucks and railroads, normally lease their facilities from the Port Authority. In addition to the traditional activities of carrier loading and unloading, freight consolidation, storage, and customs bonding and clearance, some ports and terminals provide value-added services via agreements with freight consolidators and trucking companies.

Because of their essential functions and strategic locations, the viability and productiveness of ports can have a significant economic impact on their surrounding region. Over 40 percent of Canada's GDP is dependent on trade and the federal government is seeking to grow this number as it continues to enter into free trade agreements with other countries.

There are 17 Canada Port Authorities (CPA) that make up Canada's National Ports System, as designated under the *Canada Marine Act* (CMA). These 17 Port Authorities handle 280 million tonnes of cargo annually, valued at $162 billion. Many of Canada's major ports also serve the U.S. market. For example, over half of the containers moving through the Port of Montreal are going to or coming from the U.S. Mid-West. Almost all the containers coming through the new container terminal in Prince Rupert are destined for the U.S. Mid-West. Chicago is one of Canada's most significant hubs for containerized cargo. It is thus essential that Canada take steps to complement U.S. maritime security programs.

**Maritime Security**

The maritime shipping world has long suffered from security threats. From ancient times to the present day problems off Somalia, piracy has been a continuing problem. Security threats in the Mediterranean 4700 years ago were such a problem that the Minoans build their capital at Knossos inland, away from the sea, "on account of the great prevalence of piracy." Such maritime threats led to King Minos' navy putting an end to piracy around Crete leading to an era of peace.[6] Piracy involves ship-to-ship attacks aimed at seeking plunder from cargoes and passengers. In 2010 pirates hijacked 53 ships and captured 1,181 seafarers. Over the past four years, continued to rise. There were 445 attacks on ships in 2010, up 10 percent from 2009.[7]

In our modern era, international protocols have been developed to suppress piracy by protecting ships and their crews from attacks by other vessels. This was codified in the 1958 *Convention of the High Seas* and, subsequently in the 1982 *United Nations Convention of the Law of the Sea* (UNCLOS). In both of these international legal conventions, acts of piracy were defined as universal crimes involving attacks on a ship by persons operating from another vessel and thus punishable under the laws of every state.

This narrow interpretation of piracy was subsequently undermined by shipboard attacks, which could not be easily defined as piracy. For example, the 1985 hijacking of the Italian cruise ship, the *Achille*

*Lauro* by a group of Palestinian gunmen fell outside the strict definition of piracy, but was rather a form of terrorism. The perpetrators were not "pirates" in that they did not attack from another vessel nor seek personal gain, but rather to advance political, religious and other goals.[8] The *Achille Lauro* incident led to the adoption of a resolution by the UN's International Maritime Organization (IMO) calling for "measures to prevent unlawful acts, which threaten the safety of ships and the security of their passengers and crews."[9] This resolution led the IMO to expand the scope of international maritime law to cover acts and threats that were inadequately dealt with in existing law. The 1988 *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation* (SUA) provided measures "for the prevention of all unlawful acts against the safety of maritime navigation, and prosecution and punishment of their perpetrators." The SUA seeks to ensure that appropriate action is taken against persons committing unlawful acts against ships, including acts of violence against persons on board a ship, destroying a ship or causing damage to it or its cargo, placing a substance on board that can endanger the safe navigation of a ship, and damaging or destroying navigational equipment.[10]

The expectation was that these legal maritime security instruments along with the 1988 SUA would prevent unlawful attacks on the seas. However, the tragic events of September 11, 2001 in the U.S. undermined this perception. This world-shaking terrorist act was a significant security wake-up call for the international maritime community – the vessels themselves and the cargo they carried could become terrorist weapons.

**International Response – ISPS Code**

The use of hijacked planes as a weapon of terrorism in the September 11 attacks demonstrated the need for additional legal measures to prevent ships from becoming instruments of terrorist activities. These potential terrorist acts were a significant step up from earlier piracy concerns. The IMO Assembly adopted a resolution in December 2001 to seek cooperation among governments and the shipping industry to devise strategies to eliminate or at least minimize damage to ships,

persons and goods and the disruption of international commerce.[11] Action was quickly taken to revise legal instruments and adopt technical and administrative steps to support the legislation. The two key legislative maritime instruments used to address 21st century terrorist concerns were revisions to the 1988 SUA and amendments to the 1974 *International Convention for the Safety of Life at Sea* (SOLAS).

The SUA revisions added new offences including a wide range of activities considered "terrorist acts" in several current international treaties. The IMO developed new requirements under SOLAS by adding a new Chapter XI-2 on special measures to enhance maritime security and the International Ship and Port Facility Security (ISPS) Code. These were adopted at a SOLAS Conference in December 2002 with the new provisions coming into force on July 1, 2004.

The ISPS Code has two parts: the first describes mandatory security requirements for national governments, ports, ships and shipping companies; and the second, a set of guidelines for assessing risk and implementing the mandatory elements. Essentially, the Code seeks to ensure the security of ships and port facilities as a multi-layered form of risk management. Thus, determining what security measures are appropriate in a specific situation requires a detailed risk assessment to be undertaken.

The multi-layered, risk management approach, inherent in the ISPS Code, is reflected in the security requirements for governments, ships and port facilities. Contracting governments are required to set appropriate security levels based on the nature and scope of the incident or perceived security threat. As well, each government has the responsibility of approving ship and port facility security plans.

In general for ships and ports, there is a requirement to monitor and control access, oversee cargo and passenger handling activities and ensure the availability of security communications. Specifically for ships, the Code requires: ship security plans, security officers, company security officers, and certain onboard equipment. In addition, every ship is assigned a permanent ship identification

number, which is used as part of a Long Range Identification and Tracking (LRIT) system. Shipping companies must comply with SOLAS and ISPS Code and such compliance is verified and certified. Port authorities and marine facilities are required to develop and implement security plans, appoint a port facility security officer and ensure appropriate training is provided.

All ports handling more than 500 tonnes of international cargo were required to have an approved port facility security plan in place and operational by July 1, 2004. Similarly, ships carrying international cargo were also required to be in compliance with the ISPS Code by this same date. By 2005, more than 97 percent of port facilities and 90+ percent of ships were in compliance, with no disruption in world trade.[12]

A further IMO regulation under SOLAS was a Long Range Identification and Tracking (LRIT) system, which came into force on January 1, 2008. However, delays in establishing national data centers and technological difficulties meant the entire system was not operational until well into 2009.[13] The LRIT system enables the US and Canadian Coast Guards to monitor ship movements for security reasons. Appropriate equipment is required on new ships with a phase-in provision for older vessels. The information ships are required to transmit include the ship's identity, location and date and time of the position. The Canadian Coast Guard is providing the lead internationally in the development and use of LRIT.[14]

There are security gaps in the current application of the ISPS Code. The Code excludes small ships (less than 500 tonnes), passenger ferries and pleasure craft. This creates a weak link in the marine security system. For example, the terrorists who carried out the attack on Mumbai hotels in 2008 Mumbai had hijacked a fishing vessel and arrived as pseudo-fishermen. This legitimate fishing vessel was not part of the ISPS Code. Further, there is evidence that many shipping companies and other marine interests have out-sourced their security requirements under the ISPS Code, such that they themselves do not take the issues seriously.[15]

**North American Maritime Security Responses**

Both the U.S. and Canada responded quickly to the need to secure their international maritime cargo movements. Funding was provided in each country to assist their ports in devising and then implementing their port facility security plans. From the Canadian ports perspective conforming to the ISPS Code by July 1, 2004 was essential as ships serving a non-compliant port would not be permitted access to a U.S. port for the following six months. Canadian ports could not allow this to happen. Indeed, prior to the compliance date, U.S. maritime security officials visited several of Canada's major ports to assist and monitor the steps being taken to comply with the ISPS Code. Around the world, the eighteen month period between the IMO's adoption of the ISPS Code and its compliance was a time of significant activity devising and implementing port and ship security plans

***United States***

"America's ports have become much more secure since 9/11. The primary emphasis in port security has gone from preventing cargo theft, to protecting people and facilities from terrorism. That's a major shift."[16] As the major nation concerned with acts of terrorism, the U.S. unilaterally undertook several additional security measures that were beyond the ISPS Code requirements. These included the adoption of the *Maritime Transportation Security Act* (MTSA), Container Security Initiative (CSI), Customs-Trade Partnership Against Terrorism (C-TPAT), and *Security and Accountability for Every Port Act* (SAFE). These initiatives often created a burden on other countries as the U.S. reached out to secure its borders. Much of the U.S. maritime security focus was on the threat of a Chemical, Biological, Radiological or Nuclear weapon (CBRN) being placed in an anonymous shipping container.

The *Maritime Transportation Security Act of 2002* (MTSA) addresses port and waterway security and was signed into law on November 25, 2002. The MTSA is the U.S.'s implementation of the ISPS Code. The MTSA requires Area Maritime Security Committees in ports to coordinate all stakeholders, including other federal, local and state

agencies, industry and the boating public. In addition, the U.S. Coast Guard issued regulations to enact MTSA provisions and align domestic regulations with the maritime security standards of SOLAS and the ISPS Code. The MTSA requires port facilities and ships to undertake vulnerability assessments aimed at developing risk-based security plans. Addressing these risks requires the implementation of screening procedures, security patrols, restricted areas, identification procedures, access controls and surveillance equipment.

The Container Security Initiative (CSI) is a series of security measures adopted by U.S. Customs in January 2002 to extend their container screening process outwards to foreign ports. CSI has four key components:

- Identifying high-risk containers by having more detailed electronic cargo manifests provided to U.S. Customs 24 hours prior to loading the containers in a foreign port.
- Pre-screening high-risk containers by having U.S. Customs officers stationed in foreign ports. A reciprocal arrangement enables foreign nations to place their customs officials in U.S. ports to screen their inbound containers. Only Canada and Japan have exercised this reciprocal privilege.[17]
- Using sophisticated detection technology to screen high-risk containers such as mobile gamma/x-ray and radiation detection monitors.
- Developing more secure containers to ensure their integrity including electronic seals and motion/light detectors to warn of any attempt to penetrate a secured container.

The benefit of joining the voluntary CSI is that containers pre-screened in foreign ports will not be re-checked at the US port of discharge. The first three ports joining the CSI were Halifax, Montreal and Vancouver in March 2002. Other major world ports followed Canada's lead. Currently 58 major ports in various parts of the world participate in the CSI program.[18]

The CSI is has its critics, who see the program as being beneficial from a security perspective only to the U.S. and not the host country

and port.[19] The earlier time frame for submitting electronic manifests inconveniences the supply chain and adds cost to shippers.[20] Ports also have to provide additional storage for export containers arriving in the container terminal earlier.

The November 2001 Customs – Trade Partnership Against Terrorism (C-TPAT) is a voluntary program aimed at securing and facilitating the flow of goods into the U.S. By 2004, some 7,400 companies were enrolled in this supply chain security program. These companies include importers, customs brokers, terminal operators, domestic and international carriers and foreign manufacturers. The program's guiding principles are voluntary participation and jointly developed security criteria, best practices and implementation procedures. C-TPAT partners work with U.S. Customs and Border Protection (CBP) to protect their supply chains from concealment of terrorist weapons. In support of this program, CBP sends teams of supply chain specialists around the globe to visit partners, their vendors, and vendors' plants to validate that their supply chain security meets C-TPAT minimum-security criteria and best practices. In exchange for their participation in C-TPAT, CBP offers reduced inspections at U.S. ports and expedited processing at the border. Further, CBP continues to provide implementation tools and incentives for the private sector to join C-TPAT. This instrument is a prerequisite for the Free and Secure Trade (FAST) program and other CBP expedited processing programs.[21]

The *Security and Accountability for Every Port Act* (SAFE) was adopted on October 13, 2006. The Act codified into law a number of programs to improve security of U.S. ports, such as: creating Transportation Worker Identification Credentials (TWIC), establishing interagency operational centers for port security, providing a Port Security Grant Program for construction, training, sharing threat information, ensuring all containers entering U.S. ports are scanned through non-intrusive imaging and radiation detection by 2009.

The SAFE Act requirement for 100 percent scanning was and continues to be highly controversial. Currently, about 5 percent of

suspected high risk containers are scanned with a fraction of them being physically inspected.[22] A 100 percent inspection at U.S. ports would dramatically delay trade and add costs to shippers. The concern is two fold: the time needed for the full scanning in radiation portals and gamma/x-ray inspections, and the necessity of significant additional personnel to quickly interpret the results. The difficulties facing 100 percent scanning led to an extension of the legislated deadline to 2014 with the expectation that much of the scanning will be undertaken in foreign ports.[23] For example, all major container terminals in Canada have radiation detectors for 100 percent scanning with supplementary mobile gamma ray inspections as required. Given the importance of U.S. bound containers coming through Canadian ports, a 100 percent scanning process could readily be undertaken. On the other hand, the European Union concluded that the U.S. proposal for 100 percent scanning would be excessively costly, not improve global security, divert resources from current security initiatives and disrupt trade. The EU suggests that priority be given to enhancing multi-layered risk management systems targeting dangerous cargo and strengthening international cooperation to improve supply chain security.[24]

Another key element in the SAFE Ports Act is the requirement for TWIC cards to be provided for port and transport workers accessing secure areas. As of December 2009, more than 1.4 million port employees, longshoremen, truckers, merchant mariners and others had enrolled in the program. TWIC cards are currently used as a flash pass; the next stage is to introduce biometric elements such as the holder's fingerprint to the card.[25] A further TWIC concern is the inability of some seafarers to have shore leave – a long-term traditional right of seafarers. Not only does shore leave offer a break from the monotony of long ocean voyages, it provides sailors with needed access to medical care and facilities not found aboard their ships. There is ongoing controversy about the need for a universal TWIC card for seafarers to enable them to go ashore in U.S. and other ports.

***Canada***

Given the significant degree of economic integration of Canada and the U.S., steps were taken quickly after the September 11th terrorist attack to increase security in all sectors, including marine transportation and ports. Canadian authorities quickly acceded to the IMO's ISPS Code and port authorities began to assess their security systems and develop appropriate risk management plans. Transport Canada was designated as the federal agent responsible for implementing the ISPS Code.

Initially, the ports community was concerned that there was no integrated national strategy on how port facility risk assessment plans were to be undertaken nor were there standards being provided by Transport Canada on how they were going to evaluate the resultant security plans. Transport Canada officials indicated that all major ports were proceeding in an appropriate manner in undertaking their own security risk assessments and that their eventual security plans would likely be compliant with the ISPS Code requirements. Canada's Marine Transportation Security Regulations (MTSR), incorporated in Section 5 of the M*arine Transportation Security Act of 1994* were published in the *Canada Gazette Part II* on June 2, 2004 (less than a month before the IMO's implementation deadline). Port facility security plans were approved under these Regulations.

The 2004 MTSR is currently undergoing a major review with amendments being proposed to strengthen the regulatory framework by addressing gaps, ambiguities and omissions. In addition the proposed MTSR amendments clarify interpretations and improve their harmony with major international partners, notably the U.S. There is an ongoing extensive stakeholder consultation process based on preliminary discussions in 2008-09, and current cross-country consultations in 2010. The expectation was that an amended MTSR would be brought to Parliament in late 2010.[26]

Financial support was provided to Canadian ports to assist in implementing their port facility security plans through the Marine Security Contribution Program, announced on May 7, 2004. The federal government provided a three-year special commitment of $115 million as a 75:25, federal - port cost sharing approach. These

funds were used by many ports to install security fencing, CCTV cameras, enhance security at access points, develop secure areas, acquire appropriate security equipment, develop secure communication systems and so forth. Although the federal funds were appreciated and well used by Canadian ports, the government's financial support was relatively modest in comparison to funding that was provided and continues to be offered to U.S. ports. By 2006, they had received $876 million from the Department of Homeland Security from their Port Security Grant program.[27] In the 2009, the U.S. government allocated $787 billion in the *American Recovery and Reinvestment Act* including an additional $800 million earmarked for port security funding. Transport Canada is currently evaluating the Marine Security Contribution Program as the ports and shipping community advocate a renewed program to ensure Canadian ports remain competitive with their US counterparts.

The federal government provided funds not only for port physical security but also for federal agencies involved in marine related security. In 2004, the federal government's *Securing an Open Society: Canada's National Security Policy,*[28] allocated $432 million to Transport Canada, National Defence, Public Safety and Emergency Preparedness Canada, RCMP and Fisheries and Oceans to: establish Marine Security Operations Centres, increase the on-water presence of various agencies, increase aerial surveillance by Fisheries and Oceans, provide secure fleet communications, enhance closer cooperation with US marine security agencies, initiate background security checks for port workers and work with international partners to develop new technologies such as electronic seals, GPS tracking and embedded computer chip technology to identify container breaches.

The federal government provided radiation portal monitors and mobile gamma/x-ray inspection units for Canada's major container terminals. These inspection devices have led to a 100 percent radiation detection of all containers and readily available radiographic inspection of identified high-risk containers. In addition, security personnel can carry portable handheld detection devises to sniff trace amounts of contraband, explosive and other materials. The radiation

portal monitors provide passive, non-intrusive screening for radiation leaks from nuclear devices. The gamma/x-ray devices allow security staff to see inside the container in a fast and effective manner to enable them to compare the actual contents against the declared items.[29]

The operation of radiation portals caused some operational problems in processing containers. Each container's radiation results are transmitted to the CCG operations centre in Ottawa. If radiation is detected, which could well be from a benign source, a notice is sent to the regional CCG which then notifies the terminal operator. By this time, the suspect container has likely been placed in the stacks in the container yard. It then has to be retrieved and moved to a secure area for additional testing. These additional container moves are time consuming and costly.

The federal government initiated a Marine Transportation Security Clearance Program (MTSCP) in January 2003 to introduce background checks of workers at marine facilities and ports. Similar to the U.S.'s TWIC, MTSCP's purpose is to reduce the risk of security threats by conducting background checks on marine workers who perform certain duties or who have access to certain restricted areas. The MTSCP was not a new program, but rather, an expansion of the existing Transportation Security Clearance Program, which has been in place at Canada's airports since 1985. Steps are being taken to harmonize with the U.S. to achieve reciprocity with respect to Canadian and U.S. security credentials. MTSCP continues to be developed with designated port workers being cleared as required. However, in spite of this, issues still arise in the ports community over the need for a national, uniform Transport Worker Identification Card (TWIC) so that truck drivers and others serving multiple ports such as seafarers do not need to be cleared several times and issued with different cards for each port served.

**Conclusion**

Canada's maritime and ports industry have taken significant steps to enhance the security of the country's export and import trade. Many

of the security programs have complemented similar steps in the U.S. It was sensible to develop a cooperative and integrated approach given the high degree of economic integration between the two countries and our extensive shared border. A substantial amount of cargo flowing through Canadian ports is destined for the U.S.; hence it is in Canada's best interest to ensure the security integrity of our ports and maritime trade.

Transport Canada, as the federal government's lead department for transportation security has taken several major steps to improve security in the maritime sector. These include supporting the implementation of the IMO's ISPS Code, providing program funds for identified port facility security enhancements, initiating and developing the Transport Workers Identification Card system, and taking the lead in the Transportation Sector Network of the Canada's National Critical Infrastructure program.

Despite these many advances, more needs to be done to enhance ports and marine security without hampering the flow of trade. Further program funding to support additional port facility security initiatives is essential. Canadian ports must be as secure as their competitive U.S. counterparts or trade will inevitably be diverted south to the detriment of our national economy.

**Endnotes**

[1] M. Levinson, *The Box: How the Shipping Container made the World Smaller and the World Economy Bigger,* Princeton University Press, Princeton NJ, 2006.
[2] UNCTAD, *Review of Maritime Transport 2010*, United Nations, New York, 2010, Figure 2.1, p. 31.
[3] Drewry, "Container Forecaster – June: 2Q09", Drewry Shipping Consultants, London UK, 2009, p. 6.
[4] W. Kemmsies, "2011 Better, not great", *American Shipper*, pp. 14-17, December, 2010.
[5] P.M. Marlow, "Maritime Security: an update of key issues", *Maritime Policy & Management*, 37:7, December 2010, pp. 667-676.
[6] Thucydides, *The Landmark Thucydides: A Comprehensive Guide to the Peloponnesian War,* Trans. R. Crawley, Touchstone, New York, 1998, p. 1.8
[7] "Record high-seas hostage taking in 2010", *American Shipper*, on-line edition, January 8, 2011
[8] T. A. Mensah, "The Place of the ISPS Code in the Legal International Regime", *WMU Journal of Maritime Affairs,* 3:1, 2003, pp. 17-30.

[9] IMO Assembly resolution 544 (14) adopted on November 20, 1985.
[10] 1988 SUA Convention, Art. 3, sub-paragraphs 1 (b) – (g) and paragraph 2.
[11] IMO Assembly 942 (22) of December 2001.
[12] "Maritime Security on agenda as USCG Commandant visits IMO", http://www.imo.org/Newsroom/mainframe.asp?topic_id=892&doc_id=4714 (accessed, April 12, 2010)
[13] UNCTAD, *Review of Maritime Transport 2009*, United Nations, New York, 2009, p.142.
[14] A. Bartley, "Policy Update", Marine Security Standing Committee, Canadian Marine Advisory Council, Ottawa, April 26, 2010.
[15] P. Metaparti, "Rhetoric, rationality and reality in post-9/11 maritime security", *Maritime Policy & Management*, 37:7, December 2010, pp. 723-736.
[16] K. Nagle, "Five years after 9/11: U.S. Ports More Secure Than Ever", Press Release, American Association of Port Authorities, Alexandria VA, September 1, 2006.
[17] P. Metaparti, *op. cit.*
[18] US Department of Homeland Security, "Container Security Initiative Ports", http://www.dhs.gov/files/programs/gc_1165872287564.shtm (accessed April 12, 2010)
[19] P. Metapaerti, *op.cit*.
[20] Y.C. Yang, "Impact of the container security initiative on Taiwan's shipping industry", *Maritime Policy & Management*, 37:7, December 2010, pp. 699-722.
[21] US Customs and Border Protection, *Securing the Global Supply Chain: Customs-Trade Partnership Against terrorism (C-TPAT) Strategic Plan*, Washington DC, November 2004, p. 2.
[22] P. Metaparti, *op. cit.*
[23] E. Kulisch, "False Positive: DHS rolls back 100% scanning deadline to 2014", *American Shipper*, 52:1, January 2010, pp. 8-10.
[24] "EU Commission critical of US plans for 100 percent box scanning", *Container Management Magazine*, March 30, 2010.
[25] P.S. Abbott, "Effective security must focus on collaboration, technology", *AAPA Seaports*, 18, winter 2009, pp. 12-16.
[26] D. Fuller, "Regulatory Update", Marine Security Standing Committee, Canadian Marine Advisory Council, Ottawa, April 26, 2010.
[27] K. Nagle, *op. cit.*
[28] Privy Council Office, *Securing and Open Society: Canada's National Security Policy*, Ottawa, April 2004.
[29] L. Anderstrem, "Intelligent security planning for ports", *Port Technology International*, January 26, 2010.