Chapter 11

The Challenge of Maritime Security against Terrorism: A Dialogue Between the European Union and Canada

Kamrul Hossain, Hugh M. Kindred, and Mary R. Brooks

11.1. Introduction

For centuries the principal threat to maritime security has been piracy at sea. Its suppression has been the object of customary international law throughout the history of maritime navigation. The law against piracy was eventually codified first in the 1958 Convention on the High Seas,[1] and subsequently in the United Nations Convention on the Law of the Sea in 1982 (LOS Convention).[2] However, the concept of piracy was narrowly defined[3]—in general as attacks on ships at sea from other vessels for the private gain of the pirates—despite the fact that it was declared a universal crime under both conventions.

Today, maritime security involves a broader concept of piracy at sea as well as many other threats to marine navigation. Maritime security risks now also include drug smuggling, human trafficking and threats to marine bio-security, such as the introduction of alien diseases and organisms. Amongst the wide range of threats, terrorism against shipping has become a primary concern, especially since 11 September 2001. Unlike traditional pirates (who are still an active security risk), the perpetrators of terrorist attacks on shipping do not necessarily operate from vessels other than the ships they are attacking. Indeed, their attacks may be to use the targeted ship as the means to deliver a bomb to their selected destination or to employ the ship itself as a weapon. Most important, the perpetrators may not necessarily act with a view to any personal gain for themselves.

The expanded range of security threats poses serious risks to the safety of the ships, the ports they sail to, and the persons aboard them, as well as added danger to the cargoes they are carrying. After the terrorist attacks of

---

[1] *Convention on the High Seas*, 450 *U.N.T.S.* 82, Articles 15–22.

[2] *United Nations Convention on the Law of the Sea*, U.N. Doc. A/CONF.62/122, (1982) 2 *I.L.M.* 1261 [hereinafter LOS Convention], Articles 100–107.

[3] See Z. Keyuan, "Implementing the United Nations Convention on the Law of the Sea in East Asia: Issues and Trends," *Singapore Year Book of International Law* 9 (2005):1–17, p. 8.

11 September 2001, the global perception of these threats led the international community to consider ways to combat them. As a result, new instruments and rules have been developed, not necessarily to replace the existing law but rather to supplement it and make it more suitable and effective in the new circumstances. These developments at the international level are ongoing and, moreover, require action at a national level to implement them. In this process, at both the multilateral and the regional/national levels, the European Union (EU) and Canada have been active. Their participation internationally and their law and policy making individually are the subject of this contribution, in which a comparative analysis will be made of their attempts to address the common problems of maritime terrorism.

The current regulatory response to the worldwide threat of maritime terrorism is a multilateral platform developed primarily from 2001 through 2005 by the complementary efforts of several international organisations operating in different global sectors. The backbone of this platform is the International Ship and Port Facility Security (ISPS) Code[4] promulgated by the International Maritime Organisation (IMO). The preventive measures of this Code are backed up by new penal proscriptions and penalties that IMO added to an amended convention to suppress criminal acts against world shipping. The ISPS Code to promote the security of ships and ports is also supported by a variety of protective measures taken by the World Customs Organization (WCO) towards cargoes, the International Labour Organization (ILO) regarding seafarers and the International Organization for Standardization (ISO) respecting freight containers.

In addition to these multilateral initiatives, some countries have taken significant unilateral steps to protect their trade and shipping through national legislation and regulations. One of these is the United States (US), which has legislated a number of regulatory requirements with both domestic and international effect. Some of these measures, especially those mandated by the *Maritime Transportation Security Act 2002*[5] (MTSA) and the *Security and Accountability for Every Port Act 2006*[6] (SAFE Port Act), exceed the

[4] International Maritime Organization (IMO), Amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974 [SOLAS] made by the Conference of Contracting Governments in Resolution 1, Annex Art.7 which inserted a new Chapter XI-2 on Special Measures to Enhance Maritime Security [SOLAS Annex XI-2], which, in turn, imported the ISPS Code adopted by Resolution 2, 12 December 2002 (in force 1 July 2004), SOLAS/CONF.5/31.

[5] *Maritime Transportation Security Act*, 2002, Pub. L. No. 107-295, 116 Stat. 2064 (codified at 46 USC§2101) [hereinafter MTSA].

[6] *Security and Accountability for Every Port Act*, 2006, Pub. L. No. 109-347, 120 Stat. 1884 (codified at 46 USC§901) [hereinafter SAFE Port Act].

regulatory demands of the multilateral platform. Given the major role the United States plays in world trade and shipping, the extra-territorial effects of its national security regulations add another dimension to the international regime.

Both the EU and Canada have had to respond to these maritime security developments. Each, in fact, participated in the preparation and implementation of the multilateral platform of maritime security, although by differing means and extent of application. In addition, both have had to react to the extra demands of American authorities in pursuit of their national requirements on any trade to US destinations. Hence, this chapter will first briefly explore the current international maritime security regime before, second, examining the extent of its implementation by EU and Canada. Third, the chapter will investigate how the EU and Canada are individually pursuing port and shipping security beyond the present multilateral platform, taking into account their cooperative arrangements with the United States. Finally, the chapter will engage in a dialogue comparing the similarities and differences in the approaches of the EU and Canada in order to understand if there are opportunities for strengthening maritime security.

11.2. Current Maritime Security Regime

11.2.1. The Multilateral Platform

The centrepiece of the multilateral regime of maritime security is the ISPS Code, which was promulgated by IMO in 2002 and brought into force nearly universally on 1 July 2004. Although this Code provides a highly comprehensive platform for the security of merchant ships and the marine facilities at which they call, it does not operate as a complete regime for lack of attention to the seafarers who work them, the freight containers they move and to the cargoes they carry in international trade. Other international organisations with sectoral responsibilities for these activities have also taken steps to bolster security measures. Thus the multilateral platform of marine security currently comprises rules and guidelines established by IMO, WCO, ILO and ISO, as will now be explored.

11.2.1.1. ISPS Code for Ships and Ports

The tragic events of 11 September 2001 transformed the international security situation into a much more comprehensive set of problems. In respect of maritime security, it was quickly realised that a ship itself can be used as an instrument or a threat of terrorist activities; the mere prevention of potential attacks against ships, persons and property at sea is, therefore, not sufficient. In effect, the international community recognised that terrorism at sea, from whatever motives, poses a serious threat not only to the international trade and transport system but also to the security of international society as a whole. Hence, the Maritime Safety Committee of IMO gave urgent consideration to the need for new practical measures to safeguard the world's ships, ports, offshore terminals, and other marine facilities against threats from terrorist attacks. The Committee determined that the risks to shipping required a regulatory regime covering both ships and the ports they visit.[7] As a result, the ISPS Code was developed, and given international legal force by incorporation in the International Convention on the Safety of Life at Sea, 1974 (SOLAS) under Chapter XI.[8] As Chapter XI previously covered ship safety and security, it was split by the introduction of these amendments into two new chapters—Chapter XI-1 and Chapter XI-2—the former including special measures to enhance maritime safety while the latter provides special measures to enhance maritime security. The ISPS Code itself is found in Chapter XI-2.

There are two parts in the ISPS Code. Part A covers mandatory requirements for maritime security measures while Part B provides guidelines on how those requirements could be met. Although Part B is not mandatory, some national governments have chosen to make it compulsory.[9]

In addition to addressing international maritime security concerns about terrorism, the Code establishes clear and identifiable roles and responsibilities, and provides a platform for the collection and exchange of security intelligence. Overall, the Code is designed to improve security as it recognises that the ship/port interface is a vulnerable node in the transport system. The Code

[7] See T. A. Mensah, "The Place of the ISPS Code in the Legal International Regime for the Security of International Shipping," *WMU Journal of Maritime Affairs* 3 (2003): 17–30, p. 24.
[8] IMO, n. 4 above. See also: International Maritime Organization (IMO), "IMO Adopts Comprehensive Maritime Security Measures," (2002), available: <http://www.imo.org/Newsroom/mainframe.asp?topic_id=583&doc_id=2689> (retrieved 3 December 2008), "International Ship & Port Facility Code (ISPS) What it is exactly – and what is it meant to do," available: <http://www.iaasp.net/2003%20PDF's/ISPS%20Code.pdf> (retrieved 4 December 2008) and "ISPS Code for ITIC Members," available: <http://www.itic-insure.com/downloads/publications/isps_code/ISPS_background_info.doc> (retrieved 4 December 2008).
[9] See "ISPS Code for ITIC Members," n. 8 above.

provides both "identity" and "transparency" to the players in the international shipping network.[10] Contracting governments, as part of their overall maritime security risk management programmes, establish designated authorities within government to fulfil their security responsibilities under the Code but may also delegate the undertaking of certain of the responsibilities to non-governmental Recognised Security Organisations.

Under the ISPS Code, there are three designated levels of security—Normal (Level 1), Increased (Level 2), and High (Level 3). Level 1 assumes a normal situation and requires the implementation of minimum security measures. Level 2 indicates that there is a heightened risk of a security incident requiring enhanced security measures, and Level 3 signals that there is a probable or imminent risk of a security incident. The contracting government has the right to decide the extent and application of Part A of the Code to a port facility within its territory that is only occasionally required to serve ships arriving or departing on an international voyage.[11] Paragraph 5 of Part B of the Code requires a Declaration of Security (DOS) to be issued when the contracting government of the port facility or the ship deems it necessary. It is expected that a DOS will be necessary when an arriving ship has a different security level (for example 3) than the port at which it will call (which may have a 2).[12]

The Code applies to ships engaged on international voyages and all port facilities that serve the ship for such voyages. Ships subject to the ISPS Code are passenger ships (including high speed passenger craft); cargo ships (including high speed craft) of 500 gross tonnes or more; and mobile offshore drilling units. By 1 July 2004, the date on which the ISPS Code became operative, every shipping company had to obtain an International Ship Security Certificate (ISSC) from an authorised shipping society. A ship lacking a valid ISSC would, by definition, be in violation of ISPS Code requirements.[13] Furthermore, every ship subject to the ISPS Code must have installed a Ship Security Alert System, which is a covert alarm that alerts authorities ashore.

By itself, a legal regime cannot physically prevent acts of terrorism against ships or port facilities.[14] Co-operative action is necessary and that, it was recognised, must involve not only governments and shipowners but also all

[10] Mensah, n. 7 above, p. 26.
[11] SOLAS Annex XI-w, n. 4 above, Part A, paragraph 3.2.
[12] Mensah, n. 7 above, p. 26.
[13] See "Establishment of U.S. Antiterrorism Maritime Transportation System," *American Journal of International Law* 98 (2004): 588–590, p. 589. See also Germanischer Lloyd AG, "Information on ISPS Code Certification," (2004), available: <http://www.tis-gdv.de/tis/tagungen/workshop/2004/eggers2.pdf> (retrieved 5 December 2008), p. 5.
[14] Mensah, n. 7 above, p. 29.

other persons and entities that play a role in trade by sea. The ISPS Code mandates such cooperation. The Code provides an integrated mechanism for promoting and enhancing overall maritime security, which, in turn, ensures the effective implementation of the SOLAS Convention as well as other international and national rules and regulations for preventing unlawful acts against or involving ships.[15]

11.2.1.2. SUA Convention against Maritime Terrorists

As a complement to the prevention of terrorism against ships and ports under the ISPS Code, the IMO also addressed the prohibition of maritime terrorism. In 1985, after the *Achille Lauro* incident,[16] both IMO and the General Assembly of the United Nations adopted resolutions calling for measures against acts that threaten the safety of ships and the security of the ships' crew and passengers.[17] In response, the IMO took the initiative to prepare and conclude the 1988 Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation (SUA Convention).[18] At the same time it adopted a similar set of provisions in a Protocol for the protection of fixed platforms located on the continental shelf.[19]

The primary purpose of the SUA Convention is to ensure that appropriate action is taken against persons committing unlawful acts against shipping, whether for private or political gain.[20] The proscribed acts include seizure of the vessel by force; violence against persons on board; and the placing of shipboard devices likely to damage or destroy the vessel.[21] The Convention also obliges

[15] Id.
[16] On 3 October 1985, a group of Palestinian guerrillas hijacked the Italian cruise ship, *Achille Lauro*, in Egyptian territorial waters; it was considered a milestone event in modern vessel security concerns. See Keyuan, n. 3 above, p. 8, note 30. See also Mensah, n. 7 above, pp. 18–19.
[17] International Maritime Organization (IMO), Assembly Resolution 544 (14) adopted on 20 November 1985 and UNGA Res. 40/61 adopted on 9 December 1985 respectively.
[18] *Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation*, done 10 March 1988 (in force 1 March 1992), 1678 *U.N.T.S.* 221 (1992), 27 *I.L.M.* 627 (1988), available: <www.imo.org/home.asp?topic_id=910> (retrieved 4 December 2008) [hereinafter Convention for Suppression of Unlawful Acts].
[19] *Protocol for the Protection of Fixed Platforms Located on the Continental Shelf*, 27 *I.L.M.* 685 (1988).
[20] Keyuan, n. 3 above, p. 10.
[21] Convention for Suppression of Unlawful Acts, n. 18 above, Article 3(1).

contracting governments either to prosecute or extradite alleged offenders.[22] The most important aspect of this Convention is that even if terrorist acts cannot be suppressed under the LOS Convention, they may now be punished under the SUA Convention.

While the 1988 SUA Convention overcame many of the limitations of the law of the sea against piracy, more recent incidents, especially the attacks of 11 September 2001, have demonstrated that it was still too restricted in scope to deal with modern maritime terrorism. Hence, in 2005, IMO concluded an amending Protocol to the SUA Convention[23] that enlarged the bans on criminal acts and terrorist attacks on shipping.[24] The Protocol prohibits the carriage of persons known to have committed an offence under the SUA Convention.[25] It also strengthens the international response to the proliferation of weapons of mass destruction by criminalising their illicit shipment by sea. The Protocol additionally provides ship-boarding provisions to enhance the collective ability to take action against such traffic.[26]

11.2.1.3. WCO Guidelines for Cargoes

In light of the development of integrated supply chains in the delivery of international trade, the World Customs Organization[27] has moved to simplify the customs procedures that impede the flow of goods across national frontiers by means of the International Convention on the Simplification and

---

[22] Id., Article 10. And see *Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, 1988 to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, 1988*, available: <http://www.imo.org/Conventions/mainframe.asp?topic_id=259&doc_id=686> (retrieved 3 December 2008).

[23] *Protocol of 2005 to the Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf*, IMO/LEG/CONF/15/22, 1 November 2005, available: <http://www.state.gov/documents/organization/58425.pdf> (retrieved 3 December 2008). Similar amendments were made simultaneously to the 1988 Protocol concerning attacks against fixed platforms.

[24] The Protocol particularly criminalises the use of explosives, radioactive material and biological, chemical and nuclear weapons on or against shipping in a manner that is likely to cause serious injury or death when the purpose of the act, by its nature or context, is to intimidate a population or to compel a government or international organisation to act in a desired way. Id., Article 2(bis).

[25] Id., Article 3(bis).

[26] Protocol of 2005, n. 23 above.

[27] Formally called the Customs Co-operation Council.

Harmonization of Customs Procedures (as amended by Protocol),[28] ordinarily known as the Revised Kyoto Convention of 1999. Building on this foundation, the WCO has since taken steps on several regulatory levels to enhance the efficiency and security of international trade. It began with the 2002 Resolution of the Customs Co-operation Council on Security and Facilitation of the International Trade Supply Chain,[29] which set out a programme of action for both the organisation and individual member states.

Pursuant to this action plan, the WCO subsequently elaborated a number of guidelines and frameworks for specific trade facilitation and security tasks, of which the most significant ones are mentioned here. First, the High Level Guidelines for Co-operative Arrangements between Members and Private Industry to Increase Supply Chain Security and Facilitate the Flow of International Trade, promulgated in 2003,[30] supply directions for the enhancement of co-operation between traders and national customs authorities. Then in June 2004, the WCO published a companion set of Customs Guidelines on Integrated Supply Chain Management,[31] which mandated an integrated and secure control chain between national customs based on the best practices of risk management, and recommended requirements for a Unique Consignment Reference for Customs Purposes[32]; the latter is intended to provide continuity of the audit trail of a shipment from origin to destination.[33]

---

[28] *International Convention on the Simplification and Harmonization of Customs Procedures*, Brussels, 26 June 1999 (in force 3 February 2006), available: <http://www.wcoomd.org/kybodycontent.htm> (retrieved 4 December 2008).

[29] Resolution of the Customs Co-operation Council on Security and Facilitation of the International Trade Supply Chain, 2002, available: <http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Resolutions/Security_Facilitation_Int_Trade_Supply_Chair.pdf> (retrieved 4 December 2008).

[30] See n. 28 above, Annex VII to Doc. SP0122E1, Doc. No. TF0004E3 (2003). See also the *International Convention on Mutual Administrative Assistance in Customs Matters*, Brussels, 27 June 2003 [hereinafter the Johannesburg Convention], available: <http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Conventions/Internconvmutualadmineng2003.pdf> (retrieved 3 December 2008).

[31] World Customs Organization website at <http://www.wcoomd.org> (retrieved 3 December 2008).

[32] Recommendation of WCO Concerning a Unique Consignment Reference (UCR) for Customs Purposes, and accompanying Guidelines, 26 June 2004, available: <http://www.wcoomd.org/pftoolsuchrecomm.htm> (retrieved 3 December 2008).

[33] WCO also sought to encourage the widest use of electronic transmissions of customs data, appropriately protected by security technology, by the adoption of a revised Recommendation Concerning the Electronic Transmission and Authentication of Customs and Other Regulatory Information, 24 June 2005, available: <http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Recommendations/RecommendationsIT_16_June_1981_eng.pdf> (retrieved 3 December 2008).

In June 2005, a WCO Resolution adopted these guidelines in the Framework of Standards to Secure and Facilitate Global Trade (SAFE Framework).[34] This Framework is built on the concept of customs-to-customs networking and customs-to-business partnering. It emphasizes harmonisation of electronic customs information, consistent use of a risk management approach to security, and operation of non-intrusive detection equipment. When these principles of customs operations are coupled with a Seal Integrity Programme for Secure Container Shipments, the security of the supply chain for cargo movement across borders is assured.[35] Incorporated into the SAFE Framework is the idea that any business operator that is party to an international supply chain in any way, and is approved by its national customs organisation as complying with WCO or equivalent security standards, may be designated an authorised economic operator (AEO) and thus receive faster processing and less attention from customs. Pursuant to this concept, the AEO Guidelines were prepared and adopted by WCO Resolution in June 2006 as an additional appendix to the SAFE Framework.[36] It should be noted that there is often no link between those operating with authority under the ISPS Code and those acting under authority granted by a country's adoption of WCO guidelines.

11.2.1.4. ILO Convention for Seafarers

Commensurate with the work of the IMO on ship security, the International Labour Organization recognised the need to review the security status of ships' crews both for their own safety and that of the ports they may visit. Hence, the ILO undertook a revision of its existing principles on seafarers' credentials and prescribed a new model document in the Seafarers' Identity Documents Convention (Revised), 2003.[37] The security of this document is assured, so far

---

[34] Framework of Standards to Secure and Facilitate Global Trade [hereinafter SAFE Framework], available: <http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Conventions/Framework%20of%20Standards%20to%20Secure%20and%20Facilitate%20Global%20Trade.pdf> (retrieved 4 December 2008). And see speech of Michael Schmitz, Director of Compliance and Facilitation, WCO, to the United Nations Security Council, 23 February 2007, available: <http://www.wcoomd.org/speeches/default.aspx?lid=1&id=57> (retrieved 3 December 2008).

[35] SAFE Framework, id., Appendix to Annex 1.

[36] Resolution of the Customs Co-operation Council on the Framework of Standards to Secure and Facilitate Global Trade, June 2006, available: <http://www.wcoomd.org/files/1.%20Public%20files/PDFandDocuments/Resolutions/Framework_of_Standards_to_Secure_and_Facilitate_Global_Trade_(june_2006).pdf> (retrieved 4 December 2008), para. 3.3.

[37] *International Labour Organization (ILO) Convention No. C185, Seafarers' Identity Documents Convention (Revised), 2003*, Geneva, 19 June 2003 (in force 9 February 2005),

as possible, by the use of durable materials and security features that inhibit tampering or falsification and a machine readable zone of information. The identity of the holder is established by a photograph and customary personal data together with a biometric template based on a fingerprint inscribed as a bar code.[38]

11.2.1.5. ISO Standards for Secure Freight Containers

A crucial component in the security of cargo stuffed in a container is the integrity of the seal on its lock. The International Organization for Standardization has taken steps to ensure such integrity by setting standards for high security container seals. Its published standard establishes uniform procedures for the classification and acceptance or withdrawal of mechanical freight container seals.[39] Further, the ISO is working towards the introduction of a standard for electronic container seals. This project includes work on the transmission and identification of a seal and a system for verifying the accuracy of its use, along with data protection and authentication of the electronic device.[40]

11.2.2. United States' National Initiatives

On 25 November 2002, the United States implemented the ISPS Code by passing the *Maritime Transportation Security Act of 2002* (MTSA),[41] with effect on 1 July 2004, the same day the ISPS Code came into force. In addition to the base requirements of the ISPS Code noted previously, the MTSA instituted additional ones aimed at further reducing the vulnerability of US marine container supply chains. Since its implementation, there have been

---

available: <http://www.ilo.org/ilolex/cgi-lex/convode.pl?C185> (retrieved 4 December 2008), Annex 1.

[38] Two fingerprints are used to create a biometric template, which is then loaded into a chip in the Seafarer's Identity Document and may be read as an international barcode: see DDCOM, "Seafarers identity becomes clearer: New international labour Convention for seafarers' ID documents comes into force," *World of Work Magazine* 53 (2005), p. 35.

[39] ISO/PAS 177712:2006 in ISO, *ISO Standards Handbook: Freight Containers*, 4th ed. (2006).

[40] Freight containers – Mechanical seals, ISO/PAS 17712:2006, available: <http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=42791&ICS1=55&ICS2=180&ICS3=10> (retrieved 4 December 2008).

[41] See MTSA, n. 5 above.

a number of refinements to the initial requirements,[42] and coverage has been expanded under the SAFE Port Act 2006,[43] discussed later. However, complete implementation of the US maritime security regime is highly unlikely as the US Coast Guard is hard pressed to recruit and train an adequate number of inspectors, let alone meet other requirements of the SAFE Port Act 2006.[44]

One addition to the base regime is the 96-hour rule, which requires all vessels that will call at a US port to provide the US government with a detailed notice of arrival 96 hours in advance of their arrival at their first US port of call. This information enables the US government to determine if the vessel poses a threat to US interests and to allocate its security resources to those vessels it deems warrant closer scrutiny.

A second addition, the 24-hour rule, requires both liner companies and non-vessel operating common carriers to provide the US government with a notice about each cargo container and its contents 24 hours in advance of its loading in a foreign port. This rule enables the US government to identify marine containers that are suspicious prior to being loaded and to target them for additional inspection. These two rules form a part of the programme known as the Container Security Initiative (CSI); the CSI places US customs officers in foreign ports and enables US Customs and Border Protection to optimise the advantages offered by the Department of Homeland Security's risk assessment tool—the Automated Targeting System.

The extraterritorial nature of this second rule in particular is quite wide-ranging. As of 5 October 2007, 58 CSI ports accounted for 85 percent of all traffic bound for the United States.[45] A majority of the largest container ports in the world are members of the Container Security Initiative, including 23 EU ports and three Canadian ports.[46] Exceptions, however, include some of the largest container ports in the world—Dalian, Guangzhou, Ningbo-Zhoushan, Qingdao, Tianjin and Xiamen in China as well as other large container ports in Egypt (Port Said), India (Jawaharlal Nehru), Indonesia (Tanjung Priok), Japan

[42] Government Accountability Office, *Cargo Security: Partnership Program Grants Importers Reduced Scrutiny with Limited Assurance of Improved Security*, D-05-404 (Washington, DC: Government Accountability Office, 2005).

[43] See SAFE Port Act, n. 6 above.

[44] Government Accountability Office, *Maritime Security: Observations on Selected Aspects of the SAFE Port Act* (GAO-07-754T) (Washington, DC: Government Accountability Office, 2007).

[45] US Customs and Border Protection, *Container Security Initiative Ports*, available: <http://www.dhs.gov/xprevprot/programs/gc_1165872287564.shtm> (retrieved 4 December 2008).

[46] The official US CSI web site indicates the three Canadian ports are Vancouver, Montreal and Halifax, while the Canadian Department of International Trade web site reports four, including Saint John.

(Osaka), the Philippines (Manila), Saudi Arabia (Jeddah) and Vietnam (Ho Chi Minh).[47]

In addition to the MTSA and the CSI, the United States has more recently initiated the Secure Freight Initiative (SFI) under the umbrella provided by the SAFE Port Act of 2006. This programme, established by the Department of Homeland Security in December 2006, focuses on freight screening in foreign ports. SFI programme funding is from the US budget and its initial phase deployed nuclear detection devices to six foreign ports, some deemed high risk—Port Qasim (Pakistan), Puerto Cortes (Honduras), and Port Salalah (Oman)—and others in significant trade originating markets—Southampton (United Kingdom), the Gamman Terminal at the Port of Busan (Korea), and Singapore.[48] Marine containers at these ports are scanned for radiation before being loaded for the United States. Unlike the Automated Targeting System, in the case where an alarm is sounded, both host country officials and the Department of Homeland Security are simultaneously notified. Again security of cargo (and by implication vessel) are addressed outside the United States and before the vessel sails.

The United States has also implemented a number of other programmes to ensure better management of cargo security. They are not specifically directed at shipping but they are mentioned here as they may have impacts indirectly on vessels when cargo is laden on board. One initiative often discussed in the security literature is C-TPAT, the Customs-Trade Partnership Against Terrorism. Only American companies can belong (the sole exception being some Mexican *maquiladoras* and, recently, foreign manufacturers who are invited), but it has extraterritorial application by implicating the shipping on which cargoes bound for the United States are carried. C-TPAT membership is supposed to increase the probability of faster processing at borders for the cargo of members. This implies that non-members face greater likelihood that their marine containers will be stopped and inspected.[49] What C-TPAT has done, however, is encourage US multinational companies to ensure that the security efforts of their supply chain partners are better than those of non-partners.

[47] See US Customs and Border Protection, n. 45 above.

[48] US Department of Homeland Security, "DHS and DOE Launch Secure Freight Initiative," *Press Release* (7 December 2006), available: <http://www.dhs.gov/xnews/releases/pr_1165520867989.shtm> (retrieved 4 December 2008).

[49] According to US Customs and Border Protection (website at <http://www.cbp.gov> (retrieved 4 December 2008)), more than 8,200 businesses were members as of 27 March 2005. The website content indicating membership has not been updated.

Given its US-centric approach, several countries, including Canada, have adopted their own programmes that mirror the C-TPAT requirements.[50]

A second initiative aims to interdict shipments of weapons of mass destruction (WMD). Known as the Proliferation Security Initiative, it operates cooperatively through inter-state partnership arrangements to establish best practices and to coordinate readiness and action in response to an apprehended security incident. A Statement of Interdiction Principles was adopted in Paris on 4 September 2003, one of which urges participating states "to seriously consider providing consent ... to the boarding and searching of its own flag vessels by other states" when they are reasonably suspected of moving WMD cargoes.[51]

11.3. Maritime Security in the EU and Canada

11.3.1. EU Practices and Policies

11.3.1.1. Introduction

The EU has a great interest in maritime affairs. According to the EU Commission, there is a clear case for an integrated European maritime policy.[52] Twenty out of 25 constituent states are coastal states, and the total coastline of the EU is over 65,000 km in length. Of note, the offshore marine area of the EU—encompassing territorial seas, exclusive economic zones, and continental shelves of its Member States—is larger than the land territory of the EU. European maritime areas account for over 40 percent of the gross national product of the EU.[53] Oceans, therefore, play a vital role in the EU's economic and social life, and this maritime dimension has increased especially after the 2004 enlargement. On the one hand, this maritime orientation creates

[50] The Canadian programme, Partners in Protection, was developed at about the same time as C-TPAT.

[51] See US Department of State, *International Information Programs*, available: <http://usinfo.state.gov/products/pubs/proliferation> (retrieved 4 December 2008).

[52] See Commission of the European Communities, *Towards a Future Maritime Policy for the Union: A European Vision for the Oceans and Seas,* Green Paper, COM (2006) 275 final, available: <http://ec.europa.eu/maritimeaffairs/pdf/com_2006_0275_en_part2.pdf> (retrieved 4 December 2008), Volume II-Annex.

[53] L. Juda, "The European Union and Ocean Use Management: the Marine Strategy and the Maritime Policy," *Ocean Development & International Law* 38 (2007): 259–282, p. 260.

opportunities but, on the other hand, incurs significant challenges. It is argued that the scale of these challenges, and the types of action needed to address them, is better tackled at the supranational level than by individual member states. However, the EU has certain constitutional limitations. Individual Member States exercise sovereign rights. Article 5 of the Treaty Establishing the European Community requires the Community to act within the limits of the powers conferred upon it by the treaty and the objectives assigned to it in the treaty. In areas that do not fall within its exclusive jurisdiction, the Community may take action only if and in so far as the objectives of the proposed action cannot be sufficiently achieved by the Member States. Any action by the Community also shall not go beyond what is necessary to achieve the objectives of the treaty.[54] This means that the Community action must conform to the principles of both subsidiarity and proportionality. An integrated European maritime policy therefore has to align with these principles.[55]

The Commission needed to develop the overall framework for a marine strategy for the European Union in collaboration with the existing regional conventions. In order to draw up the strategy, the Commission established a consultation process open to participation from all relevant stakeholders (e.g., Member States and candidate countries, key non-EU neighbouring countries, international commissions and conventions, industry and non-governmental organisations). On 24 October 2005, after two years of intensive stakeholder consultations, the Commission presented the European Marine Strategy (EMS).[56] The Strategy suggests the need for a comprehensive and integrated Community policy on oceans and seas by putting an end to sector-by-sector approaches to maritime affairs. The Strategy resulted in the adoption of a proposed Maritime Strategy Directive (MSD). While most of the Member States recognised the need for a co-ordinated marine strategy, some of them were not ready to accept additional binding commitments.[57] The need for "an all embracing Maritime Policy," however, has become one of the strategic objectives of the Commission for 2005–2009.[58] The proposed MSD defines common objectives and principles, but leaves Member States free to plan and implement measures at national and regional levels taking into account the

[54] See Article 5 of the *Treaty on the European Union*, Maastricht, 7 February 1992, available: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2008:115:0001:01:EN:HTML> (retrieved 4 December 2008).
[55] See V. Frank, *European Community Marine Environmental Protection in the International Law of the Sea Implementing Global Obligations at the Regional Level* (The Hague: Martinus Nijhoff, 2007), pp. 102–103.
[56] Id., p. 96.
[57] Id., p. 98.
[58] Id., p. 101.

diverse regional conditions. The proposed MSD highlights the development of strategies for the integrated management of all human activities in marine regions. Member States are encouraged, amongst themselves and with third countries sharing the same marine region, when appropriate, to act within the framework of existing regional seas conventions.[59] Finally, on 14 May 2008, the European Community adopted the Marine Strategy Framework Directive.[60]

In March 2005, the European Commission began work towards the adoption of a Green Paper on Maritime Policy. The proposals were outlined in the communication "Towards a Future Maritime Policy for the Union: A European Vision for the Oceans and Seas."[61] This was actually the first step towards a coherent and integrated oceans policy in Europe along the lines of other countries, such as Australia, Canada, Portugal, and the United States. The EU, thus, has attempted to develop a comprehensive integrated, coherent and holistic ocean management system. On 7 June 2006, the EU Commission adopted its Green Paper on Maritime Policy with the intention of generating wide-scale discussion on the need for and formation of a EU approach to maritime policy.[62] Subsequently, on 10 October 2007, the Commission adopted "An Integrated Maritime Policy for the European Union,"[63] the so-called Blue Book, with an accompanying document containing an action plan for the integrated maritime policy.[64]

---

[59] Id., p. 99.

[60] Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 establishing a framework for community action in the field of marine environmental policy (Marine Strategy Framework Directive) *Official Journal* L 164/19 (25 June 2008), available: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:164:0019:0040:EN:PDF> (retrieved 4 December 2008). Member States must transpose MSFD into national law by 15 July 2010 at the latest. The main aim of MSFD is to ensure the "good environmental status" of Europe's seas by 2020. The Directive is also seen as an environmental pillar of the European Union.

[61] See Commission of the European Communities, n. 52 above.

[62] Id.

[63] Commission of the European Communities, *An Integrated Maritime Policy for the European Union,* Communication from the Commission to the European Parliament, the Council, The EESC and the COR, COM(2007) 575 final (Brussels, 10 October 2007), available: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0575:FIN:EN:PDF> (retrieved 4 December 2008).

[64] Commission of the European Communities, Commission Staff Working Document, SEC(2007) 1278 (Brussels, 10 October 2007), available: <http://ec.europa.eu/maritimeaffairs/pdf/ActionPaper/action_plan_en.pdf> (retrieved 4 December 2008).

11.3.1.2. EU Legislation on Maritime Security

Maritime security related legislation at the Community level began after the amendments to the SOLAS Convention were adopted in 2002. Since the objectives of the IMO amendments, which introduced the ISPS Code, cannot be realised by the Member States individually, the EU adopted Regulation No. 725/2004 to incorporate the provisions of the SOLAS amendments and the ISPS Code. The Regulation defines maritime security as "the combination of preventive measures intended to protect shipping and port facilities against threats of international unlawful acts."[65]

There are two objectives in Regulation No. 725/2004. First, it is aimed at introducing and implementing Community measures to enhance the security of ships used in international trade and of associated port facilities in the face of threats of intentional unlawful acts. Second, the Regulation provides a basis for the harmonised interpretation, implementation and Community monitoring of the special measures to enhance maritime security in accordance with the SOLAS amendments and the ISPS Code.[66] However, unlike IMO rules, the Regulation also applies to some domestic shipping, i.e., between ports within the same Member State.[67] According to Article 3 of the Regulation, Member States had to apply Part A of the ISPS Code in full for international shipping by 1 July 2004 and to Class A domestic passenger shipping by 1 July 2005.[68] The Member States, based on a mandatory security risk assessment, were required to decide by 1 July 2007 how to apply the provisions of the regulations to other categories of ships operating domestic services. While the ISPS Code applies to ships, companies and port facilities, according to Article 7, Regulation 725/2004 does not apply to ships of war and troop ships, cargo ships of less than 500 gross registered tonnes, ships not propelled by mechanical means, wooden ships of primitive build, fishing vessels, or vessels not engaged in commercial activities. Moreover, in the implementation of the ISPS Code, the EU has taken a more stringent position than IMO requires. For example, in Article 3(5), the EU made much of Part B of the ISPS Code mandatory; as the IMO does not make these provisions mandatory, some argue that

[65] See EU Regulation No. 725/2004 of the European Parliament and of the Council of 31 March 2004 on Enhancing Ship and Port Facility Security, *Official Journal* L 129/6 (29 April 2004).
[66] Id., Article 1.
[67] Background Paper (to Green Paper) No. 6 on Maritime Safety and Security, available: <http://ec.europa.eu/maritimeaffairs/pdf/SEC(2006)_689%20_6.pdf> (retrieved 4 December 2008), p. 23.
[68] By Article 4 of Council Directive 98/18/EC of 17 March 1998, a Class A passenger ship is a vessel that carries more than 12 passengers.

implementation of the ISPS Code in European ports is impressive and that all players concerned are doing their best to make it a success.[69]

Regulation 725/2004 is complemented by Directive 2005/65/EC,[70] which goes beyond port facility boundaries in laying down security measures that shall be observed in ports. Member States must ensure that the port security measures introduced by the Directive are closely coordinated with measures taken pursuant to Regulation 725/2004.[71] In addition, Member States shall ensure that when port security assessments are carried out, they take into account, as a minimum, the detailed requirements listed in Annex I of the Directive.[72] Member States are required to introduce a system of security levels for ports or parts of ports as defined in Regulation 725/2004.[73] Enhancement of port security measures and clearance are delineated in Directive 2005/65/EC, which in Annexes I (port security assessment) and II (port security plan) provides detailed requirements about control mechanisms, clearance systems, luggage and cargo controls, background checks for personnel, and so on. Moreover, Regulation 725/2004 implements IMO's SOLAS regulation on Ship Security Alert System in EU law.

For the EU, violations are penalised by the respective Member States. Article 14 of Regulation 725/2004 states that Member States decide the penalties for violations of its provisions. Thus, according to EU laws, although enforcement of legislation lies with the Member States, the Commission retains the right and the duty to inspect whether proper implementation of Regulation 725/2004 within the Member States is observed.[74] Member States of the EU are expected to ensure cooperation with the Commission's inspectors. The "Member State shall ensure that, upon request, Commission inspectors have access to all relevant security related documentation," which includes the national programme for implementation of Regulation 725/2004 and its associated data and monitoring reports.[75] The European Maritime Safety

[69] See H. N. Psaraftis, "EU Port Policy: Where Do We Go from Here?" *Maritime Economics & Logistics* 7 (2005): 73–82, at p. 78. See also E. Anyanova, "The EC and Enhancing Ship and Port Facility Security," *Journal of International Commercial Law and Technology* 2, no. 1 (2007): 25–31, p. 30.

[70] Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security, *Official Journal* L 310/28 (25 November 2005), available: <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2005/l_310/l_31020051125en00280039.pdf> (retrieved 4 December 2008).

[71] Id, Article 4.

[72] Id., Article 6.

[73] Id., Article 8. These levels are consistent with the ISPS Code described above.

[74] See EC Regulation No 884/2005 of 10 June 2005, *Official Journal* L148/25, "laying down procedures for conducting Commission inspections in the field of maritime security."

[75] Id., Article 4.

Agency, created by EC Regulation 1406/2002, provides technical assistance, making technical experts available to participate in the Commission's inspection programme.[76]

Another step the EU has taken is the adoption of "security amendments" to the Community Customs Code[77] to protect the customs territory of the Community and to provide the EU with a common risk management system. The goal is a harmonised application of customs controls in order to minimise the risks to the Community and its citizens and to the Community's trading partners[78] via commonly agreed standards and risk criteria for the selection of goods and economic operators by the Member States.[79] The regulations cover entry, exit, transit, transfer and end-use of goods moved between the customs territory of the Community and third countries, as well as the presence of goods that do not have Community status. By international agreement, custom controls for the correct application of the Community legislation may be carried out in a third country as well.[80]

11.3.1.3. EU Policy Development

The EU Commission has highlighted a clear need for future policy development in the field of maritime security. In 2006, the Commission planned to launch a wider debate on the concept of a "common European maritime area," one where both the ship and the goods could be reliably tracked throughout its journey, thereby reducing the need for individual state controls in purely intra-Community trade.[81] As stated previously, in 2007, the EC published a Communication on an Integrated Maritime Policy for the European Union.[82] The Communication, *inter alia*, placed importance on a maritime surveillance

[76] Id., Article 6.
[77] Regulation (EC) 648/2005 of 13 April 2005 amending Council Regulation (EEC) No 2913/92 establishing the Community Customs Code, *Official Journal* L 117/13 (4 May 2005).
[78] Id., Preamble, para. 2.
[79] In this context, it should be noted that the EU cooperates with the United States in the framework of the Container Security Initiative (through Agreement of 28 April 2004 between the European Community and the United States of America on intensifying and broadening the Agreement on customs cooperation and mutual assistance in customs matters to include cooperation on container security and related matters (L 304/30/09/2004)), which was launched after the 11 September 2001 terrorist attacks. See Background Paper, n. 67 above, p[. 23–24.
[80] See Regulation (EC) 648/2005, n. 77 above, Article 13.
[81] See *Maritime Transport Policy Improving the Competitiveness, Safety and Security of European Shipping* (DG Transport, 2006), available: <http://ec.europa.eu/transport/maritime/doc/maritime_transport_policy_en.pdf> (retrieved 4 December 2008).
[82] Commission of the European Communities, n. 63 above.

system, on maritime data and information infrastructure, and on the visibility of maritime Europe. All these efforts are intended to ensure overall security in European waters. An integrated approach, the Commission stated, is required "to meet the challenge of transnational security threats," for which a higher degree of coordination is a necessary pre-requisite.[83]

An example of such integration is the development of a network of vessel tracking and e-navigation systems for European coastal waters and the high seas, including satellite monitoring and long range identification and tracking (LRIT). The Marine Strategy Framework Directive, discussed previously, defined European marine regions and sub-regions.[84] It is argued that LRIT systems across the European marine regions using satellite communications will have highly beneficial effects on shipping in the European Community. This is particularly important for "motorways of the sea" traffic where a ship sails between two Member States.[85] To this end, the Commission has undertaken responsibility to promote cooperation between the coast guards and similar agencies of Member States, and to take steps towards greater interoperability of surveillance systems and the establishment of a European Marine Observation and Data Network[86] to enhance maritime safety and security.

In addition, the EU Green Paper on maritime policy strongly urges Member States to ratify, as soon as possible, existing international maritime conventions, including the 2005 Protocol to the SUA Convention, so as to provide a legal framework for the US-led Proliferation Security Initiative. As some Member States have concluded bilateral boarding agreements with the United States, coordinated action at the EU level towards such initiatives is highly desirable.[87]

---

[83] Id. For example, normally, surveillance activities in Europe are carried out by the Member States even though most of the activities and threats are of a transnational nature. Within the Member States, the surveillance activities again fall under the responsibility of several different enforcement agencies operating independently. Therefore, the Commission advocates the need for a higher degree of coordination on maritime surveillance.

[84] See Directive 2008/56/EC, n. 60 above, Article 4 which sets out four regions: Baltic, North East Atlantic, Mediterranean and Black seas.

[85] See Maritime Transport Policy, n. 81 above.

[86] See Commission of the European Communities, n. 63 above.

[87] See Background Paper no. 6, n. 67 above, p. 30.

11.3.1.4. EU Cooperation with the United States

The EU has further designed its maritime security policy to enhance cooperation with third countries, especially with the United States, in the fight against terrorism. The US initiatives relating to maritime security measures were discussed above. The measures require bilateral and multilateral cooperation. For example, the US Coast Guard's International Port Security Program has worked closely with the European Union to establish a strong relationship to further improve practices in ports located both in the EU and in the United States.[88] There has been in place between the United States and the EU, since 1997, an Agreement on Customs Cooperation and Mutual Assistance in Custom Matters (CMAA). On 22 April 2004, the two parties signed a further Agreement that extended the scope of their 1997 Agreement by expanding customs cooperation to ensure that general customs control takes due account of security concerns.[89] The EU Council, by Decision 2004/634/EC, encouraged Member States to expand the CSI to all the Community ports through arrangements with the United States. As is the case elsewhere in the world, Community ports participating in the CSI station US customs officials at the port. These measures are, however, subject to conformity with the EU Treaty and compatibility with the CMAA as expanded by the 2004 Agreement.[90] By 2007, the CSI had been implemented in 23 EU ports, and no further ports have been added since, signalling that further interest on the part of the US government in expanding the initiative is unlikely.[91]

---

[88] See "For the Navies of the Mediterranean and Black Sea Countries," 6th Regional Sea Power Symposium, Venice, 10–13 October 2006, available: <http://www.marina.difesa.it/rss/2006/petermaning.asp> (retrieved 4 December 2008).

[89] *Agreement between the European Community and the United States of America on intensifying and broadening the Agreement on customs cooperation and mutual assistance in customs matters to include cooperation on container security and related matters*, *Official Journal* L 304/34 (30 September 2004), available: <http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_304/l_30420040930en00340037.pdf> (retrieved 4 December 2008).

[90] See the EU Council Decision of 30 March 2004 concerning the conclusion of the Agreement between the European Community and the United States of America on intensifying and broadening the Agreement on customs cooperation and mutual assistance in customs matters to include cooperation on container security and related matters, *Official Journal* L 304/32 (30 September 2004) available: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:304:0032:0033:EN:PDF> (retrieved 4 December 2008).

[91] The 23 are: Rotterdam, The Netherlands; Bremerhaven and Hamburg, Germany; Antwerp and Zeebrugge, Belgium; Le Havre and Marseille, France; Gothenburg, Sweden; La Spezia, Genoa, Naples, Gioia Tauro, and Livorno, Italy; Felixstowe, Liverpool, Thamesport, Tilbury, and Southampton, United Kingdom; Piraeus, Greece; Algeciras, Barcelona, and Valencia, Spain; and Lisbon, Portugal. (US Customs and Border Protection, Container Security Initiative

While the EU remains committed to working closely with the United States in order to counter terrorism, concern remains that some of the import measures applied on security grounds may be used as a disguised form of protectionism or as a non-tariff barrier.[92] The European Commission, Member States, and trading partners of the European Union are especially concerned about the US legislation. The CSI programme's stated intention of scanning 100 percent of inbound containers could incur trade-dampening costs. A detailed quantitative analysis of the benefits and drawbacks of 100 percent container scanning confirms that the impacts on costs, delays and security will be severe.[93] Furthermore, 100 percent scanning runs counter to a risk-based management perspective:

> … some European customs officials have told us that the 100 percent scanning requirement is in contrast to the risk-based strategy behind CSI and C-TPAT, and the WCO has stated that implementation of 100 percent scanning would be 'tantamount to abandonment of risk management'.[94]

In addition to the potential for major trade disruptions, the additional administrative burden for EU businesses and taxpayers, and the SAFE Port Act standards for container security and/or smart box technology are expected to negatively impact the competitiveness of EU suppliers.[95] In addition, the presence of naturally occurring radioactive materials is expected to be disruptive.[96] According to the EC Ambassador at the World Trade

---

Ports (n.d.), available: <http://www.dhs.gov/xprevprot/programs/gc_1165872287564.shtm> (retrieved 4 December 2008)).

[92] See E. Guth, "Trade Policy Review of United States," Statement by EC Ambassador at the WTO (Geneva, 9 & 11 June 2008), available: <http://ec.europa.eu/commission_barroso/mandelson/speeches_articles/spaw002_en.htm> (retrieved 4 December 2008).

[93] A. C. Bennett and Y. Z. Chin, "100% Container Scanning: Security Policy Implications for Global Supply Chains" (Masters of Engineering in Logistics, Cambridge MA: MIT, 2008).

[94] Government Accountability Office, *Supply Chain Security: Challenges to Scanning 100 Percent of U.S.-Bound Cargo Containers* (GAO-08-533T) (Washington, DC: Government Accountability Office, 2008), p. 18.

[95] "EU Issues, Annual Report on U.S. Barriers to Trade and Investment," *Online Bulletin Custom and International Trade News* (April 2008), available: <http://hocnews.blogspot.com/2008/04/eu-issues-annual-report-on-us-barriers.html> (retrieved 4 December 2008).

[96] See, for example, the findings at Southampton (UK) as part of the Secure Freight Initiative rollout, see SITPRO, *Evaluation of 100% Scanning and the Port of Southampton Trial* (n.d.), available: <http://www.sitpro.org.uk/policy/security/position-100percent-0408.htm> (retrieved 4 December 2008). This problem has also been documented in a number of other locations since the introduction of VACIS equipment based on gamma-ray technology, as is implemented in Canada at ports and some border crossings.

Organization, Eckart Guth, these measures will not necessarily increase security, but will increase transaction costs for exporters and customs services worldwide. They will affect the smooth circulation of trade.[97]

11.3.2. Canadian Practices and Policies

11.3.2.1. Canadian Legislation on Maritime Security

As one of the G8 countries, Canada is a major trading nation. Much of its trade is carried by sea; indeed, of Canada's non-US trade in 2007, 64.4 percent was carried by the marine mode.[98] Although Canada only has a small number of ocean-going merchant vessels on its national shipping registry, its flag is flown by a significant number of bulk carriers operating in the St. Lawrence Seaway/Great Lakes system. These maritime interests add to Canada's concern for safe and secure shipping. It is no surprise, therefore, that Canada has long pursued a policy of engagement in the work of the IMO and its programmes for safer ships and cleaner seas, including participation in the IMO's work on maritime security.

Canadian marine policy is also strongly influenced by US intentions and practices. This influence results directly from Canada's close associations with its powerful neighbour to the south. Canada has multiple social and political relationships with the United States, which include a range of both competitive interests and co-operative regulatory arrangements in their coastal waters and over the resources of their marginal seas. Most significant, Canada has two trade agreements of relevance—the Canada-US Trade Agreement, signed in 1988, and the North American Free Trade Agreement, concluded five years later. Neither of these agreements includes maritime shipping within their remit, but both led to considerable increases in trading activity so that by 2005, in excess of 85 percent of Canada's international trade was with the United States. Added to the exchange of trade is very substantial foreign direct investment; in fact, in a number of sectors Canada and the United States make things together. As a result, after the attacks of 11 September 2001 in the United States, Canada reflected on its own security risks as well as negotiating with the United States about their joint continental concerns. The combination of these human, diplomatic and economic interests induced Canada to take

[97] See Guth, n. 92 above.

[98] Transport Canada, *Transportation in Canada 2007 Annual Report* (Ottawa: Transport Canada, 2008), Table EC7.

vigorous action against the threat of maritime insecurity, which included rapid implementation of the international ISPS Code and additional maritime regulations that closely match the national initiatives of the United States.

The provisions of the ISPS Code are applied in Canada by government regulations[99] made pursuant to the *Marine Transportation Security Act*.[100] Their application is fulsome; indeed the Canadian regulations exceed the implementation requirements of the Code in several respects. In particular, Canada enforces the ISPS Code more widely than required by imposing it not just against ships of the size or type designated by SOLAS, but also against "non-SOLAS" vessels. These are described as ships under the SOLAS minimum limit of 500 tons gross down to 100 tons gross, any vessel that carries more than 12 passengers regardless of tonnage, and all working barges that are carrying "certain dangerous cargoes"[101] whenever they are engaged in international voyages.[102] Thus Canada applies the ISPS Code's standards to practically all foreign-going merchant ships, cruise ships, and ferries. Canada has also incorporated many elements of Part B of the ISPS Code, which are not mandatory, especially regarding restricted access to and around shipping, by imposing additional requirements on ferries, passenger vessels, cruise ships, certain dangerous cargoes facilities and barge fleeting stations, including provisions about personnel passes and keys.[103]

Beyond ships, Canada also applies the ISPS Code to all marine facilities that interface with international shipping. These are defined in Canadian law as including "an area of land, water, ice or other supporting surface [together with any buildings, installations and equipment there] used, designed, prepared, equipped or set apart for use … for the arrival, departure, movement or servicing of vessels."[104] Canadian regulations apply the ISPS Code to all such marine facilities other than offshore drilling units and platforms.[105] All ports and harbours are clearly included in separate specific provisions.[106] The ISPS Code uses the phrase "port facility" which is defined by IMO resolution, rather than the Code itself, as "a location, as determined by the Contracting Government … where the ship/port interface takes place."[107] So it seems that

[99] *Maritime Transportation Security Regulations*, SOR/2004-144 as amended.
[100] *Marine Transportation Security Act*, S.C. 1994, c. 40 as amended.
[101] *Maritime Transportation Security Regulations*, n. 99 above, s. 1.
[102] Id., s. 200(1).
[103] Id., ss. 260–265, 347–350, 384.
[104] *Marine Transportation Security Act*, n. 100 above, s. 2(1).
[105] *Maritime Transportation Security Regulations*, n. 99 above, s. 301.
[106] Id., ss. 361–375.
[107] See IMO, n. 4 above, Resolution 1, Annex art. 7, Regulation 1, s. 1.9.

Canada has chosen to give the ISPS Code its widest possible application to coastal facilities for ships.

In addition to the requirements of the ISPS Code, Canada has taken further regulatory steps in three other supportive directions, and has implemented administrative, in addition to criminal, penalties for violations. First, it has mandated the installation and use of security alert systems on vessels pursuant to IMO resolutions.[108] Secondly, it has established requirements for the background security clearance of a comprehensive range of personnel connected in any way to shipping activities, whether cargo vessels or cruise ships, in the restricted areas of 13 principal ports and the marine traffic centres of the St. Lawrence Seaway.[109] These requirements extend beyond on-site port and waterfront workers who service ships, handle cargoes or direct passengers to any person who could cause a failure in the security system by reason of advance access to ships' cargo or passenger documentation even, it seems, from a distant location.[110] Security clearance is also voluntarily available to Canadian seafarers as a prerequisite to those who want a Canadian identity document. This document is not the same as the one prescribed under the ILO's revised Seafarers' Identity Documents Convention described above and it does not contain biometric data of the holder. However, Canada is taking steps towards applying the ILO convention; tendering of a contract to fulfil ILO criteria is anticipated with a view to operating a compliant system in 2009.[111]

Third, Canada has replicated US demands for 96 hours notice in advance of entering national waters. Canadian pre-arrival notices must provide an extensive list of information about the ship and its cargo, including its International Ship Security Certificate, a statement of when its last ten declarations of security were completed, and details of any security threats suffered at, as well as information about, its last ten ports of call.[112] In addition, regulations made under the Canadian *Customs Act*[113] reiterate the requirement of a 96-hour pre-arrival notice for liner shipping[114] with the added demand that specified details about commercial goods stuffed in containers must be supplied

---

[108] *Regulations Amending the Marine Transportation Security Regulations*, SOR/2006-269, s. 5(F) pursuant to IMO Amendments to the Annex to the International Convention for the Safety of Life at Sea, 1974 [SOLAS] made by the Conference of Contracting Governments in Resolution 1, Annex art.7, Regulation 6 adopted 12 December 2002.

[109] *Maritime Transportation Security Regulations*, n. 99 above, Part 5 & Sched. 1.

[110] Id., s. 503.

[111] N. Nazha, Director of Seafarers' Identity, Transport Canada, pers. comm. (24 October 2008).

[112] *Maritime Transportation Security Regulations*, n. 99 above, s. 221.

[113] *Customs Act*, R.S.C. 1985, c. 1 (2nd Supp.).

[114] *Reporting of Imported Goods Regulations*, SOR/86-873, ss. 13.2, 13.3 & Sched. 1, Part 1.

to the Canada Border Services Agency (CBSA) at least 24 hours before loading at the foreign port of origin.[115] This data is received and reviewed in Ottawa, where a risk assessment is made and a decision is reached about stopping, inspecting or interdicting the cargo upon arrival in Canada.

Finally, as a means of enforcing all the regulatory prescriptions that give effect to the ISPS Code in Canada, the usual penal processes for violation have been enhanced by a system of simplified administrative penalties.[116] These penalties are of two forms. Under one, the offender may be served with a notice of violation and a demand for payment of a prescribed penalty, which must be paid within 30 days unless the offender requests a review by the Transportation Appeal Tribunal of Canada (TATC).[117] Alternatively, the violator may be required to enter an assurance of voluntary compliance in future and to deposit a sum of money as security for performance; a right of review by the TATC is available, but failure to comply will incur double the penalty prescribed for the original violation and forfeiture of the security deposit.[118]

While the ISPS Code seeks to prevent maritime terrorism and minimise its effects, the SUA Convention and Protocols assert the prohibition of terrorist tactics. As a party to this convention, Canada has implemented its provisions in a couple of ways, twice over in fact. First, the proscriptions of the 1988 Convention and Protocol have been engraved directly in Canada's *Criminal Code*.[119] Canada has not enacted the 2005 amendments to SUA but perhaps that is not so surprising since they are not yet in force internationally. Second, Canada has included the 1988 SUA offences in its own domestic anti-terrorism laws. In further additions to the *Criminal Code*, Canada has proscribed "terrorist activity" which is defined, in part, by reference to the offences under the SUA Convention and Protocol.[120] Moreover, the Criminal Code goes on to prohibit a wider range of criminal actions that support terrorism. These include providing, collecting, making available or using property for terrorist activity,[121] all of which are capable of encompassing terrorist attacks against ships, engaging ships to deliver terrorist bombs or other materiel, and using ships as terrorist weapons.

---

[115] Id, ss. 2.1, 13.5, 13.6 & Sched. 2, Part 1.
[116] *Marine Transportation Security Act*, n. 100 above, ss. 2(1), 33–46, 49 & 50 and SOR/2004-144, Part 6.
[117] Id., Act s. 33(1)(b) and SOR/2004-144, Part 6.
[118] Id., Act ss. 33(1)(a) & 35 and SOR/2004-144, Part 6.
[119] *Criminal Code*, R.S.C. 1985, c. C-46, s. 78.1
[120] Id., s. 83.01.
[121] Id., ss. 83.02, 83.03, 83.04.

11.3.2.2. Canadian Policy Developments

Transport Canada has declared that its marine security vision is "a nationally and internationally recognised marine transportation system that is secure, efficient and respects Canadian values."[122] Within that vision, the government department has a continuing mission that will "with partners, increase the level of Canada's Marine Transportation Security System against: 1. unlawful interference, 2. terrorism attack, and 3. terrorist exploitation of it as a conduit to attack our allies."[123] The Interdepartmental Marine Security Working Group (IMSWG), formed by the Canadian government following the attacks of 11 September 2001, leads fulfilment of this mission. Chaired by Transport Canada, the IMSWG coordinates the marine security efforts of nine other departments: Canada Border Services Agency, Canadian Security and Intelligence Service, Department of Citizenship and Immigration, Department of Fisheries and Oceans, Department of Foreign Affairs and International Trade, Department of Justice, Department of National Defence, Royal Canadian Mounted Police, and Solicitor General of Canada.[124] Together, these departments have undertaken a variety of security enhancing initiatives (in addition to the administrative programmes to operate and enforce the regulatory schemes already discussed) of which the following are of particular note.

Scanning of cargo containers and their contents on arrival in Canada has been identified as an important security precaution. Two types of scanning equipment are operated. The Canada Border Services Agency employs a number of Vehicle and Cargo Inspection Systems or VACIS units for the purpose of scanning the contents of containers. These units are truck mounted, mobile, gamma ray scanning equipment that can generate an image of even densely loaded containers.[125] Whether a container is taken temporarily out of the supply chain for VACIS scanning depends on the risk it is assessed to present. This risk assessment is made by CBSA for every arriving container by screening the information supplied by carriers 24 hours before the container is loaded in the port of origin, as described previously.

A second scanning effort detects radioactive materials. By arrangement with the terminals, every container, as soon as it is offloaded from the ship by crane and placed on a terminal transporter, is driven through a radiation

[122] Transport Canada, "Mission" (n.d.), available: <http://www.tc.gc.ca/MarineSecurity/Strategic/mission.htm> (retrieved 4 December 2008).
[123] Id.
[124] Transport Canada, "Government of Canada Announces up to $172.5 million in New Marine Security Projects," *News Release* (22 January 2003), available: <http://www.tc.gc.ca/mediaroom/releases/nat/2003/03-gc001.htm> (retrieved 4 December 2008).
[125] Id.

detection portal before being stacked in the yard or loaded for onward surface transport.[126] Any container that is shown to hold radioactive material is then isolated for further testing and investigation.[127]

Domain awareness is another important aspect of Canada's marine security system. Canada operates an air surveillance programme that conducts patrols both within and without Canada's 200 nautical mile coastal zone for security purposes, fisheries enforcement, pollution detection, and sea ice coverage. The Department of National Defence is promoting an advanced radar system that can follow the curvature of the earth over the oceans. The Canadian Coast Guard is responsible for the shore-based components required to operate the automatic identification system (AIS) now required of ships by IMO.[128] Canada also fully supports the work of IMO to establish a global Long Range Identification and Tracking (LRIT) system for ships, which is now at the testing stage. The necessary regulations to implement Canada's participation in the system are being drafted under the *Canada Shipping Act, 2001* and should be in place during 2009. Canada is also committed to provide a national data centre for LRIT data exchange.[129]

Cruise shipping in Canadian waters has grown greatly in recent years. Whether visiting port cities, cruising inland waters, or exploring the Canadian Arctic, these vessels pose a specific set of security risks beyond merchant shipping on account of the numbers of passengers on board. The requirements of the ISPS Code are enforced and security clearance is required of all personnel who service a cruise ship at sea or in port. In addition, everyone who goes on board or enters the restricted area around the dock is subjected to screening and search. Even so, Transport Canada is working towards a specific set of measures specially designed for cruise ships.[130]

Separate consideration has been given to passenger vessels classed as "tall ships." These visiting (training and cruising) sailing ships are subject to special security arrangements in accordance with ISPS Code standards, which

[126] L. Kinney, Director General of Marine Security, Transport Canada, pers. comms. (17 October & 16 November 2008).
[127] See Transport Canada, n. 122 above.
[128] Id.
[129] Canadian Marine Advisory Council, Marine Security Standing Committee, *Minutes of meeting* (29 April 2008), available: <http://www.tc.gc.ca/marinesafety/rsqa/cmac/pdf/2008-apr-committee-marine-security-min.pdf> (retrieved 4 December 2008).
[130] See Transport Canada, n. 124 above.

will be reviewed in the context of an overall review of Canada's marine security regulations of 2004.[131]

Finally, domestic coastal shipping is also the subject of security consideration. A risk assessment of different types of domestic shipping, including ferries, small commercial vessels, fishing boats and pleasure craft, as well as the port facilities they use, is being undertaken with a view to developing an appropriate security strategy. The higher risk classes of vessels, such as the large and busy vehicle and passenger ferries operating in British Columbia, will be subject to security requirements akin to the ISPS Code in order of priority. In 2008, active consultation with industry was being undertaken. Eventually the strategy will cover all domestic shipping by regulatory provisions that demand security measures commensurate by type of vessel and marine activity with the risk presented.[132]

11.3.2.3. Canadian Co-operation with the United States

As an immediate neighbour of the United States by land and sea, Canada has been co-operatively involved in North American security in all modes of transport. Perhaps more indicative than anything else, the response of Canada to the events of 11 September 2001 was immediate and supportive of its neighbour's concerns about security. In addition to Canadian authorities providing a safe haven for those air passengers en route to the United States that day and unable to enter the United States during the air space lock down, Canada moved quickly to open a dialogue with US authorities on how matching regulations might be adopted so as to expedite security procedures while maintaining trade relationships. On 12 December 2001, Tom Ridge (responsible for US security) and John Manley (Canada's Minister of Foreign Affairs) agreed on a common security approach, and signed a 30-Point Smart Border Declaration and Action Plan. The Smart Border list of projects included many that could be incorporated into a North American "perimeter clearance" process, including the agreement to station customs inspectors at each other's seaports for targeted maritime container inspections. Subsequent execution of this initiative, however, now means that US Customs may inspect marine containers at Canadian seaports, and then again at land border crossings, in

[131] See Kinney, n. 126 above. See also Transport Canada, *Transportation in Canada 2005* (2005), available: <http://www.tc.gc.ca/pol/en/Report/anre2005/4B_e.htm> (retrieved 4 December 2008).
[132] See Kinney, n. 126 above. See also Canadian Marine Advisory Council, n. 129 above.

addition to the inspection that might have been undertaken in advance of loading in the foreign port through the CSI.

A 2004 compendium of Canada-US government collaboration identified two bilateral institutional arrangements relevant to marine security issues—the Canada-US Transportation Security Co-operation Group (with the Transportation Security Administration), and the Bi-National Marine Security Compliance and Enforcement Working Group.[133] These administrative arrangements facilitate the operation of their respective national security officers and laws across their shared borders. In addition the Security and Prosperity Partnership signed between Canada, the United States, and Mexico at Waco, Texas, in 2005 set two relevant targets for North American security: (1) "Make compatible US-Canada requirements for participation in Customs-Trade Partnership Against Terrorism (C-TPAT) and Partnership in Protection (PIP) within 36 months" (June 2008), and (2) "Develop appropriate linkages, including officer exchanges among Canadian, Mexican and US customs agencies, to ensure analysis of cargo data and appropriate sharing of information on high-risk shipments."[134] There is no evidence that the first target has been reached, and while the second was reported in 2006 as initiated,[135] it can be considered in development. A detailed report on the progress achieved at the 2008 Summit of the three partners was not published; all that was released was a brief joint ministerial declaration indicating continued emphasis on security issues. It is too soon to have a clear understanding of what might be achieved under the Obama Administration.[136]

An example of the Canada-United States bilateral relationship in operation is the application of their separate marine security regulations. Having determined they provide equivalent levels of security, the two states reached an arrangement for the reciprocal recognition and acceptance of each other's documentary approval of a vessel's security plan. This arrangement was first established in June 2004 and has since been amended to accommodate alternative security arrangements for passenger vessels and ferries that operate

---

[133] D. Mouafo, N. P. Morales, and J. Heynen, *Building Cross-Border Links: A Compendium of Canada US Government Collaboration* (Ottawa: Canada School of Public Service, 2004), pp 147–152, available: <http://dsp-psd.pwgsc.gc.ca/Collection/SC103-6-2004E.pdf> (retrieved 4 December 2008).

[134] Security and Prosperity Partnership of North America, *Report to Leaders* (June 2005), available: <http://www.spp.gov> (retrieved 4 December 2008).

[135] Security and Prosperity Partnership of North America, *Report to Leaders II*, August 2006, available: <http://www.spp.gov> (retrieved 4 December 2008).

[136] Security and Prosperity Partnership of North America, "Joint Statement by Ministers Responsible for the Security and Prosperity Partnership of North America," Press Release *Commerce News* (28 February 2008), available: <http://www.spp.gov/news/news_02282008.asp> (retrieved 4 December 2008).

on short fixed routes between the two countries on their Pacific and Atlantic coasts as well as across the rivers and lakes that separate them.[137] Subsequently a Canada-United States Maritime Security Working Group was created in February 2006 to enhance the facilitation of their respective marine security operations.[138] Topics of discussion between Canada and the United States have included joint vessel inspections of foreign flagged ships, reciprocal port visits to develop best practices, and seafarers' identity documents.[139]

11.4. EU and Canadian Approaches to Maritime Security Compared

The approaches to maritime security of the EU and Canada display points both of convergence and divergence. Convergence in this context signifies similar or parallel implementation of security measures. Exactly the same tools are not necessarily used on both sides of the Atlantic Ocean; indeed maritime security regimes are typically works in progress, but both the EU and Canada can be seen as converging in their actions when they take steps for the same purpose towards the same goal.

A striking feature of the international maritime security regime at large is that its compulsory components—chiefly Part A of the ISPS Code—address the risk of terrorist threats to ships and ports but do not focus on that which gives purpose to their existence, that is to say, their cargoes. Cargo security has not been ignored, however; cargo protection is only advanced internationally by hortatory guidelines for supply chain management, such as those produced by WCO, and by whatever extra-territorial reach may be achieved by national initiatives, such as the US Cargo Security Initiative, the US Customs-Trade Partnership Against Terrorism initiative, and the Canadian Partners in Protection programme. Whatever the merits of the difference in attention paid to the elaboration and enforcement of security regimes for ships, ports and cargoes, the international character of the measures concerning ships and ports almost inevitably ensures a degree of uniformity in application that the

[137] Bilateral Arrangement between Transport Canada and the United States Coast Guard, available: <http://www.tc.gc.ca/Marine Security/Relationships/USA/menu.htm> (retrieved 4 December 2008).

[138] Canadian Marine Advisory Council, *Minutes of meeting* (3 May 2006), available: <http://www.tc.gc.ca/marinesafety/rsqa/cmac/minutes/2006-may-committee-marine-safety-report.htm> (retrieved 4 December 2008).

[139] Canadian Marine Advisory Council, *Minutes of meeting* (7 November 2007), available: <http://www.tc.gc.ca/marinesafety/rsqa/cmac/pdf/2007-nov-committee-marine-security.pdf> (retrieved 4 December 2008).

essentially national development and proliferation of cargo initiatives cannot be expected to achieve. In light of these observations, the EU and Canada might be expected to converge in their actions to advance ship and port security but potentially to diverge in their approaches to trade and cargo security issues, especially as presented to them by US initiatives. The evidence drawn from the discussion above in this chapter confirms these expectations.

Given the multilateral uniformity of maritime security imposed by the ISPS Code of the IMO and related programmes of other intergovernmental organisations—the multilateral platform as it has been described here, it is not surprising to find a high degree of convergence in EU and Canadian marine security regulations. Only small differences appear in their practices around the edges of the multilateral platform.

In addition, both the EU and Canada have been faced with the need to respond to US security concerns. Their large and well-developed trading relations with the United States have encouraged broad cooperative arrangements bilaterally for the implementation of the ISPS Code. However, beyond the multilateral platform, and in response to the unilateral security initiatives of the United States concerning the cargo traffic carried by ships, the actions of the EU and Canada are more divergent. The different geographical, political and economic contexts of their relations with the United States presage a different outlook on the priorities for enhancing the cargo-related aspects of maritime security.

These general observations about EU and Canadian approaches are substantiated by the following dialogue about the specific measures that each has, or has not, undertaken or proposed. Convergence around the ISPS Code is nearly complete. In respect of ships, Part A of the Code is mandated and Part B is also applied or followed closely. In addition, although the ISPS Code does not apply to domestic shipping, the EU has already imposed it on vessels that carry more than 12 passengers and Canada is working on a comparable security strategy for its domestic ferries. In one respect Canada has gone further than the EU, and, indeed further than the ISPS Code demands, by applying the Code to ‘non-SOLAS’ ships, i.e. to classes of foreign-going vessels that are smaller than the ships regulated by SOLAS. Finally, in accordance with other IMO requirements under SOLAS, both the EU and Canada require ships to be equipped with an operable Ship Security Alert System.

Regarding ports and harbours, the EU and Canada require the security plans and measures of the ISPS Code in all marine facilities that serve ships on international voyages. They also both mandate restricted access and personnel security clearance in sensitive areas around ships in port. In addition the EU already does, and Canada will, apply measures at least complementary to the

ISPS Code to the facilities that service domestic shipping that is subjected to security requirements.

The prescriptions of the ISPS Code are the subject of criminal penalties in the event of violation in both the EU and Canada, but, in addition, Canada imposes two types of alternative, intentionally streamlined and quicker, administrative penalties. Instead of prosecution, an alleged perpetrator of an offence may be charged with a violation and fined unless a timely appeal is launched for a hearing about the incident, or a perpetrator may be invited to sign an assurance of voluntary compliance in future in addition to paying a fine for the past violation.

Concerning seafarers, convergence also marks the steps the EU and Canada are taking towards security clearance and identification. Neither yet applies the ILO's revised Convention on Seafarers' Identity Documents but the EU has requested Member States to ratify it and Canada is working towards its implementation. Respecting the 2005 Protocol, which increases the criminal offences under the SUA Convention, the EU has similarly urged its Member States to ratify it. Canada has not, as yet, ratified the Protocol but already has wider criminal proscriptions against terrorism than the SUA Convention.

Marine surveillance and domain awareness are important matters of current concern to both the EU and Canada. Both are working with IMO to establish its proposed LRIT and both operate multiple ship, air and radar surveillance systems over their marginal seas together with national databases. The EU is additionally seeking to unify and enhance the existing Member States' ship tracking systems by establishing a Europe-wide marine observation and data network.

Beyond these internal actions and policies, the EU and Canada also recognise cooperation with other states as an essential part of the struggle to suppress maritime terrorism. Canada believes its interests are best served by working with like-minded states in institutional capacity building, in harmonising operational guidelines and standards, and in sharing best practices over maritime security. It pursues these objectives by fostering global partnerships through, for example, the G8 Roma/Lyon Process, Asia-Pacific Economic Cooperation's Marine Security Experts Sub-Group and the Organization of American States.[140] The EU has similar external cooperative involvements in addition to its internal thrust to achieve a unified and integrated

[140] Remarks of L. Kinney, Director General of Marine Security, and Marc Mes, Director, Marine Security Operations, Transport Canada, at "Canada and the IMO: Maritime Symposium 2008," Halifax, Nova Scotia, 17 November 2008.

marine policy, including maritime security, over the common European maritime area.[141]

Of particular importance to both the EU and Canada are their relations with the United States. Both have established a variety of bilateral institutional relationships and administrative arrangements with the United States for the furtherance of maritime security. Specific cooperative activities as a result of these arrangements include the posting of US Customs and Border Protection agents in EU and Canadian ports, and reciprocal appointment of customs officers in US ports. These postings implement the US Container Security Initiative, although Canada's participation predates the formal establishment of that US programme. Canada and European Member States have also pursued with the United States a varying degree of bilateral discussion or agreement about boarding and inspecting each other's flagged vessels.

The US CSI 96-hour and 24-hour security programmes discussed above have heavy information requirements that have not been resisted by other states, probably as a result of their desire to maintain positive trade and economic relations with the United States. However, the cargo related data demanded by the United States continues to increase. For example, the latest addition at the time of writing was the so-called "10 + 2 Rule," which was submitted in November 2008 to the US Federal Register as an interim final rule with effect 60 days after publication. This Rule requires importers to submit 10 data elements about their cargo at least 24 hours before it is loaded in the port of origin and demands carriers supply two further data elements—the vessel's stowage plan and any container status messages—within 48 hours of departing from that port. It is anticipated that these greater informational demands by the United States in its pursuit of cargo security will be mutely accepted as the industry has adapted to the rising volume of similar requirements in the past.

Canada cooperates with the United States in maritime security further than the EU in two particular ways. Canada and the United States have a bilateral arrangement for the reciprocal recognition of each other's ship security documentation. Canada has also established a comparable cargo programme, Partners in Protection, to the US C-TPAT initiative that is supposed to fast-track containerised cargo at border crossings.

The present point of divergence in this otherwise cooperative spirit amongst the EU, Canada and the United States appears to be their policies about cargo scanning. The US *SAFE Port Act* sets the level of scanning of arriving containers at 100 percent. This target, already noted to be likely to fail

[141] The EU also exercises unique supranational authority to impose a mandatory inspection and compliance regime over Member States. This power adds an extra layer of maritime security oversight to which Canada is not subject.

in implementation in the United States, is supposed to be achieved by 2012. At present, the EU and Canada only engage in scanning a small percentage of containers as a result of their risk assessments of cargo documentation. Neither seems intent on increasing the proportion of its own scanning. Moreover, while Canada has not spoken out, the EU has expressed strong objections to US plans to advance to 100 percent scanning of inbound containers, asserting that the costs and delays involved will be severe. For certain, the physical interruption in the movement of containers for the purpose of scanning their cargo contents is a very much greater interference in the free flow of the international supply chains than the heavy informational burden of advanced notification about those cargoes. As a result, it is argued, trade will be inhibited and competitiveness will be reduced. In any case, 100 percent cargo scanning would amount to abandonment of the risk management approach espoused throughout the multilateral platform of maritime security as well as the United States' own programmes, as the US Government Accountability Office itself has reported.[142]

A quite separate aspect of maritime security that is worthy of consideration is the repetitive nature of security checks liable to be imposed even in a supposedly security fast-tracked supply chain, such as those of US C-TPAT participants, or of AEOs within the SAFE Framework guidelines of the WCO. A single container of cargo may pass through several frontiers from its inland origin, across the ocean, and on to its inland destination; to use the language of the ISPS Code, such a container will be involved in a number of ship, port and terminal interfaces. For example, a cargo from Germany bound for Chicago via Rotterdam and Halifax, Nova Scotia, might be interdicted for inspection at the German/Dutch frontier, in the port of Rotterdam, in the port of Halifax, and at the US/Canadian border. While each state is entitled to exercise its sovereign powers to inspect cargo arriving at its borders, the multiplicity of effort to apply the ISPS Code-mandated or similar measures at every stage of the movement seems excessively wasteful of resources and likely to create unnecessary delay in trade deliveries. One may legitimately wonder about the success of the risk management approach to maritime security when, as reported, a shipment can suffer 28 security documentation or inspection

[142] Government Accountability Office, n. 94 above, p. 18. Perhaps changes are afoot. The latest indications, in April 2009, are the Obama Administration is moving away from its expectation of 100 percent inbound containerscanning. Attributed to Secretary Janet Napolitano by Ahern, Jayson (2009), Testimony before the House Appropriations Committee, Subcommittee on Homeland Security, on Cargo and Container Security, April 1, 2009, available: http://www.dhs.gov/ynews/testimony/testimony_1238603858577.shtm (retrieved 10 April 2008).

requirements in one 5-day voyage between Canada and the United States.[143] This unspoken problem of administration seems to beg the attention of the EU and Canada as well as other states that promote risk management of maritime security.

11.5. Conclusion

The EU and Canada have each put in place the ISPS Code and are moving towards fulfilment of the other elements of the multilateral platform of international maritime security. In these endeavours they have worked cooperatively with third countries, particularly the United States. Now they are addressing the security threats to their domestic shipping in apparently comparable ways. A very high level of convergence in the approaches of the EU and Canada to maritime security is evident. Divergence from the ISPS Code, in the form of unilateral action exceeding its requirements, only seems to occur in two respects: (1) the application by Canada of the ISPS Code to smaller, "non-SOLAS" ships, and (2) the use by Canada of administrative penalties as alternatives to the criminal prosecution of Code violators.

The most significant divergence between EU and Canadian perspectives arise over cooperation with the United States. Canada clearly has a closer operational relationship than the EU with the United States. Amongst cooperative practices, their reciprocal recognition of shipping security documents is clear evidence of that. By contrast, while Canada, like the EU, only engages in scanning a small percentage of cargo containers, the EU has spoken strongly against the United States' goal of 100 percent scanning. This difference of opinions over the cost effectiveness and risk management of different degrees of cargo scanning is likely to present on-going problems in the administration of cargo security programmes on the ground and to require continuous negotiations at the policy level between the EU and the United States as well. Canada has not made public its views on the issue but, given its shared landmass and borders with the United States, it is obviously more difficult for Canada to resist its neighbour's initiative even if it wishes to.

Yet the potential tension over this difference in plans and perspectives may, perhaps, be relieved ultimately by the inability of the United States to reach its goal of 100 percent scanning as a result of the practical problems it presents, and the difficulty, as the US Government Accountability Office has

[143] As recounted by J. Greenway, Vice-President Operations, Seaway Marine Transportation, at "Canada and the IMO: Maritime Symposium 2008," Halifax, Nova Scotia, 17 November 2008.

reported, that the United States is having in fulfilling the mandate of the SAFE Port Act. A more pressing problem that seems not to have been engaged by the EU, Canada or the United States in promoting maritime security is the expense, wasted effort and delay, along with the resulting costs incurred by commercial parties, consumers and taxpayers, that may be occasioned by multiple cargo scans and documentary checks. The EU and Canada, along with the United States, appear to need to extend their dialogue about the administrative quality and efficiency of their risk management of maritime security.