EUROPEAN CONFERENCE OF MINISTERS OF TRANSPORT

CONTAINER TRANSPORT SECURITY ACROSS MODES

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

OECD

EUROPEAN CONFERENCE OF MINISTERS OF TRANSPORT

CONTAINER TRANSPORT SECURITY ACROSS MODES

ORGANISATION FOR ECONOMIC
CO-OPERATION AND DEVELOPMENT

OECD

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT

The OECD is a unique forum where the governments of 30 democracies work together to address the economic, social and environmental challenges of globalisation. The OECD is also at the forefront of efforts to understand and to help governments respond to new developments and concerns, such as corporate governance, the information economy and the challenges of an ageing population. The Organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice and work to co-ordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Japan, Korea, Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom and the United States. The Commission of the European Communities takes part in the work of the OECD.

OECD Publishing disseminates widely the results of the Organisation's statistics gathering and research on economic, social and environmental issues, as well as the conventions, guidelines and standards agreed by its members.

EUROPEAN CONFERENCE OF MINISTERS OF TRANSPORT (ECMT)

The European Conference of Ministers of Transport (ECMT) is an inter-governmental organisation established by a Protocol signed in Brussels on 17 October 1953. It comprises the Ministers of Transport of 43 full Member countries: Albania, Armenia, Austria, Azerbaijan, Belarus, Belgium, Bosnia-Herzegovina, Bulgaria, Croatia, the Czech Republic, Denmark, Estonia, Finland, France, FRY Macedonia, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Moldova, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia and Montenegro, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine and the United Kingdom. There are seven Associate member countries (Australia, Canada, Japan, Korea, Mexico, New Zealand and the United States) and one Observer country (Morocco).

The ECMT is a forum in which Ministers responsible for transport, and more specifically the inland transport sector, can co-operate on policy. Within this forum, Ministers can openly discuss current problems and agree upon joint approaches aimed at improving the utilization and at ensuring the rational development of European transport systems of international importance.

At present, ECMT has a dual role. On one hand it helps to create an integrated transport system throughout the enlarged Europe that is economically efficient and meets environmental and safety standards. In order to achieve this, it is important for ECMT to help build a bridge between the European Union and the rest of the European continent at a political level.

On the other hand, ECMT's mission is also to develop reflections on long-term trends in the transport sector and to study the implications for the sector of increased globalisation. The activities in this regard have recently been reinforced by the setting up of a New Joint OECD/ECMT Transport Research Centre.

Also available in French under the title:
La sûreté du transport intermodal de conteneurs

Further information about the ECMT is available on Internet at the following address:
www.oecd.org/cem

Foreword

The events of 11 September 2001 highlighted the vulnerability of many aspects of the transport system, in particular the weaknesses in links among modes along the transport chain and the need for a coordinated security approach among modes.

A new wave of heightened security measures has emerged to address security weaknesses in the transport system since 2001. These measures are designed to ensure maximum protection from terrorist activity and are built on an existing security framework established over many years. These efforts, however, have mostly been concentrated within individual modes. It is also increasingly accepted that in the transport of freight, specific weaknesses may exist in the linkage points between modes along the transport chain.

In this context, OECD and ECMT joined forces to examine the security of the container transport chain, responding to mandates of both the ECMT Council of Ministers in Bucharest in May 2002 and the OECD Maritime Transport Committee in Paris in July 2002.

This study highlights vulnerabilities in both inland and maritime container transport. Maritime containers are the focal point as opposed to other types of containers because they are the most numerous container type in international trade, are truly intermodal, and are ubiquitous. In addition, the study specifically focuses on the potential threat of containers being used by terrorists as a delivery vehicle for chemical, biological, radiological or nuclear (CBRN) weapons, as this scenario largely underpins the national and international policy agendas at this time.

The findings of this report were agreed by ECMT Ministers at their Ljubljana Council and the OECD Maritime Transport Committee in Paris in May 2004.

Acknowledgements. *OECD and ECMT would like to sincerely thank the governments of OECD and ECMT member countries, representatives of industry and of international organisations who provided helpful input to this report. Special thanks are extended to the following entities for their contributions to the report: Alliance of Japan Cargo Inspection Associations (AJCIA), Bureau International des Containers (BIC), Commission Centrale pour la navigation du Rhin (CCNR), European Commission (EC), CLECAT, European Shippers Council (ESC), International Chamber of Shipping (ICS), International Road Transport Union (IRU), Japan International Freight Forwarders Association (JIFFA), International Union of Railways (UIC), International Union of combined Road-Rail transport companies (UIRR), United Nations Economic Commission for Europe (UN-ECE), World Customs Organisation (WCO) and the World Shipping Council (WSC).*

Philippe Crist of OECD, and Mary Crass and Masatoshi Miyake of ECMT drafted the report.

Table of Contents

List of Box

List of Tables

List of Figures

Glossary

ACI	Advance Cargo Information. See Annex B.
ADN	European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (2000), which was adopted by the Diplomatic Conference organized jointly by the UN-ECE and the CCNR.
ADNR	CCNR's Provision concerning the Carriage of Dangerous Goods on the Rhine.
ADR	European Agreement Concerning the International Carriage of Dangerous Goods by Road (1957), which was done under the auspices of the UN-ECE.
ANSI	American National Standards Institute.
APEC	Asia-Pacific Economic Cooperation.
BASC	Business Anti-Smuggling Coalition. See Annex B.
BIC	Bureau International des Containers et du Transport Intermodal.
CBRN weapon	A chemical, biological, radiological or nuclear weapon.
CCNR	Central Commission for Navigation on the Rhine.
consignment	Freight sent under a single contract of carriage.
container	Generic term for a box to carry freight, strong enough for repeated use, usually stackable and fitted with devices for transfer between modes.
CSI	Container Security Initiative. See Annex B.
C-TPAT	Customs-Trade Partnership Against Terrorism. See Annex B.
FCL	Full container load.
FIATA	International Federation of Freight Forwarders Associations.
ICC	International Chamber of Commerce.
ILO	International Labour Organisation.
IMO	International Maritime Organisation.
IRU	International Road Transport Union.
ISO	International Organization for Standardization.
intermodal transport	The movement of goods in one and the same loading unit or road vehicle, which uses successively two or more modes of transport without handling the goods themselves in changing modes.
ISPS Code	IMO's International Ship and Port Facility Security Code adopted in December 2002. See Annex B.
ITU-R	International Telecommunications Union – Radiocommunication Sector.
LCL	Less-than-full container load.

lift-on-lift-off (LO-LO)	Loading and unloading of intermodal transport units (ITU) using lifting equipment.
NII	Non-intrusive inspection.
NVOCC	Non-Vessel Operating Common Carrier.
OSC	Operation Safe Commerce. See Annex B.
RFID	Radio Frequency Identification tag.
RID	Regulations concerning the International Carriage of Dangerous Goods by Rail (1980), an annex to the Convention concerning International Carriage by Rail (COTIF).
roll-on-roll-off (RO-RO)	Loading and unloading of a road vehicle, a wagon or an intermodal transport unit (ITU) on or off a ship on its own wheels or wheels attached to it for that purpose. In the case of rolling road, only road vehicles are driven on and off a train.
SOLAS	IMO's International Convention for the Safety of Life at Sea (1974). See Annex B.
SST	Smart and Secure Tradelanes. See Annex B.
swap body	A freight carrying unit optimised to road vehicle dimensions and fitted with handling devices for transfer between modes, usually road/rail.
Terminal	A place equipped for the trans-shipment and storage of intermodal transport units (ITU).
TEU	Twenty-foot Equivalent Unit. A standard unit based on an ISO container of 20 feet length (6.10 m), used as a statistical measure of traffic flows or capacities. One standard 40' ISO Series 1 container equals 2 TEUs.
TIR	Transports Internationaux Routiers System. See Annex B.
UCR	Unique Consignment Reference developed by WCO. See Annex B.
UN-CEFACT	United Nations Centre for Trade Facilitation and Electronic Business.
UN-ECE	United Nations Economic Commission for Europe.
UN-EDIFACT	United Nations Electronic Data Interchange for Administration, Commerce and Transport.
WCO	World Customs Organization.
XML	Extensible Mark-up Language.

ISBN 92-821-0331-5
Container Transport Security Across Modes

Executive Summary

Transport authorities face a number of crime and security challenges relating to the systems under their jurisdiction. These include theft of goods and vehicles, attacks on truck drivers, illegal immigration, transport of dangerous goods and drug and contraband smuggling. In addition to these crime-related challenges, authorities must remain vigilant to possible terrorist use or targeting of transport vehicles and infrastructure. Among these multiple threats, however, one in particular has consistently been cited as being extremely important and requiring a co-ordinated international response – this threat is the possible misuse by terrorists of the *maritime shipping container transport system*. The ubiquity of these containers was, and is still, seen as the system's principle strength and sign of success. However, after the September 11th attacks on the United States, many countries realized that they had relatively little control over possible misuse of the system by terrorists.

In particular, the threat of a Chemical, Biological, Radiological or Nuclear Weapon (CBRN) being delivered via an anonymous shipping container has risen above other terrorist-linked threats to containerised transport and has become a principal driver of international transport security policy since 2001. This has had a direct impact on Transport authorities, as they are charged with ensuring the efficient flow of goods while at the same time ensuring that the parts of the container transport chain under their jurisdiction are as secure as possible.

Transport authorities must address weak links of the container transport chain

One of the greatest difficulties in addressing the security of the container transport chain is that there is no single system governing the international movement of containers, in fact the opposite is true – container transport is characterised by complex interactions among multiple actors, industries, regulatory agencies, modes, operating systems, liability regimes, legal frameworks, etc. Many of the security concerns in the container transport chain are related to inland carriers and freight integrators operating in the first few and last few links of the chain. These actors are numerous, disparate in nature and activity, operate on tight margins, and, as a result, represent more of a security risk than their larger counterparts further down the chain (*i.e.* large land, port and maritime transport operators). *It is on these larger actors and their activities that most international and bilateral security initiatives have been focused to date.*

Addressing the security of the container transport chain requires a comprehensive intermodal framework integrating measures across the entire container transport chain. *Whereas such a framework may exist at the centre of the chain covering ports and maritime transport, as codified in SOLAS and the International Ship and Port Facility Security Code (ISPS), there is not yet an analogous framework for inland transport on the outer edges of the chain.* Furthermore, while elements of this framework are emerging through the C-TPAT (for US trade), the BASC (for certain large shippers), the UN-ECE (under development for freight

forwarders and shippers), the WCO (in their "cradle-to-grave" container stuffing and seal management guidelines) and in the proposed EU Freight Security Directive, *none of these address the container transport chain in its entirety*.

More specific threat assessments involving Transport authorities needed

The spectre of containers being used to deliver chemical, biological, radiological and/or nuclear (CBRN) weapons has motivated international action to bolster the security of the container transport chain. *However, very real questions remain as to terrorists' readiness, motivation and/or capability to use a container as a delivery platform for a CBRN weapon.* These questions should not preclude action to bolster container security – especially insofar as containers can be misused by terrorists for other purposes – but they should, at a minimum, be addressed more thoroughly through national/international assessments of specific risks posed by terrorists to the container transport chain.

In their role as facilitator and supporter of efficient transport solutions for trade, Transport authorities need to be involved in this process. Differentiating the threat is important to Transport authorities because ill-adapted security measures can slow down or block the flow of goods nationally and internationally, while on the other hand, well designed measures can actually facilitate trade.

Security measures must be adapted to the threat

Specific security measures must be adapted to specific terrorist modus operandi. Terrorists targeting the container transport chain will likely use one of two approaches: *i)* they will intercept a legitimate consignment and tamper with it ("hijack" scenario); or *ii)* will usurp and/or develop a legitimate trading identity to ship an illegitimate and dangerous consignment (the "Trojan horse scenario").

Generally, the measures used to mitigate the threat of these scenarios fall into five groups: container scanning, ensuring the integrity of the container itself, controlling access to the container, tracking containers, and assessing container risk via the analysis of trade-related data. *Not all of these measures are equally suited to counteract both the "hijacked container" and "Trojan horse" threats as described above: what works for one scenario will not necessarily work for the other.*

Policy levers at the disposal of Transport authorities

Transport authorities can play an important role in countering the "hijacked container" scenario by enhancing security at all points along the chain. This involves ensuring that transport operators take into account security measures relating to container integrity and sealing, securing the access to the container and facilitating container tracking – this is especially important for inland Transport authorities who exercise oversight on the vulnerable outer links of the container transport chain. On the other hand, Transport authorities have considerably less scope for action in thwarting a "Trojan horse" shipment. In the latter case, effective Customs control is of paramount importance.

In addressing the security threat to the container transport system, Transport authorities should: *a)* establish and/or build on rules governing container handling by operators under their authority and define procedures regarding container integrity, access and tracking; *b)* introduce security criteria in the licensing process of vehicles, operators, personnel and facilities and monitor whether licensees continue to meet these security requirements; and *c)* communicate to Customs information regarding operators under their jurisdiction that might be useful in the container screening process.

Guiding principles to secure the container transport chain

Container security is a shared responsibility among all actors; any breach in security in one link compromises the security of the entire chain. However, because they are the only main actors with "real" contact with the contents of the container, *shippers and/or those stuffing the container must play a primary role in securing the container transport chain*. Accordingly, shippers and/or those stuffing a container should follow established *security procedures*, initiate an *auditable custody trail* and ensure that the container is *sealed* with, at a minimum, a *high-security mechanical seal*.

Electronic-seal technologies, *are not* currently ready for commercial deployment for international use throughout the global container handling network – primarily because of the multiplicity of competing and incompatible operating standards and limited operational experience. These conflicts will most likely be overcome yet, until that happens, Transport and/or Customs authorities should not *mandate* the use of e-seals. If such a mandate is given at a later date, a clear distinction must be made between *security-relevant* e-seal data (*e.g.* seal status and container number) and *supply-chain management-relevant* data (packing list, shipper, consignee identity, etc.). While the former should eventually be made mandatory, the latter should not.

Vulnerabilities in the container environment are highest in rail yards, road stops and parking and shipping/loading terminal facilities. Thus, insofar as these nodes are concerned, every effort should be made to physically secure the premises and to minimise the risks of unauthorised access. Thus, transport operators should screen employees according to security criteria. They should also check worker identification with other operators and develop protocols regarding access to containers by high security-risk workers in accordance with national laws.

The focus of container tracking should not be "*real-time*" but rather "*right-time*" tracking – that is, ensuring that those who need to find out where a container is can do so *when* they need to know. In this context, most existing operator-specific tracking systems are sufficient for this purpose. Transport authorities should *ensure that appropriate government agencies have access to this data as needed*. In those cases where "*real-time*" tracking is the right solution, these systems should not be deployed without the back-up of a more "traditional" chokepoint control tracking system.

Screening and scanning of containers, while complementary, are not the same. 100% container screening is possible, should an administration choose to do so – 100% scanning, on the other hand, is not practical with current technologies. Insofar as container screening is concerned, Transport authorities should assist Customs by ensuring that "proprietary" information (*e.g.* regarding transport operators, licensees, etc.) is made

available to Customs for their container risk assessment. Transport authorities should also support the concept of advanced information submission to Customs and use of the Unique Consignment Reference number among transport operators to further facilitate container screening.

Specific recommendations to inland Transport and Maritime authorities

Transport and Maritime authorities should implement agreed international rules and recommendations. These include the ECMT Ministerial Declaration on Combating Terrorism in Transport, the 2001 Ministerial Conclusions on Combating Crime and the ECMT Resolution No. 97/2 on Crime in International Transport. Likewise, countries should comply with the amended SOLAS Convention and the ISPS code that govern security measures for international ocean-going vessels and ports by the July 1, 2004 deadline.* Finally, authorities should seek to go beyond these international agreements to ensure that those parts of the container transport chain not currently secured are included in a comprehensive security framework that embodies the guiding principles outlined above.

* By early August 2004, IMO was able to report that, according to the latest figures available to the IMO Secretariat from reports received by Governments, almost 90 per cent of over 9 000 declared port facilities had their Port Facility Security Plans approved, while the information available from industry sources on International Ship Security Certificates (ISSCs) issued for ships which have to comply with the new regulatory regime, indicated that the compliance rate was well beyond 90 per cent. *Source:* IMO Press Briefing *www.imo.org/Newsroom/mainframe.asp?topic_id=848&doc_id=3756*.

ISBN 92-821-0331-5
Container Transport Security Across Modes

Chapter 1

Introduction

1. Context and mandates for this report

The events of 11 September 2001 in New York City and Washington highlighted the vulnerability of modern transport systems to be used and/or targeted by terrorists in mass casualty attacks. Of a nature and scale of destruction surpassing that of previous terrorist activity, the New York and Washington D.C. attacks served as a catalyst for a new wave of heightened security measures at international, national and local levels.

These new measures have been designed to take stock of security weaknesses revealed in the 2001 attacks; specifically, they aim to minimise terrorist threats, share good practice and assess necessary technical, legal and legislative adjustments to ensure maximum protection from terrorist activity in transport. The measures have built on an existing security framework for transport, established over many years in response to previous traumatic events involving transport such as the explosion of Pan Am flight 103 over Lockerbie, Scotland in 1988 and the numerous terrorist acts to notably public transport infrastructure and vehicles in Europe and elsewhere in the latter decades of the last century.

However, these efforts to enhance security since the 2001 attacks have mostly been concentrated within individual transport modes. It is increasingly accepted that additional weaknesses may exist in the linkage points between modes along the transport chain – this is especially true for intermodal freight transport. Lack of vigilance at any point in the intermodal freight transport chain could render the entire chain vulnerable to terrorist action. Moreover, fragmented, inconsistent and mode-specific security measures may lead to inefficiencies in resource allocation across the sector and higher costs for industry.

In this context, the ECMT Ministerial Declaration on Combating Terrorism in Transport, agreed in Bucharest in May 2002, requested ECMT and its Associate member countries to seek ways to combine efficiency and security improvements in the transport system with measures combating crime and terrorism, for example, by examining effective ways of tracking goods along the transport chain to prevent inconsistent and incompatible security enhancement measures across modes.

Likewise, at its meeting in July 2002, and following extensive consultations with member governments and industry, the OECD Maritime Transport Committee agreed to undertake a series of studies related to transport chain security – among them, verification of cargo and container tracking.

In order to respond to both mandates, and thereby cover more efficiently both inland and maritime transport, OECD and ECMT joined forces to prepare this report. The document is the synthesis of inputs from governments, industry and international organisations, strengthened by the findings of a joint expert seminar on the topic.

2. Why the focus on terrorism and the container transport system?

Transport authorities face several criminal and terrorist – related challenges. These include theft of goods and vehicles, fraud, illegal immigration, drug and contraband smuggling, potential targeting of dangerous goods shipments and the targeting of transport vehicles and infrastructure by terrorists. These illegal activities pose serious daily problems for authorities and can have important impacts on the transport sector's ability to ensure the efficient flow of goods within the national and international marketplace. Among these multiple threats, several important transport actors representing both industry and government have highlighted the threat posed by the potential terrorist misuse of freight containers (as opposed to palletised and/or bulk shipments) as one needing urgent attention.

While there are a number of freight containers in use within different modes use (*e.g.* Unit Load Devices – ULD's – used in aviation and Swap Bodies used for road-rail carriage in Europe), it is the potential threat to, and from, *maritime shipping containers*, that has been singled out in the context of anti-terrorism policy.

The shipment of goods via shipping containers is an essential component of global trade. The container transport system is to world trade what the circulatory system is to the body – it is difficult to imagine the present level of international exchanges without a functioning intermodal container transport system. This system has proven to be a highly efficient and relatively safe and reliable means of global goods transport across modes.

So why focus on maritime shipping containers to highlight security vulnerabilities in the transport chain instead of on other types of containerised transport? The reasons are three-fold:

1. Maritime shipping containers are the most *numerous* container types involved in international trade.
2. These containers, more so than other container types, are truly *intermodal* in that they are carried by maritime, inland waterway, road and rail operators.
3. Shipping containers, more so than other container types, are truly *ubiquitous*. They are not limited to use within the confines of specific transport infrastructure and nodes but can be found anywhere from major ports to small side-streets and from major cities to small villages.

Since 2001, the spectre of the Container Transport System being targeted by terrorists intent on mass casualties, economic disruption – or both – has haunted policy discussions throughout the international community.

While containers have been and continue to be used and or targeted for criminal purposes (*e.g.* drug and contraband smuggling, money laundering, illegal immigration, container theft, etc.), and that some of these uses have likely benefited terrorist groups, it is important to stress that these misuses of containerised transport are *not* what have motivated most post-September 11, 2001 container security measures.

If there is a generalised concern regarding the use of shipping containers, it is first and foremost because of the potential for these to be used by terrorists as a delivery vehicle for a chemical, biological, radiological or nuclear (CBRN) weapon.

It should be stressed from the outset that this scenario outlines only the *potential* threat posed by the nefarious misuse of containers and that there has been no public confirmation that such a scenario is being actively examined by terrorist groups. Nonetheless, as some

terrorist groups have as a stated goal to inflict large-scale physical and/or economic damage on their enemies, it is prudent that the CBRN threat, or any other threat to the container transport system, be examined by governments. To-date, the CBRN attack scenario has largely underpinned national and international agendas in this field (*e.g.* as evidenced by various national declarations, those of the EU, the G8, and APEC, among others). This report accordingly devotes particular attention to the CBRN weapon threat.

While certain security measures are solely linked to the CBRN weapon threat, there are synergies between terrorism-related security measures and those designed to prevent/sanction non-terrorism-related areas of transport crime.[1] This is particularly important when weighing the costs of container-specific security measures relative to the constraints that they place on transit of goods along the transport chain. When a policy agenda is driven by a cataclysmic scenario – such as that of the "bomb in a box" that this report specifically addresses – all measures, even the most expensive ones, make sense.

Better nuancing these scenarios through risk assessment exercises that seek to investigate the *probability* or possibility of a container being used in a CBRN attack can go a long way to provide a better framework for making cost- and trade-efficient decisions.

In this context, better risk assessment will be important for governments – in particular for Transport authorities, whose role as a facilitator of efficient transport solutions for trade is complicated somewhat by enhanced security constraints that can slow down or block the flow of goods and services nationally and internationally.

Heightened security measures should not be seen in all cases as obstructions to legitimate trade, however. Potential win-win situations could be seen between trade security and trade facilitation, where the costs of higher security can be recovered, at least partially, through greater efficiencies in the supply chain. Improved security and integrity of the transport chain can reduce the danger of tampering and direct costs of theft losses. Moreover, more focused and automated customs inspection with timely transmission of accurate information can improve efficiency of customs control and lower direct costs of customs clearance. For example, the World Customs Organisation (WCO)'s Advance Cargo Information Guidelines allows identification of security-relevant data elements on a consignment and offers guidelines for their early collection by Customs.[2] Measures such as these can help ensure the integrity of transport chain and improve the efficiency of customs clearance which, in turn, can reduce delays or uncertainty of delivery, lower supply chain costs as a whole through improved inventory management and improved customers' confidence in service quality and, therefore, facilitate trade and transport.

3. Transport authorities' role in container security

Before going further, it is important to note two things. The first is that a distinction must be made between the *Supply Chain*[3] which covers the entire manufacturing and commercial environment surrounding the design, sourcing, transport and return of goods and the *container transport chain* which concerns the movement of those goods via shipping containers. The latter, which is the focus of this report, is a sub-component of the former and, although the two are linked in very substantive ways, they are different in that the former relates to the *goods* being traded and the latter to the *containers* being moved.

From a regulatory perspective, containerised transport is a hybrid system involving moving goods in specialised packaging (the container) utilising different modes of carriage. While Transport authorities typically have authority over the latter, Customs and Trade

authorities have responsibility for the former. While mitigating threats to transport vehicles and infrastructure are an integral part of the international container security equation, Transport authorities are not necessarily those best able to ensure proper oversight over the container itself. Insofar as the principal terrorist threat related to the container transport chain concerns the *contents* of the containers, and not the *vehicles* used to transport the containers, Customs authorities play a prominent role in ensuring the security of the system.

If this is the case, then where are the points of policy leverage for Transport authorities? Why should Transport authorities feel concerned by this problem?

First, in cases of catastrophe involving transport vehicles or infrastructure, transport Ministries are among those first called to the front line to respond to the crisis.

Secondly, Transport authorities do have some say over the manner in which carriers under their authority handle containers and can establish rules to govern container handling by these parties. Furthermore, they also play an important role as "gatekeeper" to the freight transport market via their regulatory oversight and licensing of transport companies, operators, and vehicles.

Thirdly, Transport authorities have a role to play in improving the transparency and communication of information regarding those actors handling and transporting containerised consignments.

4. Objective and structure of this report

This study aims to describe the complex, hybrid system through which containers pass – from the time the container is packed, via loading and unloading at intermodal terminals and on maritime vessels, to the time it is delivered to the consignee. It attempts to provide Transport authorities and their constituencies with a comprehensive examination of container security, identifying the key actors involved in and issues related to mitigating the threat of terrorism using containerised cargo, and assessing where vulnerabilities lie along the supply chain.

The report does not aim to place responsibility for container transport security squarely on the shoulders of Transport authorities; rather it tries to highlight ways in which governments and Transport authorities in particular can in a co-ordinated way contribute to enhancing the movement of containers and their contents efficiently and effectively throughout the system. Moreover, it attempts to situate container transport security – a major driver at present for international measures to combat transport terrorism as mentioned above – in the wider context of transport crime and security issues, pointing out where synergies can be found between existing policies and measures to combat transport sector crime, and where new enhanced measures are needed.

This report is structured as follows: Chapter 2 and Annex A describe the complexity of the supply chain involving various actors and flows of containerised goods and information. Chapter 3 addresses comprehensive risk management, Chapter 4 discusses measures and strategies to reduce terrorist risk to the container transport chain and Chapter 5 offers conclusions and proposes ways forward for governments, particularly Transport authorities.

Notes

1. For example, international carriage of dangerous goods by rail, road, and inland waterways is regulated respectively by Regulations concerning the International Carriage of Dangerous Goods by Rail (RID), the European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), and the European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN).
2. See Chapter 4, Section 5 for further discussion of Trade documentation and information.
3. The Supply Chain integrates suppliers and clients (comprised of stores, retailers, wholesalers, warehouses, and manufacturers) so that goods are produced and distributed at the right quantities, to the right locations, and at the right time, while minimising total costs and satisfying service level demands (*www.stanford.edu/~jlmayer/Article-Webpage.htm*).

ISBN 92-821-0331-5
Container Transport Security Across Modes

Chapter 2

The Container Transport Chain

One of the greatest difficulties in addressing the security of the container transport chain is that there is no single system governing the international movement of containers. Not only is there not a single system (be it commercial, operational or regulatory), but the opposite is true – container transport is characterised by the complex interactions among a great multitude of actors, industries, regulatory agencies, modes, operating systems, liability regimes, legal frameworks, etc. These have co-evolved over the past half-century into a global network that has become extremely efficient at delivering goods at low cost and on time. However, the trade-focused evolution of the container transport system has led to the existence of a number of security vulnerabilities that might be exploited by terrorists. This section describes some of the most important of these.

1. General background on containers

Most of the world's non-bulk cargo travels in marine shipping containers. These standardised boxes have revolutionised the international transport of goods involving a sea leg since their first appearance in the 1950s and have given rise to a multitude of specialised road, barge and rail carriers, a fleet of over 2 700 modular container ships and the emergence of a global network of several hundred highly automated port handling facilities. The basic shipping container is nothing more than a reinforced steel box with one double door providing access on one side. These "dry box" containers are supplemented by many other container types including tank containers for gaseous or liquid cargoes, open frame containers for transporting odd-sized consignments, soft-top containers, containers fitted with special garment racks and/or refrigeration units ("reefers") for transporting chilled food. All of these containers share standard fittings on all corners that allow them to be stacked and racked on board vessels, train wagons, truck chassis, etc.

In 2002, the Bureau International des Containers (BIC) estimated that approximately 15 000 000 TEUs[1] were in circulation worldwide.[2] The World Shipping Council estimated that by mid-2003 approximately 17 000 000 TEUs were in circulation accounting for 10.8 million individual containers.[3]

The global container fleet is almost evenly divided between carriers' self-owned fleets and those of the many large container-leasing companies.[4] While the bulk of the container fleet is comprised of simple "dry boxes", a significant number are of the specialised types described above. These are relevant from a security perspective because each of these container types pose special risks. Full tank containers are not easily scanned, their contents are difficult to visually check, they can contain harmful substances and they can be modified as dispersal platforms for chemical/biological agents. Refrigerated units ("reefers") have insulated walls and refrigeration equipment – both of which can be used to disguise explosive devices. Finally, open-top containers are vulnerable to un-authorised access via the tarpaulin covering the top. This vulnerability, however, is tempered by the fact that these containers are also easy to visually inspect.

Most container moves involve an international sea leg. Figure 2.1 illustrates global flows of containers along the principal trade routes in 2002. These flows accounted for 37.7 million TEUs or roughly 24.3 million actual box moves concentrated in the dominant Trans-Pacific, Asia-Europe and trans-Atlantic trades. Container traffic figures for world ports from Containerisation Online indicate that over 264 million containers were handled in 2002. These figures account for all containers handled at the various ports including transhipped containers, empty container moves on both the export *and* import sides. These trade volumes are expected to increase in coming years as world trade increases.[5]

If there are security concerns relating to the use of maritime shipping containers, it is because these have become so tremendously popular and ubiquitous in the world trading system. Ever since their inception in the 1950s as an inexpensive alternative to break-bulk shipping, a greater and greater number of containers have been put into use to carry an ever-growing range of products both within and between countries around the world.

2. Security issues in the container transport chain

The container transport chain is such a complex one that any attempt to describe its various components and their interactions becomes a detailed and highly technical exercise. Understanding these elements and the ways in which they are connected is necessary, however, in order to identify particular security vulnerabilities inherent in the system. Annex A, therefore, provides a very detailed description of the container transport chain and container-transport relevant parts of the Supply Chain. This section is largely drawn on that description and focuses on those elements that are important from a security perspective.

Conceptually, it may serve to visualise the container transport chain, in aggregate, as a massive integrating network. On the outer edges of the network, millions of shippers rely on the services of thousands of intermediaries to organise and carry their goods to hundreds of ports where they are shipped overseas by dozens of maritime carriers. On the other end, the network operates in reverse gradually moving towards a greater state of entropy at its outer reaches where millions of buyers receive their shipments. At each step along the way to the port, the actors tend to become larger, the flows of containers tend to become more dense and concentrated and the overall visibility of the system greater. The opposite is true at each step away from the port.

Again, as there is no central system organising international containerised trade, cross-network optimisation of security measures is extremely difficult. Each component of the system has tended to seek to optimise its own operations and, in some cases, ensure that these are compatible with the next link in the chain. However, it is a well-known tenet in logistics management that the aggregation of individually optimised links leads to a sub-optimal logistics chain. Un-harmonised or inexistent security practices, incompatible operating and information management systems, un-coordinated regulatory frameworks and unclear security continuity protocols among the different links in the container transport chain – and especially at its outer edges – all represent security vulnerabilities that stem from the lack of a co-ordinated approach to securing the container transport chain.

Many of the security concerns in the container transport chain are related to the large presence of small and medium enterprises operating within the system – especially at its outer bounds. It is not so much the size *per se* of these shippers, forwarders, intermediaries and carriers (especially road carriers) that is cited as a vulnerability, but rather their limited resources and motivation to bolster security measures.[6] Thus, governments are faced with

Figure 2.1. **Global container flows along the principal trade routes in 2002**

Projection J. Bertin, 1953.

Source : Containerisation International.

a dilemma – where to intervene in the container transport chain to secure it? For very practical purposes, government intervention has tended to concentrate on the "core" of the system – large intermediaries, major carriers and natural "chokepoints" through which container trade is funnelled.

While the principal focus of governments has been to seek out where they can most effectively "control" the security of the container transport chain, it should be pointed out that there is a wide scope for the various industry actors in the chain to act. Responsible shippers, forwarders, carriers, etc. all represent important and effective allies in the fight against terrorist misuse of containerised trade and should be effectively mobilised.[7] In many cases, the securing of the supply chain could benefit more from the establishment of an auditable trail of existing security measures than from the imposition of new ones. However, there are many barriers to this at present and the following section highlights some issues that must be considered before such an auditable trail or other new security measures can be put in place.The container transport chain is comprised of various actors intervening in three principal flows: the physical movement of the container, the transmission of information regarding the container and its contents and the flow of money.

2.1. Actors in the container transport chain

The actors involved in the container transport chain can be broken down into five sub-groups according to the roles they play. While the groupings proposed below form a good conceptual overview of the actors along the container transport chain, it should be noted that relatively recent developments in the various industries involved have led to a blurring of lines among these functions/actors – most notably in the case of transport operators who have sought to expand their range of non-transport services and become door-to-door logistics providers.[8]

Based on the description in Annex A, a number of actor-related security issues should be kept in mind:

- Most containerised moves start as a commercial interaction between a seller and a buyer. In many cases (but not all) the seller is also the shipper. Both shipper and buyer have detailed knowledge of the transaction leading to the shipment of the container but, in most cases, the shipper is the *only actor in the chain with detailed first-hand knowledge of the goods placed into a container*. This fact is of fundamental importance to efforts seeking to secure the container transport chain.
- Shippers are the most numerous actors in the container transport chain and are characterised by the presence of many small and medium enterprises (SMEs). From a security perspective, the large participation of SMEs in containerised trade has repercussions on efforts to secure the container transport chain. Indeed, efforts to extend supply chain security to the originating shipper must take into account these actors' relative lack of resources available, and/or motivation, to implement security measures.
- A significant portion of international container movements concern intra-firm trade or trade between affiliates or otherwise linked firms. In many respects, intra-firm trade presents potentially fewer security risks as the parties to the transaction are known to each other and trusted – *provided that these firms have in place sufficient security measures*.
- Freight forwarders have tremendous visibility over the entire container transport chain and yet their sometimes hybrid role (*e.g.*, where they act as "carriers" to their clients and as "shippers" to their carriers) can serve to render data regarding originating shippers

Table 2.1. **Actors in the container transport chain**

Role	Actors involved
Primary customers	Seller (manufacturer/originating shipper/exporter)
	Buyer (consignee, importer)
Transaction facilitation	Buying agent
	Freight forwarder or NVOCC
	Customs broker
Transport task (physical movement of container)	Empty container depot operator
	Warehouse/container freight station operator
	Inland terminal operator (*e.g.* road-rail, road-barge, rail-barge)
	Road carrier (local, long-distance)
	Rail carrier[1]
	Barge operator
	Ocean carrier
	Port terminal operator
	Other port service operators
Authorising/regulatory	Transport authorities
	Customs authority
	Import/export licensing authority
	Phytosanitary, sanitary and veterinary control licensing authority
	Port authority
	Import/export statistical agency
	Other actors (chambers of commerce, consulates, etc.)
Financing	Bank (seller's or advising bank, buyer's or issuing bank)
	Insurance provider (carriage insurance)

1. Within Europe, in addition to the rail carrier, other actors intervene in rail transport (*e.g.*, combined transport operators and infrastructure managers).

hard to access. Forwarders are also characterised by a significant number of SMEs that may not be in a position to implement cumbersome or costly security measures.

- Just as with shippers, a significant number of transport operators in the container transport chain are SMEs. This is especially true in the road sector where most container voyages begin and end. Globally, the "first mile" and "last mile" are the most vulnerable as carriage is often undertaken by small entrepreneurs unable and/or unwilling to implement effective security measures.
- The oversight role for containerised transport is split between Transport authorities responsible for vehicles, drivers and operators (and their facilities) and Customs authorities responsible for the contents of the container. Responsibility for the container itself is ambiguous as Customs typically have responsibility for ensuring the integrity of the container once the containers and their contents are presented to a customs office, whereas Transport authorities typically have a role to play in ensuring that the interface between the container and the mode of carriage is safe.
- A secondary issue related to the previous one is the wide disparity in land-side licensing systems. Even among harmonised systems security is rarely a criteria used to deliver operating permits (with the notable exception of hazardous materials carriage).

2.2. Flows in the container transport chain

Physical flows

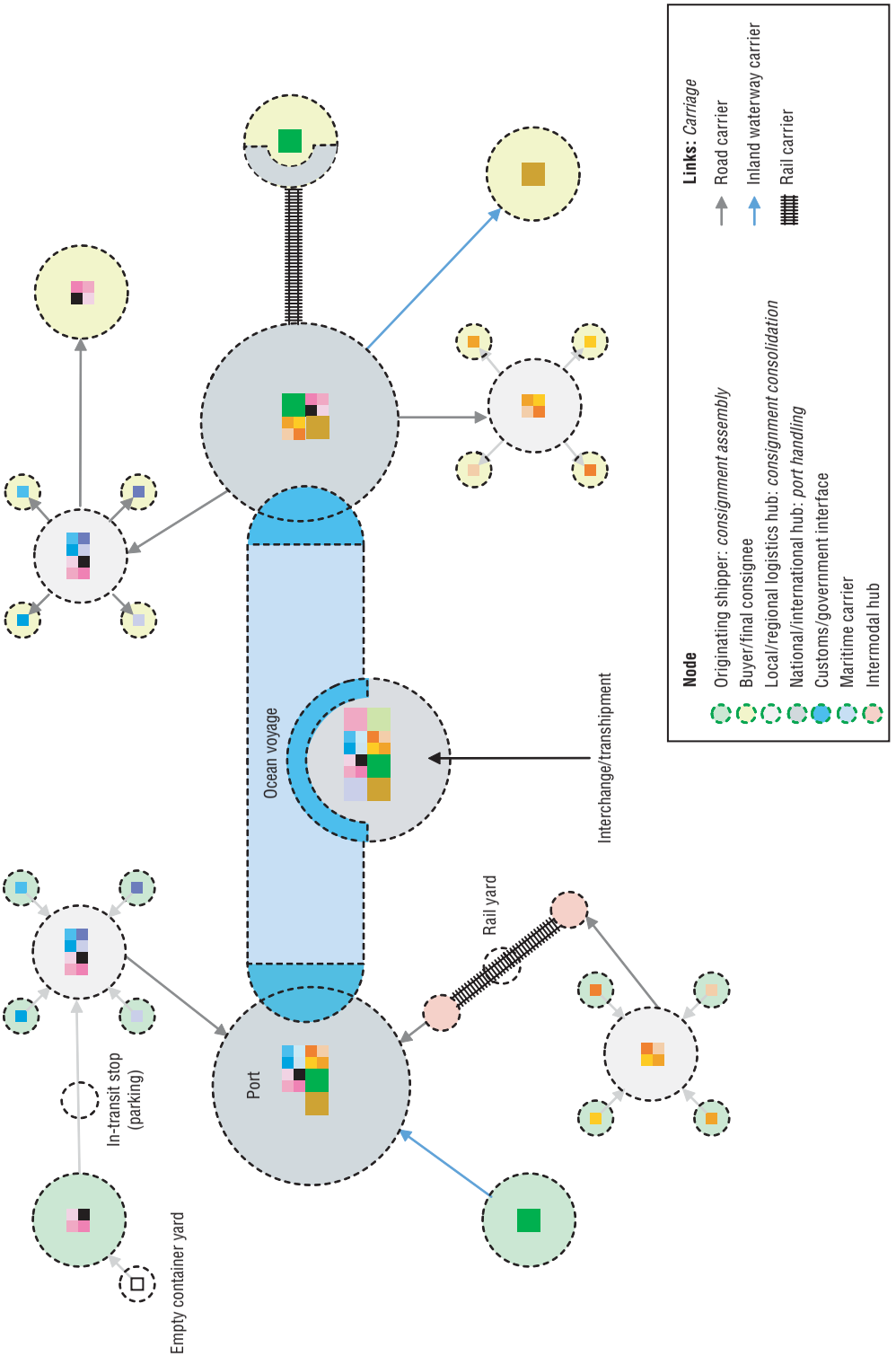
Containers move along a network of nodes and links (see Figure 2.2). The nodes are physical locations where container movement is interrupted and/or containers are handled. Many of these concern multimodal transfer points where containers are transferred from one mode to another. The links between nodes are characterised both by a *mode* of transport (road, rail, inland waterway) and a supporting *infrastructure* (roadway, canal/river, railroad track, rail marshalling yard, etc.). As containers move along this network they can either be empty, loaded with a single consignment (FCL) or loaded with multiple consignments (LCL).

The container transport chain is not uniformly secure and the level of protection offered to containers and their contents can vary tremendously from node to node and among modes. The risk of a security breach at any one of its links can compromise the security of the entire chain and imposes additional costs as additional security checks must be put in place to compensate. Also, the level of protection present at different nodes and in transit is often directly related to the value of the goods being shipped. A major electronics manufacturer will invest much more in securing his/her supply chain than will a small low-volume exporter of inexpensive porcelain objects. And even in cases where relatively high levels of protection are put in place, cargo theft remains a problem. There are literally tens of thousands of "entry points" along modern logistics chains that could be exploited by terrorist groups.

Based on the description in Annex A a number of security issues relating to the physical flow of containers in the transport chain should be borne in mind:

- The specific stuffing location is paramount from a security perspective because it represents the last point in the container transport chain where the physical contents of the container can be visually identified and reconciled with the commercial invoice and/or bill of lading. After the doors are shut and sealed and until they are re-opened by Customs or by the consignee at the final destination, all information regarding the contents of the container (*e.g.*, such as the manifest, the bill of lading and even the commercial invoice) are necessarily unverified. Thus the originating shipper has a critical role to play in the container security by generating a clear, accurate and complete inventory of the physical contents of the container. Proper site security, stuffing procedures and oversight of the stuffing process are necessary for this important link in the chain to be secure. In this regard, the joint IMO/ILO/UN-ECE *Guidelines for Packing of Cargo Transport Units* are being reviewed with the purpose of introducing security relevant guidelines.
- Containers are most vulnerable to being tampered with when they are at rest and least vulnerable when they are in motion. This means that security measures are especially important at those nodes in the network where the container is handled and/or stored.
- Land-side border crossings represent a particular vulnerability as these are characterised by sometimes poor customs control and inefficient processes that give rise to delays that can be exploited by terrorists intent on tampering with truck-borne containers.
- Containers travelling via certain modes are more vulnerable than others. Road carriage presents the greatest security challenge given its multiple stops and open infrastructure/facilities while maritime transport represents the most secure (at least once the containers are loaded onto most typical container-carrying vessels).

Figure 2.2. **Container transport chain: export focus**



- Given that it is extremely difficult to tamper with a container once loaded onto an ocean-going vessel, the quayside crane represents the last physical checkpoint before the container is dispatched to another country. As such, they represent an important security "chokepoint".
- Most international container trade passes through one or several ports. These are natural focus points for security measures – however, as with other nodes in the system – not all ports are uniformly able to put in place effective security measures. This is especially true for the large number of smaller ports that are involved in a minor way in the container trade. While these ports will have to put in place security measures in accordance with the requirements of the ISPS code, the effectiveness of these measures is dependent on government involvement in threat assessment, the adoption of realistic measures, proper approval procedures, adequate funding and subsequent periodic assessments. That all governments will ensure that adequate and appropriate security measures are adopted and enforced has been questioned – not least by other states who, in some cases, are sending their own officials to overseas ports to assess the security measures in place and determine their adequacy.
- While it is feasible that empty containers could be used by terrorists for weapons delivery or logistical support of their operations, this is not very likely given the manner in which empty containers are managed by carriers. Except for certain specialised container types, the routing of empty boxes is not undertaken in any predictable manner thus rendering them nearly useless from a terrorist's perspective.[9]

Information flows

It is said that the principal effort involved in shipping a container internationally involves correctly generating, receiving and processing information related to the container move. The importance of information in the container transport chain is paramount, since it is the examination and cross-examination of these flows that can reveal discrepancies that might indicate terrorist and/or criminal involvement. The amount of data generated by a container move is daunting, however, and can include 30-40 physical documents and several dozen electronic messages. The information collected and transmitted throughout the trade transaction can cover several hundred discrete data elements – many of which are manually re-keyed at some point in the chain and are therefore duplicative and susceptible to operator error. These data are also difficult to cross-reference among the different actors since they are transmitted via a wide range of media including paper files, faxes, proprietary information networks, e-mail, Web interfaces, pager, telephone and verbal commands and/or agreements.

The information traded among the actors ensures that the container is quickly and accurately dispatched from shipper to final consignee, that the consignment meets regulatory requirements and adheres to the terms of the commercial contract between buyer and seller. Accordingly, the flow of information in the container transport system can be broken down into three principal categories covering information relating to: *a)* trade contracts; *b)* regulatory compliance; and *c)* operational details. These categories are not mutually exclusive and in some cases they may overlap. Based on the description of these flows in Annex A, the following issues should be highlighted for their security relevance:

- Much of the security-relevant information generated early on in the commercial contracting and documentary credit cycles is not used by Customs to evaluate the

security risk of a consignment. This information is later re-keyed and/or re-transcribed by forwarders and carriers once carriage has commenced and only then made available to Customs. Early access to this information could facilitate and otherwise improve Customs security screening of containers.

- At present, the stream of data related to the movement of the container throughout the supply chain is neither harmonised in its content nor in the supporting media used to transmit this information. The latter include paper files, faxes, phone and oral messages, proprietary data networks and messaging standards, Internet-based systems and open messaging standards. When looking at the entire container transport chain, lack of messaging interoperability is still the rule and not the exception.
- Incompatible message structures and messaging systems are most likely to be found at the outer bounds of the container transport chain, especially among SMEs providing drayage services. On the other hand, considerable progress has been made to develop uniform messaging standards and systems for the core/central part of the transport chain covering forwarders, large land carriers, ports and maritime operators. Accordingly, when Customs have in place electronic filing systems, they are oriented mostly towards these actors, and not necessarily those in the container transport chains that are the first to have knowledge of a consignment or its initial movements (*e.g.*, most small shippers and small road carriers). From a practical standpoint, this means that data submitted to Customs by the former are often re-keyed from data supplied by the latter – raising the possibility of re-transcription errors.
- EDIFACT and ANSI X12 have been the principal messaging standards used for the transmission of international trade-related information. However, because of the relative complexity of their use and the need to pass through a paying third-party value-added network (VAN), rather than an open network such as the Internet, the use of these standards has been limited to large shippers and major actors in the container trade network[10] – thus explaining their use at the "core" (dominated by large actors) rather than at the outlying reaches of the container transport chain (dominated by SMEs).

Notes

1. The unit used to measure container capacity is the TEU ("twenty-foot equivalent unit"), which refers to the length of the standard container box. Given the prevalence of non-standard container sizes (ranging from 10 feet to 62 feet in length), TEU figures are always greater than the actual number of containers in question.
2. BIC, personal communication 2003.
3. World Shipping Council, 2003 ("Liner Shipping: Facts and Figures").
4. See Annex A for relative distribution of container sizes and types.
5. See Annex A for expected trade developments.
6. However, it should also be borne in mind that, at least on the shipper side, large actors generally account for a disproportionately large share of containers shipped in international trade.
7. In particular, existing partnerships such as those developed under the auspices of the ISO, WCO, UN-ECE, etc. and certain national programmes show there are considerable opportunities for private-public partnerships to strengthen the container transport chain.
8. These roles are based on those suggested by R.W. Wagenaar (Wagenaar, 1992) as presented in Oosterhout *et al.*, 2000.

9. Empty containers could, however, be routed with sufficient accuracy for terrorist misuse if the personnel handling the management, allocation, and loading of these containers were under the control of a terrorist organisation – this highlights the need for strong personnel vetting policies for these functions.
10. For instance, it has been estimated that 95% of the Fortune 1 000 companies use some form of VAN-based EDI, whereas only 2% of SMEs do – and in many cases only because their business partners have imposed its use (Virtuele Haven, Messaging: State of the Art EDI XML, 2001).

ISBN 92-821-0331-5
Container Transport Security Across Modes

Chapter 3

Threat Assessment

The previous section and Annex A examine security issues related to the complexity of the container transport chain. It is this complexity, along with the lack of a single controlling entity over the entire container transport chain, which has led many governments and industry specialists to conclude that the system is vulnerable to terrorist misuse. This conclusion is supported by the relative ease with which criminals have used and or targeted the container transport system for their purposes.

Containers have been and still are routinely misused in order to smuggle drugs, contraband goods and even people. Containers are also the target of theft by organised criminal groups. Furthermore, these criminals have shown an increasing level of sophistication in their operations in response to heightened vigilance from customs authorities and other government agencies. If such knowledge is readily available to criminals, it should not stretch the imagination to believe that terrorists have access to such knowledge.

The former point is especially relevant considering that terrorists are often linked to criminal activities that help to raise and/or launder money. In fact, if containers are already being used by terrorists, it is most likely in this respect. Containers have been used to transport suspected terrorists, and trading vessels have generated operating revenue and/or provided logistical assistance in carrying out certain attacks. While the most extensive example of such misuse of the international trading system remains the Sri-Lankan-based LTTE (see OECD *Report on Security in Maritime Transport: Risk Factors and Economic Impact*, 2003), Al Qaida also used maritime transport to deliver components of the bombs used in the 1998 embassy bombings in Tanzania and Kenya (Transcript of United States v. Osama bin Laden [5 v. S(7) 98 Cr. 1023], United States District Court, Southern District of New York) and is suspected to have used containers to smuggle operatives in various instances.

As pointed out above, terrorist groups can use containers in "legitimate" or illegal trade in order to generate revenue in support of their activities. They can also use shipping containers to launder illegitimate funds (much as drug smugglers have done) and/or provide logistical support for their operations. Indeed, up until now, this has been the only way that containers have been used by terrorists. But the threat of the "bomb in a box" remains – indeed, any scan of literature related to container security reveals that the threat of a chemical, biological, radiological and/or nuclear (CBRN) weapon delivered via container is the principal terrorism-related threat to container traffic.

In fact, most of the literature and discourse surrounding the issue of container security *vis-à-vis* terrorism unquestioningly postulates that terrorist groups will seek to use containers as a poor-man's delivery platform for such weapons. Given the tremendous impacts that some container security measures may have on international trade, it is important that this postulate be re-examined – especially since a better understanding of the threat can help to develop more effective responses.

The question is therefore: "will terrorists target containers as a means of delivering a CBRN weapon?". The simple answer is: "no one knows". Not because the answer is unknowable – countries can certainly have a better idea of the threat than they currently do –

but because many government agencies in charge of overseeing the different parts of the container transport chain have not undertaken a thorough and comprehensive risk assessment according to internationally accepted risk management standards. This report will not undertake such an assessment – this is a task more suited to national Customs, Defence, Transport and Intelligence administrations – but will address two points related to the need for a more complete evaluation of the container security threat. The first is a description of what is involved in a comprehensive risk management approach and the second is a discussion of some of the factors that should be considered in such an evaluation.

Finally, this section will also examine the manner in which a terrorist group might actually insert a weapon into a container as the technique used will have important repercussions on the counter-measures deployed by governments.

1. Risk management and modelling

Risk management and modelling methodologies are typically used both in government and the private sector to analyse strategic threats and to develop appropriate counter-measures.[1] Risk management can be characterised as "a systematic process to analyse threats, vulnerabilities, and the criticality (or relative importance) of assets to better support key decisions linking efforts with prioritised efforts for results".[2]

Typically a risk management exercise is carried out by a multi-disciplinary team that, in the present analysis of terrorism risk in the container transport chain, would include sociologists/terrorism experts, industry representatives, transportation and logistics experts, physicists and other scientists, physicians and security experts. No single discipline should be dominant to ensure that the analysis incorporates all viewpoints. This team should investigate the issue at hand, possibly through a scenario exercise, by incorporating the following eight elements:

1. Threat Assessment: identifies adverse events that can have an impact on the issue at hand. These events can occur either at the local national or global level.
2. Vulnerability Assessment: identifies weaknesses in infrastructure or other physical structures, processes, personnel policies, or other vulnerabilities that might be exploited by terrorist groups.
3. Criticality Assessment: identifies, assesses and prioritises action strategies based on the relative importance of possible targets and impacted systems.
4. Risk Assessment: either qualitatively or quantitatively seeks to determine the likelihood of an event (*e.g.* terrorist use of a container to deliver a CBRN weapon) occurring. Also seeks to evaluate the severity and impact of the event.
5. Risk Characterisation: seeks to assign risk on a scale (*e.g.* low, medium, high) and serves as a basis for developing effective responses.
6. Risk Mitigation: implementation of counter-measures, taking into account risk, costs and other factors that could have an impact on implementation.
7. Systems Approach: a systems approach in risk management of container security *vis-à-vis* terrorist action should address all areas that have an impact on the issue. This means addressing processes, actors, technology, infrastructure, policy and governance issues *not only in the field of transport* but upstream as well.

8. Monitoring and Evaluation: These are continuous assessment processes undertaken to ensure the relevance of current security measures and strategies. These include external peer review, testing and validation.

All of these elements are essential for a balanced risk assessment exercise. However, many government agencies have not fully undertaken this exercise – and even in countries that have been pro-active in this field, certain key elements have been neglected. The result is that while countries have a fairly good idea of the vulnerabilities of the container transport system and the severity of possible CBRN weapon attacks[3] (the columns in the table below), many have only a notional idea as to the real probability of a container being used for such an attack (the rows in the table below).[4] This information, however, from a whole-of-government policy perspective, is of vital importance – not so much for the implementation of low-cost and un-intrusive security measures – but for the hard decisions that must be made *vis-à-vis* high-impact, costly and trade-unfriendly measures.

Table 3.1. **Risk assessment matrix**

Probability of occurrence	Severity level			
	I Catastrophic	II Critical	III Marginal	IV Negligible
A – Frequent	IA	IIA	IIIA	IVA
B – Probable	IB	IIB	IIIB	IVB
C – Occasional	IC	IIC	IIIC	IVC
D – Remote	ID	IID	IIID	IVD
E – Improbable	IE	IIE	IIIE	IVE

Finally, threats will vary between different national States and world-wide measures will not be appropriate in all cases. Measures for counter-terrorist security need to be proportionate to and take account of the threat, which will vary from place to place and from time to time.[5] Furthermore there are different threats to the various modes and cargoes. Seeking largely common measures in areas where the terrorist threat, and vulnerability, differs markedly would reduce the measures implemented to the lowest common denominator. In this context, the notion of varying "security", "alert" or "threat" levels as used in varying national contexts and by the IMO International Ship and Port Security Code can serve as a helpful framework to better match specific threats and counter-terrorist responses.

2. Factors to be considered in a container security risk management approach

Applying such an analysis to container security is especially important because, at present, many security initiatives view the threat as relatively undifferentiated – terrorist groups and various possible weapons types are all amalgamated into a generalised threat of the CBRN weapon-containing shipping container. The threat is *not* uniform, however, and any analysis based on that assumption will necessarily gloss over some important nuances that could help develop more effective responses. At a minimum, a comprehensive risk management process should investigate the following questions.

2.1. Who are "the terrorists" and how might they use containers?

Despite efforts at the United Nations, there is no single internationally accepted definition of terrorism.[6] This difficulty in defining "terrorism" (and therefore "terrorists") stems from the fact that there is a wide range of sub-state groups that would have recourse to violence to further their ends. However, to believe that all would have recourse to the same methods of violence would be false. Terrorists use violence to attain their ends – and these ends are as diverse as there are "terrorist" groups. While some groups might use CBRN weapons (indeed some as the Aum Shinrikyo and Al Qaeda have actively sought such weapons), others would view such a recourse as extremely counter-productive to their cause. Understanding the motivations of various terrorist groups is therefore a first step in determining their relative threat to the container transport chain.

Linked to the goals of a terrorist group is its potential motivation for using containers in support of its ends. There has not been a single known incident where terrorists have sought to use a container as a delivery vehicle for a weapon of mass destruction nor have there been any publicly revealed evidence that terrorist groups have targeted containers for this use. There is, on the other hand, considerable evidence that terrorists and "rogue" states have used shipping containers in support of their actions. Containers have been used for weapons smuggling, for raising "legitimate" revenue for terrorist groups, for possibly inserting terrorist operatives and for delivering CBRN weapon precursor materials and supplies. In this context, one might legitimately ask whether the container transport system holds more value to certain terrorist groups as a logistical support system rather than as a weapons delivery system. The two are not compatible because if a CBRN weapon were to be detonated using a container, the resulting security counter-measures would likely shut off all possibility for terrorists to use containers in support of their operations.

3. What is the nature of the CBRN threat?

One of the principal motivations for improving container security remains the spectre of using these boxes as a delivery system for a CBRN weapon. Of course, containers could be used to deliver a weapon built around conventional explosives but it is likely that the resulting impact would be limited and not supportive of the terrorists' goal of instilling fear.[7]

CBRN weapons, in contrast to conventional explosive devices, require much greater expertise and their development, construction and deployment is both a complicated and time-consuming process. While much of the focus regarding weapons of mass destruction are on the final weapons themselves, it should be highlighted that in many (but not all) cases, the development of these weapons requires acquiring components and materials not through theft or sabotage, but rather through commercial transactions and oftentimes containerised shipments. One study of the international regime for Multi-lateral export control notes: "A great deal of policy attention has been directed towards addressing this proliferation threat, as well as towards securing nuclear materials from possible theft or sabotage. Nevertheless, policymakers should not overlook a basic fact: most countries and terrorists seek to purchase the components they need for developing weapons of mass destruction"[8] This highlights the need to act not only to discover CBRN weapons in containerised shipments, but to also intercept CBRN weapon precursors.

As illustrated in Figure 3.1 in Box 3.1, there are numerous points where "traditional" non-proliferation techniques can help to thwart the development of CBRN weapons before they get into the container transport chain. Given limited resources to address the threat, a

Box 3.1. **Chemical, Biological, Radiological and Nuclear (CBRN) weapons: factors to be considered for container security**

There are four principal classes of CBRN weapons. A risk management exercise for container security should evaluate each particular type of weapon and assess the probability of its use, the suitability of delivering the weapon via a container and the points where governments can act most effectively to thwart terrorist plans involving CBRN weapons. Some of the issues to be considered in such an exercise are outlined below.

Nuclear weapons: This is the most unlikely weapon to be used by terrorists. The difficulties in acquiring and/or assembling such weapons are numerous and possibly impossible for a terrorist group to overcome. The acquisition of a nuclear weapon by a terrorist group entails overcoming relatively strong access restrictions and asset control protocols while detonating such a weapon requires overcoming robust internal safety mechanisms designed to prevent unauthorised use. Assembly of a nuclear weapon, on the other hand, while complicated, is theoretically more in the reach of certain terrorist groups. Both Aum Shinrikyo and Al Qaeda have made attempts to assemble the components necessary for such a weapon. However, many of the materials necessary to construct a nuclear weapon are not easily available and must be purchased from relatively tightly controlled sources. Traditional anti-proliferation measures can be effective in thwarting terrorists' plans early in the process of assembling such a weapon. Finally, a nuclear weapon would represent a tremendous investment in time, effort and resources for a terrorist group. It is not at all sure that a terrorist group would utilise a shipping container as a delivery platform for this "valuable" asset when other, lower-risk options might be available to them (*e.g.* such as placing the bomb in a commercial delivery vehicle, a pleasure craft or a bulk freighter – all of whom receive less scrutiny than the typical container).

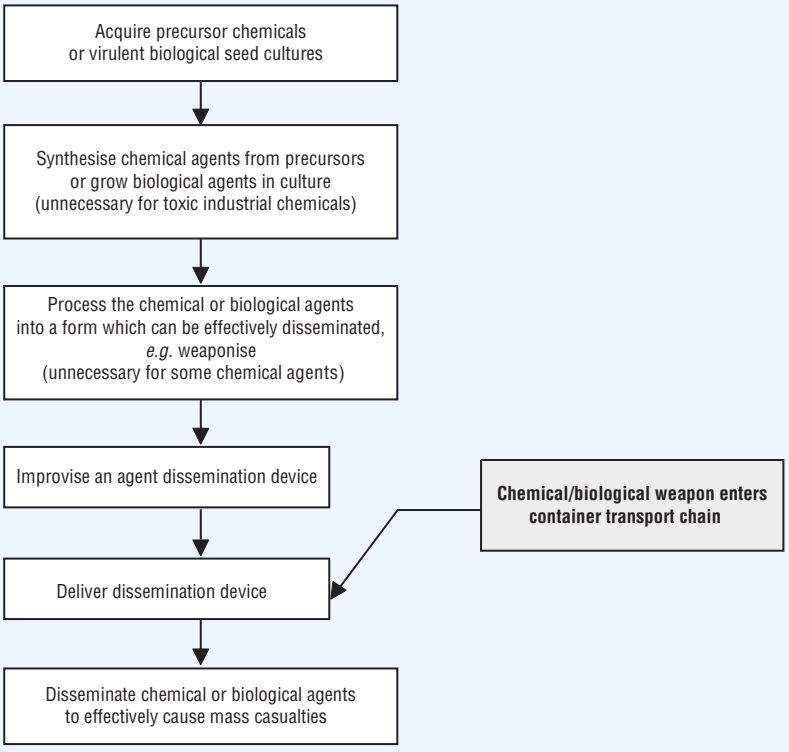
Radiological dispersal weapons: This is a more likely scenario for a terrorist attack using radioactive materials. In this scenario, a strong conventional explosive is combined with non-military radioactive materials (*e.g.*, from medical scanning devices or food irradiation machines). The principal damage would be linked to the dispersion of radioactive dust particles and the secondary effects due to public panic. Such an attack would likely entail very few actual casualties – even in the worst case – but the psychological and economic impacts might be significant. Depending on the nature of the radioactive source (*e.g.* cesium, cobalt, americium, plutonium, etc.), the strength of the conventional explosives and the atmospheric conditions at the time of the explosion, the area impacted and possibly rendered uninhabitable could range up to several square kilometres (which, in a city centre, would entail tremendous costs). Most literature relating to these weapons stresses the need to deploy a network of sensors at "choke-points" in order to detect tell-tale radioactive signals – *e.g.* in transport facilities and ports. Knowing this, a terrorist group may wish to assemble these devices *in situ* from locally available materials thus by-passing the use of a container as a delivery platform.

Chemical and biological (CB) weapons: As with nuclear weapons, the risk from terrorist use of these weapons should be differentiated according to whether the weapons are acquired from state actors or assembled by the terrorist groups themselves. As with nuclear weapons, ready-made CB weapons are generally closely guarded and accounted for – however, some states may have more lax procedures than others. Except for certain crude chemical weapons (*e.g.* those based on common toxic chemicals such as chlorine), most CB weapons require relatively high levels of expertise and sophisticated labs to develop. Even in the Aum Shinrikyo attacks, despite large financial resources, advanced technical expertise and well-equipped laboratories, the cult was only able to assemble a poor quality chemical agent linked to a

Box 3.1. **Chemical, Biological, Radiological and Nuclear (CBRN) weapons: factors to be considered for container security** *(cont.)*

rudimentary dissemination device. Figure 3.1 below traces the typical steps in assembling CB weapons. The figure highlights the fact that there are numerous opportunities to detect such a weapons programme, and act against it, before such a weapon actually makes it into a container. Finally, especially in the case of biological agents, it can be argued that it makes little sense to use a container as a weapons delivery platform when other, "lower risk" (from the terrorists' perspective), and more adapted delivery mechanisms exist (*e.g.*, such as the ventilation system of a high-rise building).

Figure 3.1. **Stages for terrorists working outside a state-run laboratory to conduct chemical and biological terrorism**



fundamental question for States to address is what should be the balance between efforts seeking to prevent the *development* of CBRN weapons and those seeking to *discover and stop* the delivery of these weapons via the container transport chain? Arguably, the chances of discovering a CBRN weapon once it is placed within a container are relatively slim and it may make better sense to invest heavily in preventing the development of the CBRN weapon in the first place.[9] Some countries are already active on this front. For instance, in an effort to take targeted action to prevent nuclear proliferation, the United States Department of Energy's "Second Line of Defence" co-operative programme with the Russian Federation places radiation detectors in Russian ports and helps train Russian Customs officers in order to prevent the smuggling of radioactive material out of the country.[10]

Part of the risk management exercise is to ensure that responses are commensurate to the particular CBRN weapon threat. In the case of a terrorist group that has spent considerable resources developing a CBRN weapon and ensured its secrecy, it may not make sense to use a container as a delivery platform. The risk of discovery is not negligible and it is largely outside of the control of the terrorist group. Furthermore, detonating the CBRN weapon within a container (especially in the case of a biological weapon) may not ensure the greatest impact. In evaluating their options, terrorist groups might decide that another, non-container based, delivery system might be a more effective way to ensure the greatest return on their "investment".

4. Possible techniques used by terrorists

As noted earlier, containers have long been vulnerable to criminals and susceptible to being misused for criminal purposes. Indeed, most of Customs and Transport authorities' experience in the domain of container security stems from their experience in countering narcotics/contraband smuggling and container theft. Based on this body of experience, some insight can be gained into the manner in which a terrorist group might go about diverting containers from their legitimate uses.

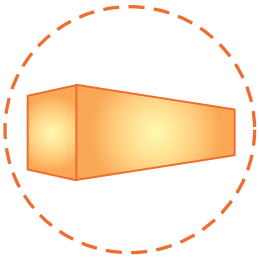
The techniques used by criminals to smuggle drugs and contraband are not necessarily the same as those used to steal the contents of a container. In the first instance, the criminal wishes to ensure that their illegal consignment gets to final consignee unnoticed and untouched whereas in the second, the criminal is interested in removing the contents of the container in such a manner as to avoid, or at least delay, discovery. The techniques used by drug and contraband smugglers are probably more in line with the potential *modus operandi* of the terrorist than are those used to steal the contents of the container – although understanding the manner in which containers can be accessed without leaving visible traces is also of interest to counter-terrorism experts.

The insertion or placement of an illegal consignment within a container can take place in one of two manners (see Figure 3.2). The first is to target a legitimate container, intercept it during its voyage, open it and hide the illegal consignment inside, re-seal the container and re-insert it back into the legitimate trade flow. The "hijacked" container is thus used unknowingly, and at the expense of all the legitimate actors in the container transport chain in order to fulfil the criminal's goals. The second way involves mimicking a legitimate trading environment in order to ship a consignment illegally. The "Trojan horse" method involves setting up (or purchasing) a legitimate trading company and building a good reputation via normal trading patterns before, suddenly, switching to illegal consignments.[11]

The former technique is more opportunistic (although it requires relatively good intelligence regarding the container, its contents and its voyage plans) while the latter requires an extensive investment of time and resources. Both techniques have been used in drug and contraband smuggling, although, arguably, the second has likely met with more success than the former given the extreme difficulty in uncovering its operation. What is important from the perspective of container security is that the most effective responses to each of these techniques are not the same. What works for one will not necessarily work for the other.

It should also be noted that in many cases of container-related crime, internal conspiracies between criminals and "inside" personnel (belonging to warehouse managers, carriers, forwarders and even Customs) have been involved. Criminals often

Figure 3.2. **Terrorist *modus operandi*: hijacked *versus* Trojan horse containers**

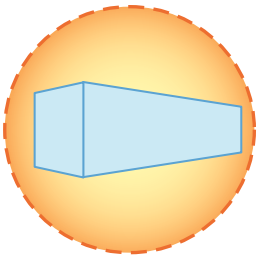


"Hijacked" container

Modus operandi:
Container is intercepted at some point along the logistics chain and opened illicitly. Weapon is inserted and container is closed/re-sealed. Weapon detonates in target area.

Precedent:
Not very common-some use in contraband and drug smuggling. More likely scenario for theft where container tampering/entry is very common.

Risk of discovery:
Possibility of discovery given multiple handlers and numerous visual inspections along the transport chain.



Container from "Trojan horse" shipper

Modus operandi:
Terrorist establishes "legitimate" export business, builds trading record and trust through legitimate operations over a period of time. Implements and receives vetting for on-site security practices.

Precedent:
Fairly common practice to pack container with drug and/or contraband at source, less common for a trader to build a reputation before going bad.

Risk of Discovery:
In the case of a trader with an established "legitimate" trading record, very low.

find that it is perhaps easier and more cost-effective to recruit knowledgeable staff among the various container transport chain actors, than to develop their own skills. While it seems unlikely that a terrorist group could persuade workers and/or oversight staff to knowingly conspire to deliver a CBRN weapon, it is possible to imagine that they may be able to do so by posing as a more "mundane" criminal group bent on earning revenue from illegal activity. Furthermore, a few terrorist organisations have sought to put in place "sleeper cells" consisting of covert operatives whose purpose is to act as inconspicuously as possible – for extended periods of time – until "activated". The persistence of internal conspiracies in containerised crime and the risk of "sleeper cells" highlight the need to closely control the dissemination of sensitive information and oversight duties to trusted and vetted staff.

Notes

1. The United States General Accounting Office (the audit, evaluation and investigative office of the United States Congress) has undertaken extensive work on risk management in relation to threats from terrorism and weapons of mass destruction. This section draws heavily on their work.
2. US GAO, 2003.
3. For example, the US GAO preliminary review of US Customs and Border Protection (CBP) container security measures has highlighted that despite the many positive efforts undertaken by that agency, "CBP has not performed a comprehensive set of threat, criticality, vulnerability and risk assessments that experts said are vital for determining levels of risk for each container and the types of responses necessary to mitigate that risk… [also] CBP has not subjected [its] targeting system to external peer review or testing as recommended by the experts we contacted" (GAO, 2003).

4. For instance, an attack using the smallpox virus might have devastating consequences but it is not at all clear what the probability of such an attack using a container might be – arguably, terrorists have much better adapted and effective dispersal systems for viruses than containers. In this case it also makes better sense to inoculate first-responders and medical personnel than to attempt to inoculate the population at large or subject containers to expensive and cumbersome testing.
5. Measures for counter-crime security, on the other hand, will generally remain constant across states and time.
6. For more on this, see *www.unodc.org/unodc/terrorism_definitions.html*.
7. Two things should be noted here. The first is that the impact of a conventional explosion on a container vessel can be dramatically multiplied by detonating the weapon near other containers containing hazardous compounds. The dramatic result of several container vessel explosions involving explosives and catalysts illustrate this. The second is that certain terrorist groups – Al Qaeda in particular – have as a stated goal to inflict economic damage on their enemies – a co-ordinated bombing campaign using conventional containers could potentially help to realise this goal.
8. Beck Craft, Gahlaut and Jones, 2002.
9. Experience from past drug interdiction efforts are instructive on this point. While many illegal shipments were and still are discovered through effective Customs control, a significant number of illegal consignments did and still do make it through. The chances of a CBRN-containing container getting through Customs control are equally non-negligible. Just as drug interdiction efforts have not focused solely on preventing the delivery of drugs but have moved upstream to prevent the harvesting and production of drugs, so too CBRN weapon interdiction efforts should not focus solely on the delivery of the weapon.
10. The Russian Federation and other ex-Soviet republics have long been a focus of nuclear and radiological non-proliferation programmes due to the large quantities of fissile material left after the break-up of the Soviet Union. US DOE and the Russian Federation also have in place a "First Line of Defense" programme that seeks to secure this material at nuclear facilities.
    In a similar vein, the recent Proliferation Security Initiative (PSI) was launched by 11 countries including Australia, France, Italy, Japan, Germany, Netherlands, Portugal, Poland Spain, UK and US in 2003 as a cooperative initiative to fight against the proliferation of weapons of mass destruction (WMD). A "Statement of Interdiction Principles" identifies practical steps aimed at interdiction of WMD, their means of delivery and related materials. It is intended that this initiative address proliferation of WMD not only by State, but also by non-State entities and terrorist organisations.
11. In such a scenario, the buyer may be a part of the conspiracy or may be an innocent party that has the misfortune to contract with a "Trojan horse" shipper.

ISBN 92-821-0331-5
Container Transport Security Across Modes

Chapter 4

Container Security Measures: Overview and Analysis

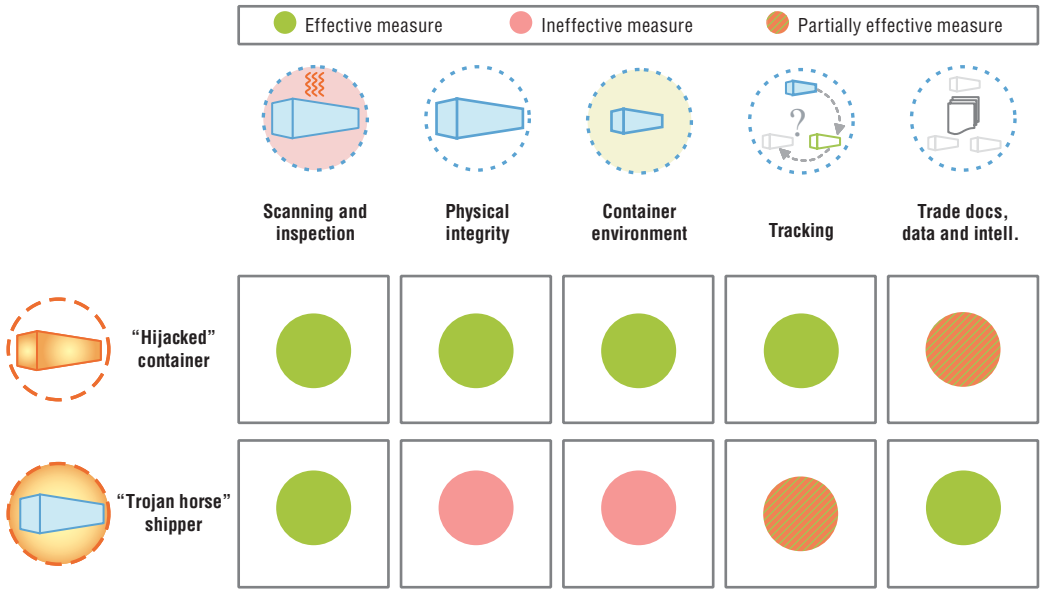
The September 11th attacks on New York and Washington galvanised global action to increase the security of the container transport chain. The United States, understandably, has helped to lead efforts to develop new international instruments (such as those negotiated at the IMO) and has put in place numerous national and bilateral initiatives. However, other international organisations (such as the WCO, ILO and ISO), regional groupings (the EU in particular, but ASEAN and APEC as well) and industry actors have also undertaken new work (or re-oriented existing work) to address container security. A detailed accounting of these measures is provided in Annex B.

Generally, the measures put into place or strengthened following the September 11th attacks fall into one of the following five groups.

- Measures seeking to *scan* or otherwise physically confirm the contents of the container.
- Measures seeking to ensure the *physical integrity* of the container.
- Measures aimed at ensuring the security of the *container environment* as it moves and is handled in the container transport chain.
- Measures seeking to *track and trace* the container in the supply chain.
- Measures centred on the provision, and use of, *information* related to the shipment.

Not all of these measures are equally suited to counter both the "hijacked" and "Trojan horse" threats as described in the previous section. Figure 4.1 below illustrates where these measures are most effective. It highlights the fact that technical measures focusing on the integrity of the container and its environment are not of much use in the "Trojan horse"

Figure 4.1. **Security measures and the hijacked/Trojan horse scenarios**



CONTAINER TRANSPORT SECURITY ACROSS MODES – ISBN 92-821-0331-5 – © ECMT 2005

scenarios, that scanning remains the one of the most effective measures to discover either of the two threats and that intelligence and information-based measures must necessarily be deployed to thwart the "Trojan horse" shipper. Each of these categories of measures is examined in this section. However, the overall context for these measures is illustrated in Figure 4.2 which describes the generalised trend to "push" security upstream in the supply chain.

1. Scanning

The physical inspection of the contents of a container remains the most effective security measure that can be deployed in the container transport chain – it is also one of the most costly and cumbersome measures available to authorities. Although 100% physical inspection would be ideal, this remains an impossible goal given current trade imperatives and technologies. In reality, much lower container scanning and inspection ratios are the norm. Of the more than 7 million containers which came into the United States in 2002 for example, approximately 10% is inspected and scanned by the US Customs and Border Protection,[1] this is up from about 2% prior to September 2001. Roughly 5% of all import containers are subject to an inspection at the Rotterdam Port.[2] In the UK, 4 to 7% of imported containers are checked.[3]

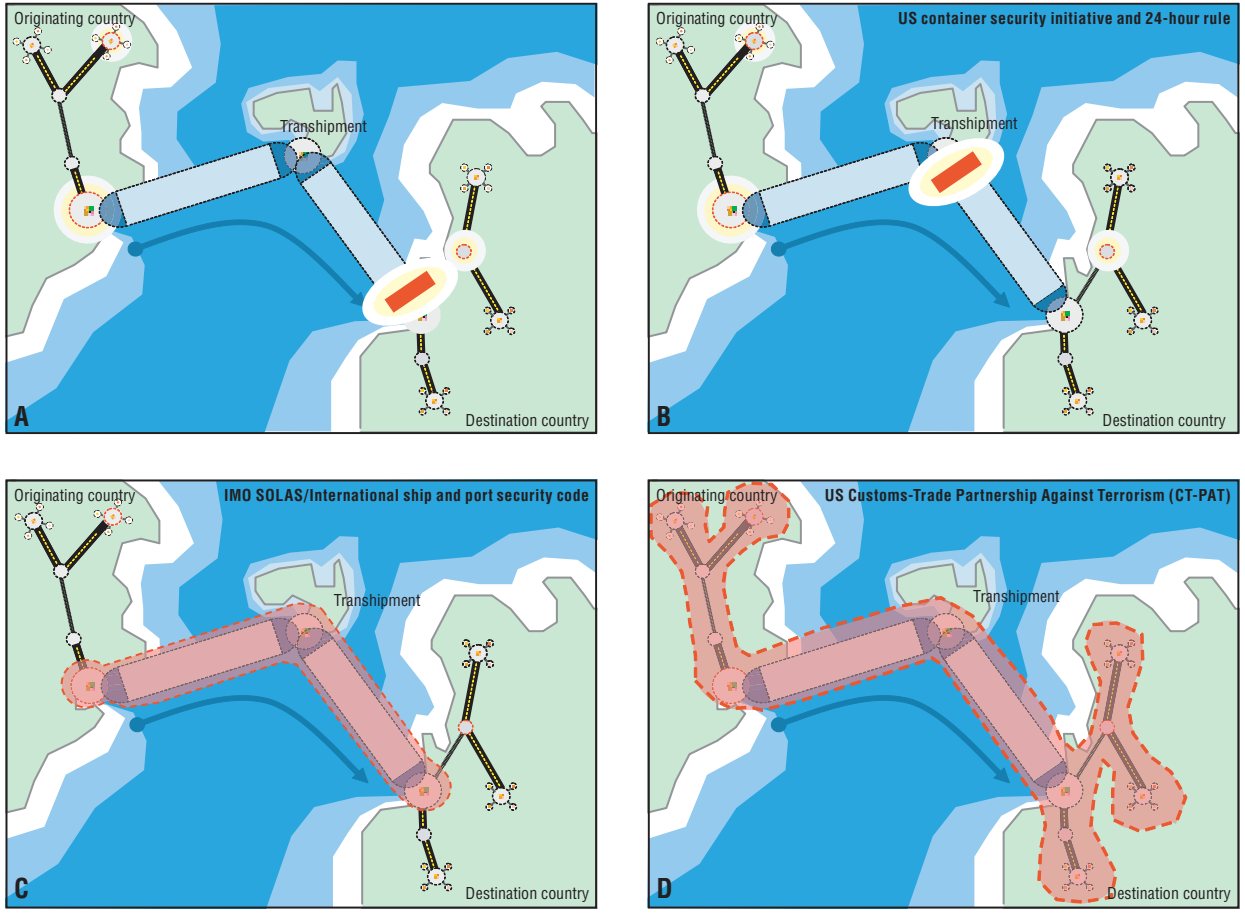
An important distinction must be drawn, therefore, between container screening and container scanning. The former is the act of assessing the security risk posed by a container based on available information (this process is described in Section 5), the latter is the physical act of scanning or manually inspecting the contents of a container. Screening establishes which containers are considered to be high risk and are therefore candidates for scanning and inspection. It should be stressed that low ratios of scanned containers do not preclude 100% screening of containers as is the case in many OECD countries. Although the United States requires information regarding the consignment 24 hours in advance of the planned loading onto container ships destined for the United States, pre-information to assess the risk is not always available for non-US trade. Indeed, in many countries, Customs may screen relatively few containers and scan/inspect even fewer. Even when they do screen containers, they may do so according to non-security criteria – such as tariff compliance.

This 24-hour rule is part of the Container Security Initiative (CSI), which was announced in January 2002. The CSI in effect extends the zone of security for the US upstream to foreign ports of origin (see Figure 4.2). Through CSI high-risk cargo containers are identified and examined for CBRN weapons at foreign ports before they are shipped to the United States. CSI consists of four core elements of the inspection efforts:

- Establish security criteria for identifying high-risk containers based on advance information.
- Pre-screen containers at the earliest possible point.
- Use technology to quickly pre-screen high-risk containers.
- Develop secure and "smart" containers.

Under the CSI program, the screening for WMD in cargo containers is conducted by teams of customs officials deployed to work in co-operation with their host nation counterparts. Reciprocally, participating countries can send their customs officers to major US ports to examine containerised cargo to be exported to their countries.[4]

Figure 4.2. **Evolving container security paradigm**



Evolving border security paradigm

This figure illustrates the evolving border security paradigm as it shifts from traditional border control to comprehensive supply chain security.

A: Customs Control typically intervenes at the border of the importing country. This is the first occasion that most Customs agencies have to assess the risk of an incoming consignment. Some security measures are also in place at various locations within the container transport chain.

B: After the September 11, 2001 attacks on New York and Washington, The United States "pushes" the border back to the last port of loading. Security assessment by US Customs now takes place before containers are loaded onto the last leg of their voyage.

C: In 2002, the International Maritime Organization agrees on a comprehensive package of security measures for ships and ports (ISPS Code). These serve to secure the maritime leg of international transport and came into force on July 1, 2004.

D: The next step, illustrated by the US C-TPAT initiative, seeks to extend security management up the supply chain. Here, land-side (carrier, forwarders, depots, etc.) security practices are bolstered through a comprehensive framework to build on existing industry security best-practice.

There are two ways to physically inspect and verify cargo contents. First, the containers are scanned by Non-Intrusive Inspection (NII) devices such as X-ray scanners, which give a fairly accurate image of the container's contents. When the contents are not sufficiently identified, the container is physically opened and manually reconciled with the bill of lading. The process of opening, unpacking, and inspecting a container takes approximately 8 hours, although the time depends on the individual case. Since the opening can cause significant delays of cargo flows, non-intrusive scanning is used as far as possible to minimise delay.

Non-intrusive inspection consists of various technologies (*e.g.* X-ray, gamma ray) with different capabilities to identify specific materials (*e.g.* drugs, radioactive material, explosives) with different kinds of equipment (*e.g.*, mobile, crane mounted, hand-held). Table 4.1 summarises the non-intrusive inspection technologies and their security functions.

Authorities have a number of options at hand to discover radioactive materials that may form part of a radiological or nuclear weapon. These include, for radiological weapons, backscatter x-rays, high energy x-rays, trace detection, and radiation sensors. To detect a nuclear weapon, radiation detectors would provide an alarm if the nuclear material is unshielded. If the weapon is shielded to reduce radiation, x-rays could also be used to alarm on dense mass.[5]

Research is being done to improve further non-intrusive inspection abilities that could identify chemical, biological, radioactive or nuclear materials. In order to detect and identify these hazardous materials and drugs, more data must be obtained such as mass density and data must be processed with a sophisticated computer program.

The ability of machines, even with the latest technology, is limited and identification of materials relies on the expertise of operators. X-ray machines assess the density of materials and sound an alert but the screeners need to judge and identify the materials by viewing the image and sometimes by physical search. The inspectors need to be well trained to interpret the x-ray images and other indicators produced by machines.

It is not always easy to install these machines because of limited space availability at terminals and costs of machines as well as operators' manpower particularly in developing countries. However, if the scanning is seen as a multi-purpose process, it would help installation. Scanning could be not only to detect CBRN weapons but also to detect drugs or illegal immigrants. When there are white powders in a container, inspectors have to identify whether they are sugars or drugs or plastic explosives in one scanning process. For example, the installation of the Vehicle and Cargo Inspection System (VACIS) by the Malaysian Customs has brought an immediate financial benefit, because the use of the scanning machine has helped enormously deter smuggling activities and as a result, tax collection increased by approximately 30%.[6] If the probability of fraud is reduced in a country, it would earn the international community's trust and attract more trade, which could improve economic prosperity.

Conclusions: container scanning and inspection

- Screening and scanning of containers, while complementary, are not the same. 100% container screening is possible, should an administration choose to do so – 100% scanning, on the other hand, is not.

Table 4.1. **Technology characteristics**

	Descriptions	Indicates potential presence of threat	Provides material discrimination	Time for inspection	Installation	Cost
Active systems						
Acoustic	An ultrasonic transducer is put into the container and a sensor detects the reflection and forms an image	Yes, in liquids	No	2-5 minutes/ object	Portable/ desktop equipment, which can be operated by battery or wall plug power	$$
Gamma ray	The gamma rays interact with the object and are displayed as an image	Yes	No		Mobile, fixed or relocatable sites. Fixed and relocatable sites require local infrastructure of power, road access, personnel facilities and attention to radiation safety	$$$
Pulsed Fast Neutron Analysis (PFNA)	Pulsed neutrons are directed at the object and create gamma rays with energies characteristic of its elemental composition	Yes	Yes	90+ minutes/ object		$$$$$
Thermal Neutron Activation (TNA)	Sophisticated sensors detect the energy of the gamma ray photon emitted when the thermal neutron is absorbed by material within the object	Yes	Yes			$$$
X-ray						
Standard transmission	The transmission of x-rays is directed through the cargo to a detector and presents one "shadowgram" image to that overlays all items in the beam path	Yes	No	2-5 minutes/ object		$$$/$$$$
Dual energy transmission	Two different x-ray energy spectra are used. Generally ineffective for large cargoes	n.a.	Not in high density cargos			n.a.
Dual view transmission	Two views of the object are displayed	Yes	No			$$$$$
Backscatter with transmission	Two or more views are displayed. Backscatter images highlight items in the object that contain low atomic number elements	Yes	Yes			$$$$
Passive systems						
Canine use	Dogs are trained to alert the presence of explosives and other threat objects	Yes	Yes	0.5-1 minute/ object	Requires care, feeding and shelter, together with trained handlers	$
Radiation detection	A detector measures the ionizing radiation or other characteristic radiation emitted from a radioactive substance	Yes	Yes		Portable/ desktop equipment, which can be operated by battery or wall plug power	$
Trace detection/ vapour detection	A "sniffer" type sensor collects and analyses air samples	Yes	Yes			$

Cost key: $ ≤ $50 k; $$ ≤ 100 k; $$$ ≤ $1 M; $$$$ ≤ $5 M; $$$$$ ≥ $10 M.

Source: This table was created based upon the information in COAC Border Security Technical Advisory Group Volume 6 – Report on Non-intrusive Detection Technologies.

- Screening can be improved with additional sensor-based or information-based inputs. Additional data, whether from the container (*i.e.* tamper indication), from the facility infrastructure (*i.e.* radiation detection portals) or from information systems (additional shipment detail), could be used to improve screening/targeting processes.
- Continuous research and development of non-intrusive inspection technologies are needed to detect dangerous materials without interrupting the flow of goods. One technology cannot detect everything. Thus the combination of technologies and attentive human operators is necessary.
- The personnel side of scanning process should also be examined so that the inspectors are well trained to interpret the x-ray images and other indicators.
- In order to promote installation of scanning devices, to note multiple benefits and objectives to have a good scanning system could help. Improving scanning ability could serve not only to detect CBRN weapon but also to reduce smuggling, to raise tax collection and to earn the trade community's trust to attract more trade.

2. Securing container integrity

As noted earlier, the typical container is simply a reinforced steel box designed to be easily stackable transferred among modes and carried by specialised sea-going vessels. It has one point of entry – a double-sided door on one end – that is closed using a multi-point locking bar system. Once the container is stuffed and it leaves the originating shippers' premises, the container is vulnerable to being intercepted and having its contents tampered with. Past experience with container theft indicates that most container tampering involved removing the contents of the container – but the same techniques used for gaining access to containers can equally be used for removing or placing items in containers. In order to prevent this from happening, the Customs Convention on Containers (1972) and the TIR Convention (1975) set out technical specifications on secure containers and sealing. Sealing devices that shippers and/or carriers generally resort to can be either mechanical or electronic and fall into one of the four general categories outlined below. However, it should be stressed that the vast majority of seals only indicate *whether the seal itself has not been tampered with – not that the container's integrity has been compromised.*[7] Furthermore, seals are only useful when referencing a document (manifest, bill of lading, etc.) that provides a "snapshot" of what was in the container when it was sealed. Ideally, seals should only be placed on containers by the party *directly responsible for stuffing and/or visually verifying* the contents of the container. In this respect, it should be stressed that the party responsible for stuffing and sealing the container is the first, and most important, link in a "secure" container transport chain.

Mechanical seals:[8] *indicative seals*

These seals are affixed either on the handle mechanism directly or to the door superstructure. Their primary function is to indicate when unauthorised entry into the container has occurred. Simple indicative mechanical seals such as plastic or metal band/wire seals are made such that any attempt to open the handle and/or door destroys the seal. These seals require visual inspection to determine if they have been tampered with. These seals are extremely easy to defeat by simple means (*e.g.* cutting the seal and replacing it with a similar unit once the container has been accessed).

Mechanical seals: security seals

These seals are similar to the indicative seals in that their primary function is only to indicate whether the seal has been compromised. However, in order to overcome the former's weaknesses, these seals have a unique identification number and are marked by the seal owner's stamp. Even if a tampered seal were to be replaced with a similar unit after entry, the seal's unique identification number might not match that recorded when the original seal was affixed.

The sealing process for security seals is as important if not more important than the seal itself. Proper sealing protocols are comprised of a number of elements including the following:

- Purchasing/sourcing and shipping procedures for seals.
- Training in seal use and verification.
- Correct application of seals.
- Recording seal numbers.
- Managing and transmitting seal numbers.
- Recording seal operations and identification of people involved and time and date.
- Recording seal anomalies.
- End-of-use and end-of-life disposal of seals.

Without these sealing and checking protocols, use of seals can be counter-productive as they can instill a false sense of security as to the status of the container handle/door.

In theory, such a security seals should prove effective in detecting any attempt to tamper with the container. In reality, however, simple security seals are relatively easy to defeat. The reasons are numerous but include the ease with which they can be cut, the possible lack of proper seal documentation, the possibility of poor security management in the container transport chain[9] and the relative ease of replicating certain seals and their numbers.[10] As with simple indicative seals, verifying the seal is both a manual and time-consuming process and thus many seals are only summarily checked, if checked at all, while in transit. Finally, and this is not a problem unique to security seals, experienced thieves have devised ways to bypass the handle or the container doors entirely when gaining entry to the container.

Mechanical seals: high-security seals

High security seals fulfil the same functions of the previous two mechanical seals but also serve to physically prevent, or at least delay, entry into the container. They have recourse to stronger materials and sometimes more strategic locations in order to act as a barrier to entry. The most common forms of high security seals are the bolt seal and the cable seal – the latter being more easy to apply than the former. These seals also have unique identification numbers and require the same type of sealing and in-transit checking protocols as simple security seals. They, too, can be defeated either physically (although they are designed to have much greater shearing/bending tolerances) or by by-passing the seal altogether. High security seals can also be counterfeited. Finally, as with security seals, they rely on visual inspection for discovering any tampering attempts and are subject to possibly being overlooked while in-transit.

Electronic seals

The need to further secure containers containing high value goods from terrorists and thieves has led to the development of several types of "smart" seals. These types of seals have integrated physical security *and* information management capabilities. It is the latter functionality that sets these aside from their mechanical counterparts since they can transmit data regarding their status as well as the information regarding the contents of the container.

At a minimum, an electronic seal system combines a physical sealing device with a data chip capable of recording and restituting basic information regarding the container contents (*e.g.* an electronic cargo manifest) *and* a mechanism for reading the information recorded on the chip. A higher level of functionality is added by systems capable of electronically communicating whether the seal has been broken or otherwise tampered with. These seals use radio frequency (RF), infrared (IR) or fibre optics to transmit data. In their most advanced iterations, electronic seals can be coupled with a variety of sensors (*e.g.* radioactive, radiological, chemical, biological, light, CO_2, etc.) that can record and communicate data regarding the in-container environment. In combination with a global positioning system (GPS) transceiver, alerts or status messages regarding the container can be transmitted in real time to a central processing system that can pinpoint the container's location. As with high security manual seals, electronic seal location (*e.g.* door handle, door superstructure or elsewhere) is important.

Electronic seals can be either passive or active. A passive seal has no autonomous power source, is relatively inexpensive and is disposable. Its power comes from the reader or scanner thus limiting its use to short-range applications. The lack of on-board power means that these seals can only provide data on their current state at the time of reading (*e.g.* tampered or non-tampered) but cannot record the time of the tamper event.[11] When combined with a high security mechanical component, these seals can be seen to provide at least equivalent protection as a high security mechanical seal with the added benefit of better counterfeit and/or tamper protection (*e.g.* through encrypted identification numbers). The ability to restitute container manifest data on demand can also contribute to non-port screening applications, especially by transport operators that may not have access to detailed manifest information (*e.g.* local drayage firms). This feature is also a vulnerability since unauthorised access to the manifest data would enable criminals, and possibly terrorists, to target high-value and/or high-interest consignments.

Active seals have much greater functionality because they incorporate an autonomous power source enabling them to continually record events and transmit their data over greater distances. These seals have varying data storage capabilities – they can be factory or "first-user" programmable, be writable and/or be re-writable. In the first case, the seal is programmed at its first point of use and can be queried along the transport chain as to its status. The only difference with a passive seal in this case is the distance over which the data can be accessed. In the second case, the seal continually monitors its own status (as well as the status of any connected sensors) and can restitute detailed information regarding this continuous record when queried (or, alternatively, with appropriate transponders, it can broadcast an alert regarding its status). In the third instance, the seal's "write" capability allows authorised users to add to the information already held in its memory.[12] Finally, active seals can be designed either for single or repeated usage.

E-seals, especially when they are combined with the mechanical features of the high security seal as outlined in ISO PAS 17712 are an appealing solution from a number of points of view. They allow some form of instant polling that allows instant access to data regarding the seal's status and the container inventory and/or shipping documentation. In their different iterations, they allow progressively more comprehensive security monitoring of the seal and the container environment and allow for remote alerts. Finally, because the seal data is electronic, they can contribute to tighter integration with, and between, different users' information systems. However, there remain important caveats that must be borne in mind.

What do e-seals monitor?

The first is that the e-seals only monitor the seal's status and that of any sensors connected to the seal – they do not monitor the condition inside the container. This nuance is important. As pointed out earlier, a container's integrity can be compromised without compromising the integrity of the seal. Even when sensors are attached, the seal records sensor events which may or may not reflect what is actually happening within the container environment. "False-positive" readings from sensors are a particular concern but one should not overlook the possibility that sensors can be defeated by more or less sophisticated means.

What shipping-related information do e-seals provide?

E-seals cannot provide detailed information on the contents of a container. What they do provide is information regarding what the party responsible for sealing the container *said* was in the container. If that party was an originating shipper, one might assume that the information is more or less correct. However, if that party is once or twice removed from the originating shipper (*e.g.* in the case of a carrier placing an e-seal on a container that arrived at the terminal with a non-conforming mechanical seal), then the shipping documents loaded into the seal's memory only reflect the e-seal-affixing party's best available information as to the contents of the container. In a worst case scenario, a conforming e-seal on a container containing illegitimate cargo might actually facilitate the transport of that cargo, rather than prevent it. Non-declaration or mis-declaration of goods is not an unknown phenomenon in international transport and the catastrophic outcomes of certain incidents (*e.g.* mislabelled calcium hypochlorite or fireworks-containing containers) highlights both the reality and the risk of such situations. Any sense of security instilled by the presence of an e-seal on an intentionally mis-manifested container containing a CBRN weapon would have dramatic consequences.

E-seal infrastructure

For e-seals to be an effective part of a global container security strategy, they must be accompanied by a host of reading devices/scanners, computer hardware and a suite of underlying information management software systems capable of properly processing the seal data. These requirements are far from being met today, and their fulfilment throughout the container transport chain is not at all assured in the near future. It is likely that major terminal operators will be the first to place e-seal readers at strategic locations within their container terminals and to use such systems to monitor and track the status of such seals. Some of the major maritime carriers might start to deploy e-seal readers as well. However, it is not at all sure that smaller ports will be able to deploy *and* effectively manage such systems in the medium term.[13] Furthermore, while it is feasible that major

railroads and barge operators might also be able to deploy the underlying infrastructure and hardware necessary to support e-seals, it is highly unlikely that small road carriers and smaller barge/rail operators will be in a position to do so any time soon – if ever. What is likely to emerge is uneven support for e-seals across the container transport chain with certain "high security" nodes capable of processing e-seal data punctuated by areas of low or no e-seal functionality. Properly identifying the boundaries of these zones and developing appropriate container transfer protocols among these zones are necessary components of a comprehensive container security plan.

E-seal standards

For e-seals to be effective in helping to secure international trade, they must be useable throughout the global container transport system. This means that any e-seal affixed to a container must be readable in any transport node equipped with e-seal readers, and, conversely, reading/scanning equipment in any transport node worldwide should be capable of reading any e-seal passing through. This is not the case today as many competing vendors have proposed numerous and sometimes incompatible systems. These incompatibilities fall into two principal categories: proprietary readers/scanners capable of reading only one vendor's seals and incompatible data transmission methods.

Both of these barriers can be seen partly as the result of a vendor-led process where various manufacturers have tried to promote their technology solution to the detriment of others. This can be somewhat understood given the urgent responses to the perceived need to roll out e-seals to protect the container transport chain from terrorist attacks. In this context, it was easiest to propose off-the-shelf systems that have had some real world applications. However, many administrations and the trading community in general now agree that broadly accepted standards are necessary if e-seals are going to be effectively deployed throughout the supply chain. At a minimum, these standards should separate proprietary hardware solutions from information transmission protocols and codes. The latter should not be wedded to the former so that users can choose from a wide range of readers that all interpret the same code or "e-seal language". A recent evaluation of several solutions currently available on the market highlighted that this was not yet the case.[14]

The issue of data transmission protocols is an important one because it has a direct impact on cost.[15] As noted earlier, there are several possible data transmission methods. While there are some proponents of "touch" seals where a person must physically contact the reader wand to the seal, most manufacturers have opted for seal systems based on the remote transmission of data. One technology in particular has emerged to the forefront because of its relative low-cost and extensive real-world experience: the Radio Frequency Identification tag (RFID). These tags broadcast seal information over narrow bands of the radio spectrum over short-to-medium distances and do not require direct line of sight access. However, there are some issues concerning their use in radio-wave dense environments and there is a pressing need to agree on a common internationally allocated operational radio frequency for these devices.

Radio frequencies are allocated on a regional basis by the International Telecommunications Union – Radiocommunication (ITU-R) and sub-allocated by different countries according to their needs. However, the ITU-R has not designated a specific band for container e-seal use and thus a number of public use and industrial, scientific and medical (ISM) bands are available for use. This has led to a number of possible RFID operating frequencies. While one frequency is available worldwide (2.44 GHz), regional differences in

its allocation make it not currently suitable for uniform e-seal performance.[16] For one tag to operate internationally under the current regime, it would have to be able to identify and switch frequencies automatically – thus increasing its costs of production.

Work is currently underway at the International Standards Organization (ISO) to address these issues and to develop standardised seal functionalities and seal transmission protocols. ISO works through technical committees that develop draft standards that are then put to a vote before becoming full ISO standards. Two ISO technical committees (104 and 122) are developing a suite of standards relating to the supply chain applications of RFID and, in particular, have developed a working draft standard for the use of RFID in conjunction with freight containers (ISO/WD 17363). This working draft defines the broad characteristics that RFID-enabled e-seals should share so that systems adhering to this standard would be completely interoperable. In parallel, ISO technical committee 104 is also developing a draft standard outlining common platform- and frequency-independent communication protocols for RFID-enabled e-seals (ISO/DIS 18185). However, to-date, there is no consensus on a common dedicated RFID e-seal radio frequency and/or associated technical specifications relating to power levels and duty cycles. This means that any near-term deployment of seals and/or readers must account for multiple operating frequencies – or have their effectiveness compromised.

"Smart" and safe containers

Current efforts to ensure the integrity of containers have focused on the sealing mechanism used to secure the container entry points. It is possible, however, to imagine that future container security efforts might go beyond the sealing and door mechanisms and extend to the very conception and construction of the container. It is already possible to equip containers with multiple sensors that track the environmental conditions within the container. These may measure temperature, humidity, light, motion, and any number of either radioactive or chemical compounds. These sensors need not be directly integrated with a door-sealing device and can be purpose-built within the container itself. Physical barriers to entry can also be deployed for the whole of the container and not just the door. These would include break-wire grids and "smart" membranes that detect any forcible entry the container as well as reinforced container construction. However, all of these technologies and/or enhanced design standards introduce new costs and added weight. Given that two of the most attractive features of containers are their relative low cost to cargo-value ratio and their low weight to cargo-weight ratio, it is uncertain that users would embrace any new technology that would significantly increase either the price of containers or their weight.[17]

At present the "smart" container solutions envisaged by the US C-TPAT, OSC and CSI initiatives limit themselves to a more "classic" mix of high-security mechanical seals combined with sensing and tracking technology.

Tracking container repairs

Unauthorised access to a container often leaves tell-tale signs. These can include re-painted bolts and/or visible welding/repainting of the container walls/roof/floor. For this reason, it would be helpful if the repair history of the container be readily available to authorised parties along the container transport chain. This is not the case at present with container-owning maritime carriers having a relatively high awareness and access to their containers' repair history and other parties in the chain having low to no awareness of the containers' repair record – especially when they are handling leased containers. Including

this data in the current container transport chain is not easy given that much of it is decentralised and inaccessible to different container carriers and/or handlers. However, it would be relatively easy to include such data in an e-seal based container-handling protocol.

Conclusions: container integrity

- Ensuring container integrity is fundamental to ensuring container security. However, past experience with anti-theft devices and container door/handle seals have revealed the inadequacy of these devices to fully protect containers from and/or reveal unauthorised access by determined criminals. Clearly, better seals must be deployed if the container is to be targeted by terrorists. However, it would be incorrect to believe that a technological fix in the form of an advanced mechanical or electronic seal *alone* would be sufficient to ensure that containers are not tampered with during their voyages. Any container seal is only as good as the container stuffing and sealing *process* in which it is involved. This process must include controlled stuffing procedures by the shipper, seal identification and management throughout the seal's lifespan (and not just during the container voyage), verified and secure links to between seals and shipping documents detailing the contents of the container, proper and documented seal disposal procedures and tracking repairs to the container associated with the seal. The primacy of the process over any single technology should be highlighted because while there are efforts underway to standardise sealing technologies – only recently have efforts been undertaken by the WCO and the UN-ECE to provide standardised guidance on secure container stuffing and seal-management processes. At a minimum, one should expect that in the short-term, high-security mechanical seals conforming to ISO PAS 17712 should become the norm in international trading.
- The comprehensive overview of container seal technologies undertaken by the US Cargo Handling Co-operative Programme has demonstrated that e-seal technology is both mature and ready for deployment. These technologies, however, *are not* currently ready for commercial deployment for international use throughout the global container handling network – primarily because of the multiplicity of competing and incompatible operating standards.[18] Current work at ISO aiming to resolve these conflicts has been relatively slow and has suffered from lack of input from the government and industry user community. These conflicts will no doubt be overcome and the container-using community will most likely gravitate to the use of e-seals once broad international standards are in place. Until that happens, however, it makes little sense to mandate the use of e-seals as such a move would almost necessarily favour one seal manufacturer to the detriment of a broad seal standard.
- Furthermore, a distinction should be made between that data recorded and managed by an e-seal system that has particular *security* relevance (*e.g.* seal status and container number) and that data that could potentially be recorded and managed by e-seal systems that have more utility from a *supply chain management* perspective. If e-seal usage is mandated, only use of the former should be made mandatory.
- Real questions remain as to the appropriateness of seeking to design and deploy hardened "safe" containers given the current state of knowledge of the perceived threat from terrorists to the container transport chain. Such an evolution would require a more detailed balancing of the costs and benefits of this strategy compared to other interventions both within and outside the container transport chain. It may make little sense to increase the weight and costs of containers when other, less onerous policy interventions are available to governments.

- Finally, while there are many possibilities to render containers more "smart", these are not all appropriate for a single device and/or use. It may make sense to separate out these functionalities into several tiers. For example, a three-tier system might include: 1) a permanently affixed passive RFID *container tag* could record container number and owner; 2) a semi-passive read-only single use *e-seal* affixed by the party stuffing the container to track the latter's integrity through one door-to-door voyage; and 3) an active read/write *cargo identification tag* that would provide supply chain-oriented data on the particular contents of the container.[19]

3. Securing the container environment

Once the container is stuffed, it is important to ensure the security of the container and minimise the risk of tampering while the container is in transit. This is equally true while the container is moving and while it is stationary – although, generally, the risk to containers is significantly less while they are in movement.

The risk of security breaches naturally increases as the more nodes are added to the container transport chain. As described in Annex A, the sealed container is transported throughout the container chain by various means of transport such as ocean and river going vessels, trains and trucks. The container is handled by mechanical devices such as cranes and forklift trucks at interchange points of these transport modes, where the container can be stored and left unattended for long periods. On the inland side, vulnerabilities in the container environment are highest in unsecured rail yards, road stops, possibly at border crossings (in unsecured parking areas), shipping/loading interchange terminal facilities rather than while the container is in transit onboard ships, lorries and trains.

Border crossings, as described in Annex A, are the points at which container trucks interface with customs verification procedures upon leaving one country and entering another. Customs officials control vehicle, consignment and personnel documentation, sometimes requesting that trucks be unloaded so that the cargo can be inspected.

A recent study conducted among ECMT member countries[20] has shown that there is great disparity in the rigour and overall quality of border crossing control from country to country. The Single Market of the European Union has largely done away with delays and difficulties at border stations of EU member countries. However problems involving infrastructure, personnel and procedures persist along countries bordering the EU to the East, for example. Areas of concern include:

- Lack of or insufficient computer equipment necessary to properly process customs and other documentation.
- Inadequate x-ray verification capacity.
- Poor co-ordination among authorities responsible for the border verifications.
- Lack of respect for the TIR procedures (see Annex B).
- Insufficient number of customs personnel, who are also sometimes inadequately qualified or trained in customs rules, procedures and documents.
- Unethical corrupt behaviour of some customs officials.

There are security issues associated with these problems, notably in terms of the possibilities of container tampering during the delays, and inadequate controls when container trucks and/or trains pass through these border checking points.

Beyond the border crossing, there is a need to extend stronger security measures to the various sites in the container transport chain where containers are stuffed, handled, and/or stored. A number of technologies are available or under development to enhance physical security: for example, smart cards as access control cards, biometric authentication, intrusion detection and alarm systems, close circuit TV system (CCTV).[21] Various sites are already using such access control methods to track identities of truckers and cargo handlers. However, such security devices have not yet been installed in every critical facility principally because of the considerable installation and operation costs involved. These costs are daunting, especially when one considers the large number of SMEs in the container transport chain and their tight operating margins. In the case of land transport (rail and road), it is simply not practical to make all the facilities in the container transport network closed and secured. But the general level of security practice can be raised throughout the concerned transport operators and facility managers.

The ECMT and the International Road Transport Union (IRU) have issued a booklet, Truck Parking Areas in Europe, last updated in 2003, which provides, for each European country, the list of truck parking areas with the ratings of security levels as well as security feature available on site such as 24-hour guards, fences, and video systems.

Since the attacks of September 2001, some US trucking operators have re-evaluated their overall security procedures for pick-up and delivery, for their service locations, terminals and loading-dock facilities, for dispatch operations to vehicles in cities and on the road. Examples of actions taken include: initiating new background checks through systems available to motor carriers; emphasising to all trucking company employees to stay alert and remain aware of their surroundings at all times, especially when transporting hazardous materials;[22] advising drivers transporting hazardous materials avoid highly populated areas when possible; and advising drivers to notify supervisors and law enforcement personnel of any suspicious activity.[23]

For the US railway industry, photo ID or proximity cards are used at major office buildings and other critical facilities. Contract security, mechanical keypads, and swipe or RF cards are used in major facilities handling intermodal or finished automobile shipments. A railroad keeps a database of approved drayage drivers. Video surveillance is used around intermodal and automotive facilities, buildings, and some strategic assets such as bridges. Railroad police use mobile video recording devices for surveillance. Intrusion detection systems are also deployed in intermodal facilities and automotive loading/unload facilities, some signal bungalows and microwave transmitter sites. Some railroad police forces are being equipped with thermal imaging devices to identify the presence of trespassers. The US railway industry, in collaboration with the Association of American Railroads and other organisations, has developed a Terrorism Risk Analysis and Security Management Plan. Components of the confidential document identify risks associated with the transportation of hazardous materials and specific countermeasures that are commensurate with the railway's threat level.[24]

The IMO security package, the amendments of SOLAS and ISPS Code adopted in December 2002 mandate a number of measures seeking to improve the security of ocean-going vessels and the ports they call on. These include the development of ship security plans for all ships engaged in international trips; the designation of a ship security officer (responsible for crew training, implementation of the ship security plan and co-ordination with port security officers); the designation of a company security officer in

shipping companies (responsible for preparing ship security plans and designating security personnel); the designation of a port security officer; the preparation of port security plans as well as the carrying out of port vulnerability; and mandatory security training for port workers.

The International Labour Organization (ILO) and IMO have now drafted a Code of Practice on Security in Ports, which extends the consideration of port security beyond the area of immediate ship-port interface which is the focus of the IMO rules into the whole of the port including areas beyond marine terminals (*e.g.* warehouses, logistics facilities, etc.). These are intended to be compatible with, and complementary to, the IMO package. The draft code addresses port security policy, assessment and plans as well as physical security, security awareness and training. These call for the establishment by national authorities of national and local port security committees to foster co-operation in the security area. On the land side, the United Nations Economic Commission for Europe (UN-ECE) is currently working on a security approach for the whole supply chain including drafting of the International Shippers and Freight Forwarders Security Code.[25] The WCO is also working on guidelines for container stuffing and seal management protocols. However, at present, there are no established international standards or mandatory rules for land-side container security management (except in the case of rules regarding the transport of hazardous goods in containers).

Measures for securing container environment are taken also under government-business co-operation framework. Under the Customs-Trade Partnership Against Terrorism (C-TPAT), a US joint government-business initiative, Customs and the C-TPAT participant jointly reviews the participant's C-TPAT security profile in its validation process to ensure that security actions in the profile are being effectively executed. The security profile includes procedural security, physical security, access controls, personnel security and consignment security.[26] The Business Anti-Smuggling Coalition (BASC), a voluntary co-operation program between the private sector, governments, and international organisations, promotes the strengthening of supply chain security standards and procedures. The BASC standards contain a variety of measures to secure the supply chain from illegal activities such as personnel selection, prevention of internal conspiracies, lock and key controls, ID systems as well as security procedures on reception and delivery of containers. The companies that form BASC are periodically audited and assured that their products and services are produced and delivered under strict security controls and monitored at every step of the transportation process.[27]

The WCO has also included government-business cooperation as part of its plan to secure the container transport chain. Following the adoption of the "Resolution on Security and Facilitation of the International Trade Supply Chain" in June 2002, a Task Force composed of Customs experts working in close collaboration with other international stakeholders in international trade, began to develop common solutions designed to ensure targeted controls and facilitate the movement of licit goods. The Task Force has developed high-level guidelines for Customs Cooperation with business and is now developing sectoral guidelines to further formalise and define the terms of this collaboration. The WCO guidelines build on C-TPAT, BASC and other existing national agreements to develop common international standards.

Conclusions: container environment

- Vulnerabilities in the container environment are highest in rail yard, road stops and parking, shipping/loading facilities (including shippers' stuffing locations) and at all interchange points where the containers can be stored and left unattended for considerably long periods. Dwelling time at terminals should be reduced by rationalising and optimising the process of container handling for both economic and security reasons.
- Such intermodal facilities should be physically secured to minimise the risks of unauthorised access. Physical security includes clear segregation of restricted areas, perimeter fencing, properly locked doors gates, and windows, lighting, signals and warnings, security guards on site, etc. All transport chain actors should be able to check worker identification and be made aware of high-risk workers in accordance with national laws. The restricted areas should be approached only through access control by positive identification of employees and visitors and should be under constant surveillance.
- Personnel security is another element to secure container environment. The reliability and qualification of personnel in the transport chain are essential elements for ensuring its security. First, terrorism or other criminal activities by internal employees should be prevented by screening and interviewing prospective employees, checking employees' background periodically, and verifying provided data. Any organisation should prevent their employees bribed or bought out by terrorist and criminal organisations perhaps by providing an incentive programme to encourage internal reporting of suspicious activities. Secondly, all the personnel should be educated to have security awareness and trained with regard to security policies and practices in their functions so that they can certainly implement procedures on cargo receiving, storage and monitoring.
- It is desirable that common and robust guidelines, common training programmes and standard operating procedures for securing intermodal nodes be established and agreed internationally to improve trust among actors throughout the supply chain.

4. Container tracking

It seems evident that if authorities are concerned by the potential misuse of containers by terrorists, then they should have the ability to track containers throughout the transport chain. This is not only important so that containers identified as risky can be found and inspected, but also so that containers that have gone missing (*e.g.* in the case of a "hijacked" container) can be identified and possibly found.

There are two broad ways in which containers can be tracked. The first involves recording the passage of containers through "chokepoints" in the container transport chain and managing the location data via database systems. The second involves utilising a transponder or satellite-based system to deliver real-time data on the location of the container. Both of these approaches are discussed below.

Most containers are tracked in the supply chain using some iteration of a "choke point" checking system. The checks can be accomplished manually (*e.g.* by a driver orally or otherwise confirming the loading of a particular container onto a truck) semi-automatically (*e.g.* through some form of barcode scanning) or automatically (as envisaged in several active e-seal solutions). The data generated by these checks is tracked and can be restituted with more or less ease (and more or less quickly) depending on the particular information management system in place. As noted in Chapter 2 and Annex A, current container tracking processes tend to operate in isolation of one another and use

various different support systems (vocal commands, paper-based systems, computer databases, etc.) that may or may not be compatible with each other. Container tracking within each individual system, however, can be highly effective. For instance, maritime carriers and terminal managers typically operate highly effective gate, container yard and vessel loading "chokepoint" tracking systems that allow them to have a precise knowledge of where containers under their responsibility can be found. However, even "low-tech" solutions can be effective. Many small road operators using no more than paper and cell-phone based systems can track their consignments both quickly and effectively.

The second strategy involves some form of continuous and "real-time" tracking. The main determining factor in deciding which technology option to use relates to the desired geographic scope for the tracking. In the case of relatively small areas (such as in a container terminal), real-time tracking can be accomplished via a combination of RFID tags and readers. However, real-time tracking throughout the supply chain necessarily requires some form of satellite positioning system and a related transponder. Already, several commercial solutions are available based on this principle but these are considerably more expensive than existing tracking systems.

Currently, satellite tracking is accomplished through the civilian use of the US military Global Positioning System (GPS). GPS satellites emit a weak signal that ground receivers triangulate and synchronise according to a satellite timing signal in order to pinpoint the receiving station's location. These receivers are small and are becoming fairly common for civilian use. Each unit, however, can cost upwards of one to several hundred euros depending on its functions. While GPS is currently a widespread technology, several issues remain that should be addressed before its deployment for critical use applications – such as container tracking.[28]

The first is that the civilian-use GPS signal is a degraded version of the military GPS signal. GPS systems typically integrate a software work-around to compensate for this and this is not so much an issue for operational GPS use anymore. The second is that GPS systems operate on extremely weak signals. During the cold war, the Soviet Union developed GPS-jamming and GPS emulation techniques that are now widely available in relatively inexpensive handheld devices. Depending on their power levels, they can jam or generate false GPS readings over considerable ranges (*e.g.* a simple handheld 4-volt GPS jammer can be effective over 100 km radius at sea).[29] As this technology and its use are widespread, it is conceivable that a terrorist organisation could use an emulated GPS signal to hide its actions and deliver a GPS-tracked container to a location without raising any external alarms. Finally, GPS use in complex urban environments and in tunnels is compromised by reflected, scattered and/or unavailable satellite signals. Several strategies are available to overcome these limitations (for instance combining a GPS receiver with an inertial motion tracking device) but most of these add to the systems cost.

However, this situation is changing, as Europe is developing its own satellite positioning system – GALILEO – which is expected to be available in 2008.[30] GALILEO considerably improves the capabilities of satellite positioning and tracking through the use of 10 signals tailored to specific user needs. The first of these services, the open access service, will freely offer metric accuracy (1 m-10 m). An improved version of this service, the commercial service, will provide guaranteed sub-metric (< 1 m) accuracy. A third service – the Safety-of-Life service – is specifically adapted to applications where human lives could be at risk (aviation, maritime, etc.) and therefore broadcasts an "integrity"

message, informing about the quality of the service received. Finally, governmental authorities are provided with the encrypted Public Regulated Service, which is broadcast on separate frequencies, adding to its robustness.

Simultaneous use of systems like GALILEO, GPS or the Russian GLONASS (forming altogether "GNSS", the Global Navigation Satellite System), will improve signal reception and accuracy in all situations, including cities (and potentially even inside buildings), allowing for efficient container tracking solutions. The agreement reached between Europe and the United States on satellite navigation foresees a very high level of compatibility and interoperability between GALILEO and GPS.

Finally, if GNSS tracking systems are to be used in order to track containers in relation to a set route (and presumably raise an alarm if the container signal deviates from the route), two issues must be considered. The first is the number of "false positive" route exception alerts that may be generated. These, if numerous, can reduce the effectiveness of the tracking system. The second is that tracking containers to a set route requires an underlying Geographic Information System in which the road, rail and/or waterway network is digitalised. While access to this data, even at very fine scales, is not a problem for most OECD countries, this is not necessarily the case for some parts of the world where such tracking would be more difficult.

Conclusions: container tracking

- While in the long-run, developing some form of global multimodal "chokepoint" container tracking system may be desirable, it is probably more effective at present to help carriers to optimise their own tracking systems and to ensure that appropriate government agencies have access to this data as needed. In this context, the notion of creating joint carrier-industry and government cargo tracking centres such as those pioneered by the US Transportation Security Administration should be examined.
- One of the key questions related to container tracking is the issue of timing. Does the container tracking system in use provide sufficiently current and useful data so that threats can be acted upon? The focus of container tracking should not necessarily be *real-time* data but "*right-time*" data. In some instances, real-time data may be appropriate and useful (as in the case of hazardous substances and/or in regions known to harbour terrorist operatives), but in many others, existing choke-point tracking systems might be perfectly adapted to tracking containers. It may be sufficient to know, for instance, that a container was late arriving at a checkpoint and know who the last carrier was and how they may be contacted.
- Finally, countries should fully assess whether real-time tracking systems based on GNSS technology are sufficiently robust at this stage for security-sensitive operations such as container tracking. At a minimum, these should not be deployed without the back-up of a more "traditional" chokepoint control tracking system. Furthermore, given the cost of GNSS-enabled transponder devices, it is not at all clear that their use should be mandated for all containerised consignments. Again, appropriate risk management exercises might better target these systems for specific uses.

5. Trade documentation and information

While measures seeking to track, ensure the integrity of, and control access to containers can be effective strategies to reduce the risk from "hijacked" or otherwise

tampered containers, they are nearly useless in a "Trojan horse" scenario. If either the originating shipper, the party responsible for stuffing and/or sealing the container and/or the load consolidator are controlled by a terrorist group, all that the aforementioned measures will be to provide a false sense of security surrounding a dangerous but outwardly "legitimate" consignment. In this instance, the only truly effective measure remains the scanning and/or physical inspection of the suspicious container. Some have called, therefore, for scanning all containers entering a country. As noted earlier, given the current state of scanning technology, space constraints in port areas, the lack of trained inspectors and the imperatives of global trade facilitation, 100% scanning is not a realistic option. However, even if some of these barriers were overcome, it would make little sense to seek to scan all incoming containers since *not all containers pose the same risk*. Indeed, much of containerised trade is repetitive, involves large and well-known traders operating in predictable patterns and can be screened relatively easily by customs authorities. Correctly identifying these containers, therefore, remains one of the principal tasks of Customs since the remaining containers may pose a security risk and require greater scrutiny, scanning and/or physical inspection.[31]

Most Customs agencies apply some form of risk management-based evaluation to incoming consignments. Depending on the country and the context, the targeted non-compliant behaviour might be tax- and/or duty-evasion, contraband or narcotics smuggling, endangered species or counterfeit goods trade and/or terrorist-related activity. What remains constant, whatever the non-compliant activity targeted, is the need for Customs to receive and process information regarding the consignment.[32] The type of information typically used by Customs was outlined in Chapter 2 and Annex A but is generally limited to data available on the Bill-of-Lading/manifest or equivalent shipping documentation. This information is either manually checked by a Customs officer and/or evaluated by some form of automatic targeting system. Even in the latter case, a custom's officer is typically involved in making a final determination as to the security status of the container.

The actual determination of risk associated with a containerised consignment relies equally on external intelligence available to Customs and the ability of Customs to uncover tell-tale anomalies with a particular consignment. The former is necessary so that Customs authorities can be apprised of terrorist operatives, front companies, zones of activity and specific threats. This information is gathered by the intelligence community and should, ideally, be made available to Customs authorities in both exporting and importing countries so that they can use this to better target containers for inspection. In this context information from Transport authorities relating to suspicious and/or blacklisted companies and personnel, if available, should also be made available to Customs. In the second case – that is, the ability of Customs to identify trading anomalies – experience plays a paramount role. Either through automated means (such as automated targeting systems) or through direct involvement of Customs officers, Customs authorities should have enough data available to them to determine if a particular consignment fits a logical pattern or not. In the latter case, tell-tale signs might include unusual transport arrangements for the goods concerned, non-standard routing, mis-matches between the stated contents and typical weights, and/or factual errors on the submitted documents. Such anomalies can prove essential in discovering non-compliant and possibly dangerous containers – and in the case of a "Trojan horse" scenario, might be the only sign of anything wrong.

In seeking to identify trading anomalies, Customs should also seek to avail themselves of the experience of the trading community – including carriers. These actors have considerable experience in identifying anomalous trades and are more numerous than Customs officials.

There are three central issues related to the effective implementation of risk management techniques by Customs authorities in relation to efforts seeking to address risk from terrorist groups. These are directly linked to the very nature of CBRN weapons. As seen in Chapter 3, if the threat of terrorist use of containers to deliver CBRN weapons to a target country were to materialise, exercising Customs control once a CBRN weapon-bearing container has already reached the country in question would be too late. In fact, one might say that once a CBRN weapon-containing container has started international travel, it is almost too late for effective government intervention. Thus the questions of *who* should exercise regulatory control over the consignment (export customs?, import customs?, transhipment customs?), *what* information is necessary to make a security determination by that agency and *when* should this information be made available are central to Customs' ability to identify and intercept high-risk containers before they reach their targets. Before investigating these issues however, it is important to understand the link between "authorised" traders and Customs risk management.

The "authorised" trader

The implementation of risk management methodologies in Customs is often linked to the concept of the "authorised" trader. This concept is rooted in the fact that traditional Customs control over consignments generally involves (sometimes significant) costs. As seen in Section 1 (scanning), these can involve direct costs linked to Customs-mandated container moves and scanning or indirect costs linked to delays and/or storage costs. Shippers, carriers and consignees are therefore eager to avoid these interventions and may be willing to act proactively to gain "authorised" trader status with Customs. Customs authorities are also eager to grant this status since this can lead to reduced congestion at, and greater operational effectiveness of, their installations. Thus, when importing Customs receive all of the required data related to an incoming container load for the "authorised" trader, simplified clearance procedures (*e.g.* at the shipper's premises) may be offered. Equally, consignments sent by authorised traders are less likely to require examination by Customs. The concept of "authorised traders" can also serve as the basis for the development of a "secure" supply chain where consignments transit through a number of "authorised" parties.

Customs risk management: Who makes the determination of risk?

As noted earlier, in light of the threat of CBRN weapon-bearing containers, Customs need to undertake their risk assessment before a consignment arrives at a national point of entry. The concept of "pushing" out the border to the last port of call is the basis for the US Customs Security Initiative described in Figure 4.2, Section 1 and Annex B. The CSI has opened up some interesting perspectives on the manner in which Customs oversight is exercised but many questions remain – the foremost being the role of export customs control in determining the security risks of containers.

The CSI is currently composed of a number of bi-lateral agreements concluded between the United States and other countries or regional groupings in the case of the EU. While the development of such a programme in the wake of the September 11th attacks is

understandable, the CSI has proven to be a costly programme for the United States to administer and one that cannot serve as a model for global export control. There is simply not enough port space, Customs officers, political will and/or money to extend such a system to, and among, all trading nations. This is especially true given that national Customs authorities are already in a position to exercise Customs control over exported containers. However, just because Customs administrations are in a position to exercise this control does not necessarily mean they will do so – or will do so to the satisfaction of importing countries. Not all Customs administrations operate in the same context as those of potentially targeted countries. Many administrations exercise very weak export controls and are heavily focused on administrative compliance for imports since these generate considerable revenue. Changing and/or broadening these Custom authorities' focus will require greater buy-in from these countries regarding the need for heightened export control, increased funding and technical capacity-building.

An additional issue to consider is the prevalence of corruption in certain Customs administrations. This is a recognised problem within the international trading community and efforts seeking to improve integrity in Customs administrations are central to many initiatives undertaken by the WCO[33] and the World Bank. A recent World Bank report states the problem clearly:

> "*Customs [are] vulnerable to corruption because the nature of its work puts its officials, even at junior levels, in situations where they have sole authority and responsibility where they are authorised to make important decisions on the level of duty/taxes or admissibility of imports and exports, and where careful supervision and accountability is difficult. In addition, they work face to face with members of the trading community who have strong economic or criminal incentive to influence decisions taken by Customs officials… That many officials are poorly paid is often a strong incentive to accept or solicit bribes in the execution of their duties.*"[34]

If a terrorist organisation were to successfully solicit the blind eye of a corrupt Customs officer by misrepresenting itself as a more "mundane" criminal organisation, the consequences might be catastrophic. The extent of risk posed by corrupt Customs officers is extremely difficult to ascertain but it should be sobering to know that in 2002, over 27 million containers moves were handled in ports of countries receiving a rating of less than 3 (out of ten) in Transparency International's Corruption Perception Index indicating a high level of corruption among public officials.[35]

Finally, on a fundamental level, effective export control will have to involve greater co-operation between different Customs administrations. The former have the ability to look further back in the supply chain and the latter have specific security concerns that they need to have addressed before allowing containers to depart for their shores. Mutual recognition of exporting, transit and importing Customs control and risk management processes will go a long way to facilitate early and effective security screening for containerised consignments. Work currently being undertaken at the WCO supports this goal and, in particular, the revised Kyoto Convention on the Simplification and Harmonisation of Customs Procedures establishes principles in these areas. As of June 2003, only 14 countries had ratified this Convention but there are now signs that it will come into force during 2004. The principles outlined in the Convention have already been adopted by many administrations in advance of formal ratification.

Customs risk management: What information is necessary?

The need for a common Customs "language" has long been recognised. Internationally shared standards for collecting, categorising and communicating customs data can improve compliance rates, increase the effectiveness of tariff collection and better serve as a basis for criminal and/or terrorist pre-screening of consignments. In 1996, the G7 (the "G8" since 1998) group of nations agreed to develop such a common list of Customs data elements before the year 2005. Early work on this dataset identified nearly 800 single data elements that could potentially be used. This was later reduced to a more manageable set of 113 data elements for imports. The G7 envisioned a two-step clearance process whereby goods could be released on a simplified declaration after which the shipper would submit a more detailed declaration for final clearance and payment of taxes and duties. It should be noted that the principal focus of the G7 work on common Customs data was to facilitate the fiscal (and not necessarily the security) aspects of imports and exports.

In 2002 the G8 turned over its data model to the World Customs Organization who then issued it under a slightly revised form as the WCO Customs Data Model v. 1. This model represents the maximum framework for standard data elements to be used by Customs administrations in their control of exports, imports and transit goods. However, the WCO advises its members to only request as few data elements from this broad set as necessary to ensure compliance with national laws.[36] Among these, the WCO has identified 27 data elements that it views as essential for the identification of high-risk consignments. The United States, on the other hand, only requires 17 data elements (essentially drawn from the Bill of Lading) for the Inward Cargo Declaration (CBP form 1302) that it uses to assess the security risk posed by containers arriving by sea. While these two data sets share many elements, they are not aligned with one another – *e.g.* the US data set requires more extensive information regarding the means of consignment than does the WCO data set. Thus, one might conclude that the minimum data required for properly assessing the security risk of a container is somewhere between these two – at least the 17 US requirements but not many more than the 27 WCO data elements.[37]

Customs data confidentiality and protection

It is important to set guidelines on the confidentiality and use of these (and other) data elements used to screen containers. While most of the information required by a single Customs authority for the security screening of a consignment would have eventually been communicated to that agency during the course of the goods clearance process, this is not necessarily the case when other government agencies or foreign Customs authorities are concerned. The transmission of this information outside of the agency and especially to foreign Customs must be authorised by law and follow agreed protocols.[38] Furthermore, before such a transmission or exchange of information, Customs services in the exporting or importing country must, to the extent possible, ensure the accuracy, reliability and the completeness of information to be communicated. Absent strong confidentiality protection from non-security use, traders may be tempted to bias or falsify their security-related filings in order to protect commercially sensitive data.

Customs risk management: When should information be made available and who should provide it

The issue of *when* these security-related data elements are provided to Customs (and which Customs authority: import, export, transit, or all three?) is closely tied to the issue of

who should be responsible for providing the information. As noted before under the threat of a CBRN weapon-containing consignment, importing Customs must operate their control over a container before it reaches their border. Ideally, this would mean that *information regarding a consignment is made available to both exporting and importing Customs as soon as the information is generated and by the party responsible for generating the information*. Thus, customs-relevant information contained on a commercial invoice would be made available to Customs as soon as terms were agreed between a buyer and seller, forwarders and carriers would complement this information at an appropriate time (*e.g.* when a bill of lading was issued) and so on. However, this is far from being the case today where Customs agencies exercise their control over a consignment at the last point before it enters a country – at the very earliest – and from a single consolidated document. There are three reasons for this sub-optimal (from a security perspective) processing of information. The first is the inability for importing customs to "look" further up the supply chain, the second is the lack of a common reporting framework in which traders can communicate information to Customs and other government bodies and the third is the relative scarcity of electronic filing systems able to handle information from all supply chain actors. These barriers are examined below.

The need for a Unique Consignment Reference number

Even when importing Customs attempt to discover more information about a particular consignment, their task is rendered extremely difficult by the lack of visibility of individual consignments throughout the supply chain. Customs authorities have highlighted the need for a mechanism that allows them to track a consignment from originating shipper to final consignee. Such a mechanism can currently be cobbled together with more or less ease depending on the level of integration among various supply chain actors. In the case of a single shipper sending a FCL shipment with one maritime carrier and an associated land carrier, Customs can relatively easily scan the entire transaction using the Bill of Lading. On the other hand, when the originating shipper has contracted for a LCL shipment to be consolidated by a freight forwarder before being sent on to a number of un-affiliated land and sea carriers, the supply chain can be relatively opaque for Customs and data on the originating shipper extremely difficult to uncover. Hence the need for some form of common identification number that can help to unify all sources of information regarding a single consignment.

This additional data field exists in various forms among many actors in the container transport chain. It can be a Bill of Lading number, an internal tracking code, etc. but these numbers are not universal in their form, scope and/or application. The WCO, therefore, has proposed the use of the Unique Consignment Reference (UCR) to fulfil this role. This number would, according to the WCO, serve as "staple" enabling diverse pieces of information to be linked to a single consignment throughout the supply chain. In fact, the UCR acts as a common database key allowing disparate and non-centralised data fields to be linked together.[39] Currently the WCO UCR working group is formulating a final specification of the code based on ISO 15459 (the ISO License Plate numbering system that ensures unique identification for transport units) or equivalent industry solutions so that the resulting UCR can be easily integrated by the business community. As an example for an equivalent industry solution, the WCO has recognized the tracking number issued by express carriers for their door-to-door transactions, where the tracking number is also used as a reference to the trade layer. The final UCR recommendations will be presented to the WCO Council in June 2004.

The concept of a UCR is essential to pushing back Customs visibility of the Supply chain. It will broaden the capacity for Customs to effectively audit a shipment's origin and history, will allow for a much broader range of data inputs to Customs' risk management process and will allow for these inputs to be provided when they are generated by the parties responsible for the information (see Figure 4.3). Moreover, effective Customs-to-Customs communication relating to the security assessment of a consignment requires the presence of a UCR because it provides a common access key to different sets of information. The fact that the UCR will allow origin to destination information and visibility is already an effective improvement in any Customs control activity as described in the WCO Guidelines on Advance Cargo Information (ACI Guidelines). However, in order for the UCR to be used effectively in the security screening of containerised consignments, Customs authorities must have in place information management systems capable of processing electronic filings from shippers and other actors in the container transport chain.

Finally, it should be noted that the UCR would not only assist Customs in their risk assessment exercises, but would also contribute to greater efficiencies throughout the supply chain by allowing greater sharing of information among business partners.

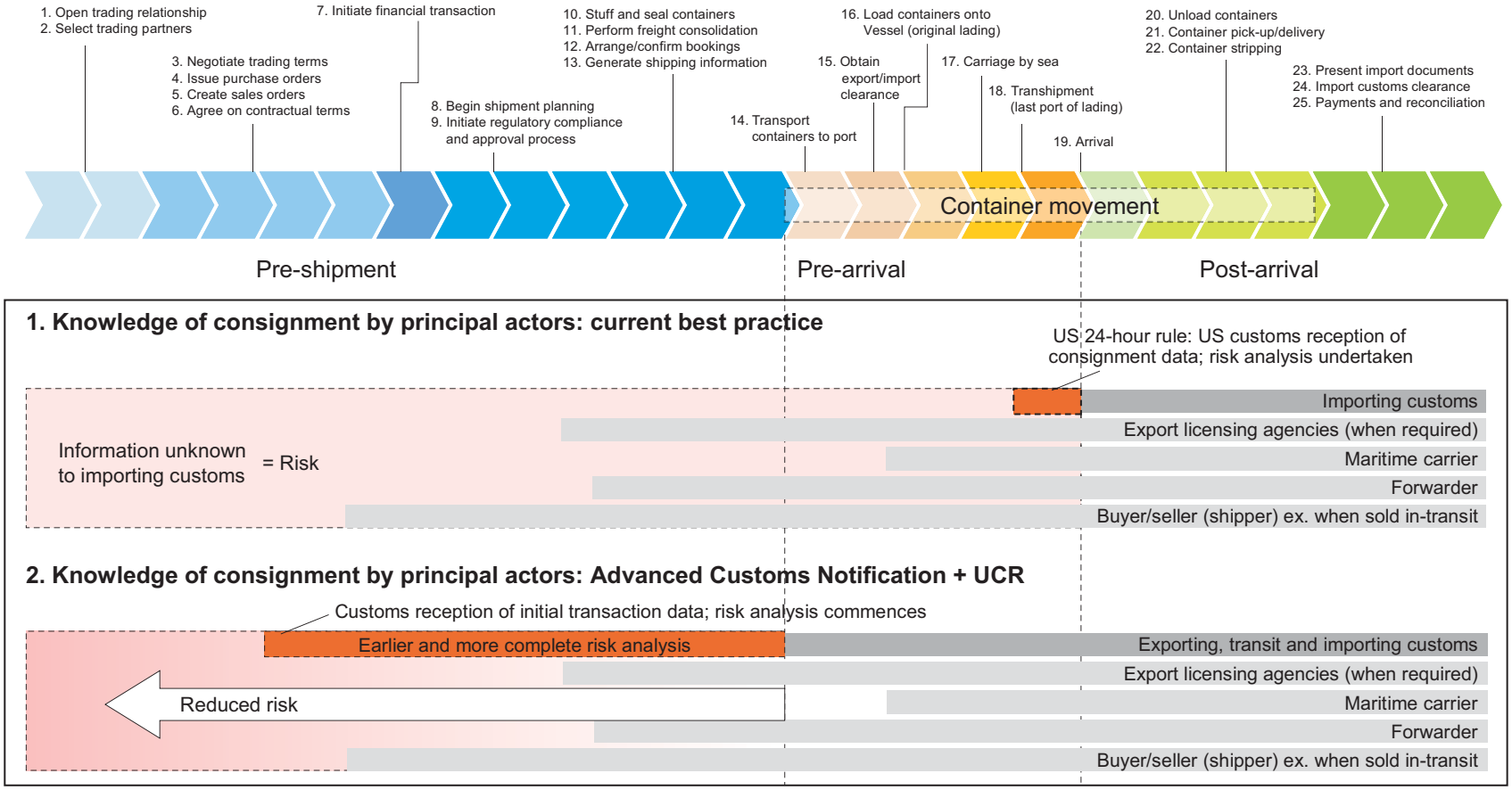
The "single window" government-trade interface

Whereas the UCR can help track a consignment throughout the container transport chain, it does not necessarily address the often inefficient manner in which traders must communicate data, including security-relevant information, to different government bodies. In order to respond to these inefficiencies, the G7/G8, the WCO, the UN-ECE and the ICC have promoted the use of a "single window" interface for communicating international trade information. Under this system, parties to an international transaction supplied information only once during the transaction.[40] The UN-ECE describes the "single window" as "a system [either paper[41] or electronic] that allows traders to lodge information with a single body to fulfil all import- or export-related requirements".[42] Such as system has been put into place in a number of countries and can facilitate the security screening of consignments while at the same time delivering tangible benefits to traders via reduced filing and streamlined procedures. However, it should be noted that the "single window" concept is oriented towards use by traders in communicating with *one* government (either the importing or exporting country). Under this context, even in the best of cases, traders will have to deal with two "single windows" – one for export control and one for import control. From a security perspective, the presence of a "single window" system would only be truly effective in enhancing container screening when combined with the use of a UCR and/or in conjunction with a protocol allowing for the sharing of information between Customs authorities.

Variable custom and trade e-capacity

Although within the WCO there is a generalised consensus that Customs' authorities must increase their capacity to receive, handle and transmit information electronically[43] many Customs administrations still operate either on a paper basis or with a low-level of computer functionality. Even within e-capable Customs administrations, not all systems are able to receive and process inputs from all supply chain actors. Despite the fact that some Customs administrations that operate at a high level of automation with systems that are already fully compliant with the WCO Customs Data Model and the UCR *and* allow for interaction and data input from all actors in the container transport chain, many other

Figure 4.3. **Supply chain security: trade processes and consignment visibility**



CONTAINER TRANSPORT SECURITY ACROSS MODES – ISBN 92-821-0331-5 – © ECMT 2005

administrations still limit access to carriers only, focus only on the last port of loading and allow only for Bill of Lading data. While work is underway to remedy this within UNCTAD,[44] it should be pointed out that many developed nations also need to allow for broader electronic input from the entire range of supply chain actors – and not solely the principal carrier and/or freight forwarder. Finally it should be noted that the lack of e-capacity on the part of Customs also hinders the development and use of automated e-seal systems and/or tracking systems. These systems are of limited use when Customs authorities cannot fully exploit their capacities due to poor information technology support.

It is also be worth mentioning that there is not only an IT deficit on the side of Customs, but also one on the side of traders. Even if countries of a lower level of development would have state-of-the-art Customs computing, if the trading community is not of the same or similar level of IT readiness, the whole exercise would be of limited use.

Conclusions: Trade documentation and information

- The principal conclusion relating to the relationship between security and trade information/documentation is that all actors in the container transport chain should work towards a system where the party responsible for generating security-relevant data provides that data to Customs when the data is first generated. This is a mid- to long-term goal as such a system requires widespread and interoperable e-capacity throughout global supply chains on both the industry and government sides, requires some form of consignment identification protocol (like the WCO UCR) and some form of guidelines on the advanced provision of data to Customs.
- From the perspectives of Transport authorities, every effort should be made to incorporate and/or communicate "proprietary" information to the principal agency in charge of screening containerised consignments. This information might cover information generated during the driver licensing, carrier registration and/or vessel registration process as well as other sources of information relating to specific carriers, their companies and/or their personnel.

Notes

1. JOC Online June 26, 2003.
2. Risk Analysis of Container Import Processes, Virtuele Haven.
3. "Seacurity" Improving the Security of the Global Sea-Container Shipping System, Rand Europe.
4. US Customs and Border Protection, *www.customs.ustreas.gov*.
5. Volume 6 – Report on Non-intrusive Detection Technologies, US Advisory Committee on Commercial Operations of the United States Customs Service (COAC).
6. Non-intrusive Container Inspection, Port Technology International.
7. One well-known and relatively common method for defeating a container door handle seal is to drill out the bolts affixing the container handle to the door, removing the handle entirely (with its intact seal), accessing the contents, replacing the handle, gluing in or otherwise affixing replacement bolts, and repainting the bolts and surrounding areas with a matching paint. In this manner, the container seal has remained intact but the container's integrity has been breached.
8. The International Organization for Standardization (ISO) has developed a Publicly Available Specification (PAS 17712 – *not* yet an international standard) that sets out specifications for Mechanical Seals. It details technical requirements for indicative, security and high security seals. It does not, however, detail the sealing processes/protocols that should accompany the use of the latter two categories of seals.

9. For example, in a fairly common "bad" sealing process, Customs authorities will remove a high security manual seal in order to inspect the contents of the container and then re-seal the box using a simple, low-security, strap seal.
10. The container seal market is a tightly competitive one with many seals being produced outside of the OECD member countries. On-site security at seal manufacturing plants and in the shipment of seals is of paramount importance since any diverted seals and/or seal designs and numbers can compromise the seals' effectiveness. The International Seals Manufacturers Association (ISMA) is addressing the problem of illegal copies of security seals made by unscrupulous manufactures. It remains to be seen if there is a need for government regulation or industry standards for seal manufactures.
11. However, it is possible to add a small battery to such "passive" (non-emitting) e-seals in order to maintain memory, clock, or other functions. Such devices would still be considered "passive", because of the communications method, but have greater functionality than "traditional" un-powered passive e-seals.
12. This capability may in fact introduce new security risks where un-authorised parties might overcome any security encoding and intentionally change the data contained in the e-seal's memory.
13. In fact, on a very basic level, a steady source of electricity necessary to run such systems is the exception rather than the rule in some areas of the world.
14. "A key finding of the evaluation effort is that although all RF based e-seals operate using the same basic underlying technology, there are widely divergent solutions in terms of how the technology is applied. E-seals from different manufacturers use not only different communication frequencies but also widely different communication protocols, reader infrastructure architectures, and tamper detection methods. Although there are a limited number of devices available in the marketplace, the devices tested showed a wide range of design features" (SAIC, 2003, p. 2).
15. … and the cost of RFID tags has a direct incidence on their uptake. RFID tags cost considerably more than high security manual seals do now, especially since RFID-enabled seals already include a hardened mechanical component. The cost of RFID tags is a much discussed topic and estimates range from $.05 to $250 – depending on design features and order size. Care should be taken in interpreting the lower estimates at face value however since the lower cost estimates are based on impossibly large orders (the $.05 per tag estimate would require an order of approximately 700 billion to 1 trillion tags today – Goldman and Crawford, 2003) – and these estimates often only cover the RFID tag itself and not the entire seal and associated sensors.
16. Different allowable power levels in the 2.44 GHz band would mean that e-seals complying to one region's radio frequency regulations would *de facto* not comply with another's.
17. This last point is important since even though there is a tendency for many cargoes to "cube-out" – that is to fill the available volume of the container before reaching the container's weight limits – there are still significant numbers of containers trading at or near their weight limits. Any increase in the empty weight of the container would decrease the available cargo capacity and therefore increase shippers' costs.
18. The Cargo Handling Co-operative Program notes in its report that "The results of the testing and evaluation clearly emphasize the need for standards in the area of electronic seals design and operations. There are a large number of potential e-seal design and operational parameters that can be selected. If there is to be any sort of interoperability of devices used by the various carriers and shippers in the industry then it is critical to develop a set of standards that will allow communication between seals and readers from various manufacturers" (SAIC, 2003, p. 2).
19. This scheme has been suggested by the World Shipping Council (WSC, 2004).
20. Report on *Removal of Obstacles at Border Crossings*, CEMT/CM(2004)23.
21. Details of such technologies are available, for example, in reports by the US Advisory Committee on Commercial Operations of the United States Customs Service (COAC).
22. For regulations concerning carriage of dangerous goods, see *International Carriage of Dangerous Goods* under UN-ECE in Annex B.
23. Statement by the American Trucking Association, Inc. (ATA), US Advisory Committee on Commercial Operations of the United States Customs Service (COAC).
24. Statement of the Association of American Railroads, US Advisory Committee on Commercial Operations of the United States Customs Service (COAC).

25. United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), International Trade Procedures Working Group (ITPWG), The International Shippers and Freight Forwarders Security Code – Draft (Security-management Systems for the supply chain).
26. US Customs and Border Protection, C-TPAT Validation Process Guidelines.
27. World BASC Organization, *www.wbasco.org*.
28. A US DOT report on the Vulnerability Assessment of Transportation Infrastructure relying on GPS notes "The GPS system cannot serve as a sole source for position location… for certain critical applications" (Volpe, 2001). While the report highlights vulnerabilities linked to navigational use of GPS, the same vulnerabilities could be cited for container tracking.
29. Volpe, 2001.
30. See *http://europa.eu.int/comm/dgs/energy_transport/galileo/index_en.htm* for details.
31. It is important to highlight here the unique situation within the EU. Customs oversight on internationally traded containers operates at the EU Border for the EU-25. *However, international trade among EU-25 countries (including short-sea shipping and EU port-to-port trade on vessels otherwise trading internationally) takes place without Customs or border controls*. Thus, security and risk assessments of intra- EU-25 container traffic will necessarily involve other non Customs authorities.
32. The TIR transit system is an established international framework of Customs-to-Customs information exchange with trader input. Information on this system is provided in Annexes A and B.
33. The WCO has produced the "Arusha Declaration" incorporating anti-corruption principles as well as a number of practical tools for its members.
34. McLinden, WCO/WB 2003.
35. The TI Corruption Perceptions Index (CPI) ranks countries in terms of the degree to which corruption is perceived to exist among public officials and politicians. It does not target Customs administrations *per se*, although perceptions of Customs corruption will contribute to the overall score. For more information on the survey and its methodology, see *www.transparency.org*.
36. This request is in fact a requirement for the signatories of the revised Kyoto Convention.
37. It is worth noting that the US data set only refers to the Cargo Declaration and does not use other information sources. The WCO list of necessary data for security screening is drawn up on two sources of information, *i.e.* the trade layer with commercial information from the supplier/customer and the transport layer with transport information from shipper/carrier. It is therefore difficult to compare both.
38. For instance, in the case of the United States "24-hour" rule US Customs receives information relating to Containers bound for non-US destinations that happen to be on vessels calling in US ports. Under normal circumstances, this information would not have been communicated to US Customs. The situation is complicated by the fact this information can be released under the "Freedom of Information Act" unless the carrier specifically files for protection of the information with US Customs.
39. Use of the UCR could also alleviate problems associated with the contractual nature of Bills of Lading as described in Section 2.2 and Annex A. Carriers could submit a Bill of Lading that conforms to their need for proper liability coverage and the shipper could submit more detailed information regarding the goods. The two would be linked through the UCR and thus the carrier would not be held liable for information that it cannot control.
40. It was, and still is, common for exporters to have to file and/or re-key multiple declarations with exporting Customs, importing Customs, importing sanitary authorities, etc.
41. The "single window" concept was originally developed in order to facilitate common trade tasks and communication with different government agencies. Time was not a strong constraint as most of these related to compliance with administrative rules relating to tariff and duty collection. From a security perspective, however, advance screening of containers is very time-sensitive and thus paper-based "single-window" systems may not add much value to the security screening of consignments.
42. UN-ECE (Trade/2002/22), 2002.
43. In fact the Customs Data Model v. 1 and the UCR are both largely predicated on the use of computerised information management systems.

44. In particular through the promotion of the UNCTAD Customs management software package ASYCUDA. This system has been used in 80 countries, although the majority of these concern the less-evolved version 2.7 of the software rather than the more recent ASYCUDA++. No administration is currently using the latest version ASYCUDA-World, which would be the only version qualifying for being called "e-customs software platform". ASYCUDA++ has some, but limited EDI capabilities, while 2.7 is using Direct Trader Input as the only remote data capture facility. Of the 80 countries that are said to be operating ASYCUDA, some of them are not operating it any longer.

ISBN 92-821-0331-5
Container Transport Security Across Modes

Chapter 5

Conclusions: Transport Authorities, Container Security and Terrorism

Transport authorities face a number of crime and security challenges relating to the systems under their jurisdiction. These include theft of goods and vehicles, attacks on truck drivers, illegal immigration, transport of dangerous goods and drug and contraband smuggling. In addition to these crime-related challenges, authorities must remain vigilant to possible terrorist use or targeting of transport vehicles and infrastructure. All of these challenges – and their responses – pose serious daily problems for authorities and can have important impacts on the transport sector's ability to ensure the efficient flow of goods within the national and international marketplace.

Among these multiple threats, however, one in particular has consistently been cited for being extremely important and requiring a co-ordinated international response – this threat is the possible misuse by terrorists of the container transport system.

Containerised transport[1] is both an essential and massively complex system that can be likened to the global economy's circulatory system. The system is supported by a Web of specialized terminals and handling facilities, transport operators, freight integrators and other actors as well as multiple strands of information flows. These have all co-evolved with the single-minded purpose of delivering steel boxes to the right destination at the right time. The ubiquity of these containers was, and is still, seen as the system's principle strength and sign of success. However, after the September 11th attacks on the United States, many countries realized that they had relatively little control over possible misuse of the system by terrorists.

In particular, the threat of a Chemical, Biological, Radiological or Nuclear Weapon (CBRN) being delivered via an anonymous shipping container has made it to the forefront of the transport security debate and the "bomb in a box" scenario has become a principal driver of international transport security policy since 2001. This has a direct impact on Transport authorities as they are charged with ensuring the efficient flow of goods while at the same time ensuring that the parts of the container transport chain under their jurisdiction are as secure as possible.

1. Transport authorities must address weak links of the container transport chain

One of the greatest difficulties in addressing the security of the container transport chain is that there is no single system governing the international movement of containers, in fact the opposite is true – container transport is characterised by complex interactions among multiple actors, industries, regulatory agencies, modes, operating systems, liability regimes, legal frameworks, etc. Conceptually, it may serve to visualise the container transport chain, in aggregate, as a massive, funnel-like integrating network that collects and concentrates container flows to a few, large actors, before dispersing these out again to final consignees.

Many of the security concerns in the container transport chain are related to inland carriers and freight integrators operating in the first few and last few links of the chain. These actors are numerous, disparate in nature and activity, operate on tight margins, and, as a result, represent more of a security risk than their larger counterparts further down the chain

(*i.e.* large land, port and maritime transport operators). It is on these larger actors and their activities that most international and bilateral security initiatives have been focused to date.

Addressing the security of the container transport chain requires a comprehensive intermodal framework integrating measures across the entire container transport chain. *Whereas such a framework may exist at the centre of the chain covering ports and maritime transport, as codified in SOLAS and the International Ship and Port Facility Security Code (ISPS), there is not yet an analogous framework for inland transport on the outer edges of the chain.*

Furthermore, while elements of this framework are emerging through the C-TPAT (for US trade), the BASC (for certain large shippers), the UN-ECE (under development for freight forwarders and shippers), the WCO (in their "cradle-to-grave" container stuffing and seal management guidelines) and in the proposed EU Freight Security Directive, none of these address the container transport chain in its entirety.

2. More specific threat assessments involving Transport authorities needed

The spectre of containers being used to deliver chemical, biological, radiological and/or nuclear weapons has motivated international action to bolster the security of the container transport chain. *However, very real questions remain as to terrorists' readiness, motivation and/or capability to use a container as a delivery platform for a CBRN weapon.* These questions should not preclude action to bolster container security – especially insofar as containers can be misused by terrorists for other purposes – but they should, at a minimum, be addressed more thoroughly through national/international assessments of specific risks posed by terrorists to the container transport chain.

In their role as facilitator and supporter of efficient transport solutions for trade, Transport authorities need to be involved in this process. When Governments work in the context of the cataclysmic "bomb in a box" scenario noted above – again, the main driver of the current policy agenda – all measures, even the most expensive ones, begin to make sense. Differentiating the threat is important to Transport authorities because ill-adapted security measures can slow down or block the flow of goods nationally and internationally.

There is evidence that well-conceived security measures can, however, actually facilitate trade: measures to enhance the early, "upstream" sharing of information on the identity, activity and consignments of traders can alleviate time-consuming delays for these purposes at border crossings and in terminals for example.

3. Security measures must be adapted to the threat

Specific security measures must be adapted to specific terrorist modus operandi. Terrorists targeting the container transport chain will likely use one of two approaches: i) they will intercept a legitimate consignment and tamper with it ("hijack" scenario); or ii) will usurp and/or develop a legitimate trading identity to ship an illegitimate and dangerous consignment (the "Trojan horse scenario").

Generally, the measures used to mitigate the threat of these scenarios fall into five groups: container scanning, ensuring the integrity of the container itself, controlling access to the container, tracking containers, and assessing container risk via the analysis of trade-related data. *Not all of these measures are equally suited to counteract both the "hijacked container" and "Trojan horse" threats as described above: what works for one scenario will not necessarily work for the other.*

4. Policy levers at the disposal of Transport authorities

Transport authorities can play an important role in countering the "hijacked container" scenario by enhancing security at all points along the chain. This involves ensuring that transport operators take into account security measures relating to container integrity and sealing, securing the access to the container and facilitating container tracking – this is especially important for inland Transport authorities who exercise oversight on the vulnerable outer links of the container transport chain. On the other hand, Transport authorities have considerably less scope for action in thwarting a "Trojan horse" shipment. In the latter case, effective customs control is of paramount importance.

Transport authorities should use the policy levers at their disposal to enhance the security of the container transport chain:

- They should establish and/or build on rules governing container handling by operators under their authority in order to introduce security criteria and define procedures regarding container integrity, access and tracking.
- As "gatekeeper" to the freight transport market via their regulatory and licencing oversight, they should also introduce security criteria in the licensing process of vehicles, operators, personnel and facilities and monitor whether licensees continue to meet these security requirements.
- Finally, they should communicate to Customs information regarding operators under their jurisdiction that might be useful in the container screening process.

5. Guiding principles to secure the container transport chain

When undertaking the above actions, Transport authorities should bear in mind a number of principles that should guide their responses. These include the following:

Container integrity:

- Container security is a shared responsibility among all actors; any breach in security in one link compromises the security of the entire chain. However, because they are the main actors with any "real" contact with the contents of the container, *Shippers and/or those stuffing the container must play a primary role in securing the container transport chain.*
- Shippers and/or those stuffing a container should follow established *security procedures*, initiate an *auditable custody trail* and ensure that the container is *sealed* with, at a minimum, a *high-security mechanical seal conforming to ISO PAS 17712.*
- Electronic-seal technologies *are not* currently ready for commercial deployment for international use throughout the global container handling network – primarily because of the multiplicity of competing and incompatible operating standards and limited operational experience. These conflicts will no doubt be overcome, yet until that happens, Transport and/or Customs authorities should not *mandate* the use of e-seals.
- A clear distinction must be made between *security-relevant* e-seal data (*e.g.* seal status and container number) and *supply-chain management-relevant* data (packing list, shipper, consignee identity, etc.). If e-seal usage is mandated, only use of the former should be made mandatory.

Access to containers:

- *Vulnerabilities in the container environment are highest in rail yards, road stops and parking and shipping/loading terminal facilities. Dwelling time at terminals should be* reduced by rationalising and optimising the process of container handling for both economic and security reasons.
- *Intermodal facilities should be physically secured* to minimise the risks of unauthorised access. Restricted areas should be approached only through access control by positive identification of employees and visitors and should be under constant surveillance.
- *Transport operators should screen employees according to security criteria*. They should also check worker identification with other operators in accordance with national laws and develop protocols regarding access to containers by high security-risk workers.

Container tracking:

- The focus of container tracking should not be "*real-time*" but rather "*right-time*" tracking – that is, ensuring that those who need to find out where a container is can do so *when* they need to know. In this context, most existing operator-specific tracking systems are sufficient for this purpose. Transport authorities should *ensure that appropriate government agencies have access to this data as needed*.
- In those cases where "*real-time*" tracking is the right solution, these systems should not be deployed without the back-up of a more "traditional" chokepoint control tracking system.

Co-operation with customs: container scanning and trade documentation:

- Screening and scanning of containers, while complementary, are not the same. *100% container screening is possible, should an administration choose to do so – 100% scanning, on the other hand, is not practical with current technologies.*
- Transport authorities should assist Customs in their container screening exercises by ensuring that "proprietary" information (*e.g.* regarding transport operators, licensees, etc.) is made available to Customs for their container risk assessment in accordance with national rules on data confidentiality.
- Transport authorities should also *support the concept of advanced information submission to Customs and use of the Unique Consignment Reference number* among transport operators.

6. Specific recommendations to inland Transport and Maritime authorities

Agreed recommendations should be implemented and existing initiatives improved.

Applying the ECMT Ministerial Declaration on Combating Terrorism in Transport, agreed by Ministers in 2002, will go a long way to improving security of the inland container transport chain. Specifically, Ministers agreed to:

- Promote a co-ordinated intermodal approach to security in the transport sector in co-ordination with other relevant bodies within national governments.
- Share to the extent possible experience and best practice on transport security and counter-terrorism with other governments in order to further understanding and co-operation in this area.
- Provide support as needed for risk and vulnerability assessments as well as training for personnel on emergency procedures within and between modes and on regional and local levels.

Ministers also agreed in the 2001 Ministerial Conclusions on Combating Crime in Transport to set up specific contact points within Ministries to handle all crime and security questions. At this time, some Ministries appear to have done this – many others not. Given the wide and diverse range of issues related to transport crime, security and terrorism, a contact point able to centralise and co-ordinate the inquiries to the appropriate individuals of competence within the Ministry would be extremely useful.

In addition, the ECMT Resolution No. 97/2 on Crime in International Transport contains elements that can be adapted to counter terrorist threats in the container transport chain.[2]

The establishment of an inter-governmental task force (along the lines of that set up in the UK) to implement a common approach to container transport security would facilitate the necessary co-ordination between Transport authorities, Customs, and security and police agencies.

On the maritime side, the mandatory framework of SOLAS and the ISPS code already govern security measures for international ocean-going vessels and ports involved in international trade. However, there is some concern that the 1 July 2004 deadline for the ISPS has not been taken sufficiently seriously by some vessel operators and/or ports. At a minimum, Maritime authorities should do the following:

- Ensure that ports and vessels under their ultimate authority comply with the terms of the ISPS by the deadline. Furthermore, they should also ensure to the best of their abilities that real compliance with the ISPS code, rather than superficial "paper" compliance, is achieved.
- Strictly enforce ISPS code compliance by vessels entering their ports after the July 1, 2004 deadline.
- Ensure that many of the basic provisions of the ISPS extend to those vessels and ports not covered by the ISPS (as certain countries have already done).[3] For instance, the European Parliament and Council Regulation COM (2003)229 on enhancing ship and port facility security encourages countries to consider extending ISPS coverage to non-ISPS regulated ships and ports. In this context, co-ordination with inland navigation vessels not covered by ISPS, particularly in areas where inland and maritime waterways and ports interface, will be essential.
- Non-EU ECMT member countries should consider applying relevant provisions of EU Regulation COM(2003)229 as well in order to ensure the overall security of European maritime shipping.
- In addition, countries may consider extending coverage of the ISPS, now limited to port facilities and terminals, to the entire port as well as to adjacent areas where these have direct or indirect impact on the port (*e.g.*, rail facilities, warehouses, etc.). Such an approach is articulated in the Proposed Directive of the European Parliament and Council on Enhancing Port Security COM(2004)76 Final.

Notes

1. While there are a number of freight containers in use within different modes use (*e.g.* Unit Load Devices – ULD's – used in aviation and Swap Bodies used for road-rail carriage in Europe), it is the potential threat to, and from, *maritime shipping containers*, that has been singled out in the context of anti-terrorism policy because of their numbers, ubiquity and intermodal nature.

2. These include recommendations that Ministries of Transport:
   - Set up improved contacts with the police and customs authorities as well as trade organisations to ensure that information on crime, crime trends and criminals is exchanged wherever appropriate; (N.B. though not specified in this Resolution, it would seem important to add in the case of container transport security the exchange of information with intelligence and security services).
   - Check that operators given licences and permits are bone fide operators without criminal records pertinent to vehicle/freight crime.
   - Maintain information on persistent offenders and withdraw licences or refuse to grant permits to them.
   - Provide information and advice to operators on theft avoidance, safe practices, recommended routes, protected parking areas and appropriate precautions.
   - Encourage the setting up of secure and safe parking areas and freight traffic centres for trucks and loads (containers, trailers, swap bodies). Standards of protection for such areas must be defined to commonly agreed levels or criteria.
3. These include ports not participating in international trade, vessels of less than 500 GT and vessels not trading internationally.

ISBN 92-821-0331-5
Container Transport Security Across Modes

ANNEX A

Description of the Container Transport Chain

General background on containers: supplementary information to Section 1

The unit used to measure container capacity is the TEU ("twenty-foot equivalent unit"), which refers to the length of the standard container box. Given the prevalence of non-standard container sizes (ranging from 10 feet to 62 feet in length), TEU figures are always greater than the actual number of containers in question.[1] In 2002, the Bureau International des Containers (BIC) estimated that approximately 15 000 000 TEUs were in circulation worldwide.[2] The World Shipping Council estimated that by mid-2003 approximately 17 000 000 TEUs were in circulation accounting for 10.8 million individual containers.[3] Containers are assigned individual numbers that are registered by the BIC.[4] The container number is printed on both the inside and outside of the container sidewalls and, in some cases, on the doors.

The global container fleet is almost evenly divided between carriers' self-owned fleets and those of the many large container-leasing companies. Figures provided by the Institute of International Container Lessors (2003) provide some insight into the relative distribution of container sizes and types. 53% of leased containers are 40-foot boxes accounting for over 70% of the leased container fleet capacity. Approximately 8% of the TEU capacity in the leased fleet concerned container types other than the standard dry box. These included tank containers, refrigerated containers (including self-powered units) and open top containers (0.1%, 5.2% and 1.9% of the leased fleet capacity). These numbers remain quite small even when extrapolated to the carrier/shipper-owned fleet but they are relevant from a security perspective because each of these container types pose special security risks.

Global flows of containers along the principal trade routes in 2002 accounted for 37.7 million TEUs or roughly 24.3 million actual box moves concentrated in the dominant Trans-Pacific, Asia-Europe and trans-Atlantic trades. Container traffic figures for world ports from Containerisation Online indicate that over 264 million containers were handled in 2002. These figures account for all containers handled at the various ports including transhipped containers, empty container moves on both the export *and* import sides. These trade volumes are expected to increase in coming years as world trade increases. In particular, container movements will largely be influenced by trade developments in Asia – on both the export *and* the import side. Indeed, while the United States is projected to remain the world's top container-importing country by 2005 (16.2 million TEU), China will represent the fastest growing importing country. Overall, Asia is projected to account for 52.8 % of all containerised exports and 37.3% of all containerised imports by 2005.[5]

Actors and their roles in container transport

Containers are not autonomous entities – they are set into motion as the result of a series of transactions amongst multiple actors. It is important therefore to understand who these actors are, how they relate to each other and to the container, what type of information they produce and what type of information relating to the container and/or its contents they have access to. These actors can be broken down into the following five sub-groups whose roles are described below.

Role: primary customers

The shipper and the buyer

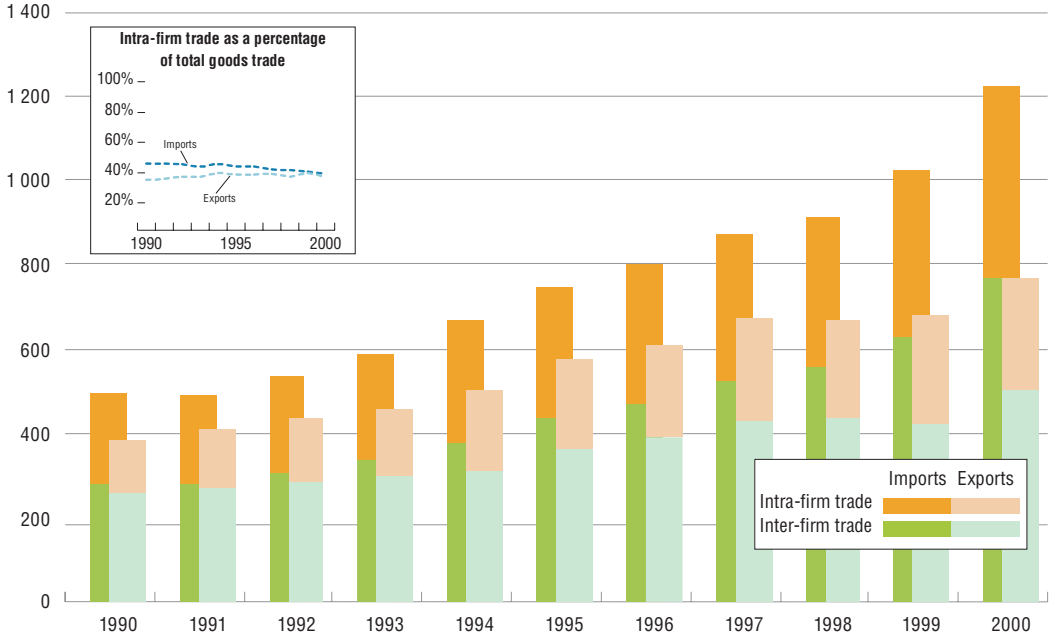
From a security perspective, the shipper represents one of the most import links in the container transport chain. Not only does the shipper have detailed knowledge about the entire transaction leading to the shipment of the container but, in most cases, the shipper is the *only actor in the chain with detailed first-hand knowledge of the goods placed into the container*.[6] The shipper packs ("stuffs") the container, closes and seals the door and sends the container on its way. Depending on the terms of the transaction, the shipper and carrier agree to one of several possible liability arrangements for the goods during their voyage.

Many analyses of container security start with the stuffing and sealing of the container at the originating shipper's location. This process, however, takes place well downstream of the actual start of the commercial transaction that eventually sets the container in motion. It is important therefore to understand who is involved in initiating the container movement upstream of its actual departure from the shipper's premises.

Containerised transport is the physical manifestation of a commercial transaction between two parties – a buyer and a seller (or importer and exporter when the container crosses international boundaries). The buyer expresses an interest in acquiring a good that the seller is willing to sell and ship. While in many cases the seller is also a manufacturer as well as the originating shipper, this is certainly not true in all cases. There are four principal exceptions:

- **Intra-firm trade**
  The first is where the shipper is both the seller and buyer. This case arises when the importer and exporter are within the same company and/or family of companies. A significant portion of international container movements concern intra-firm trade or trade between affiliates or otherwise linked firms. For example, in the United States, intra-firm trade accounts for approximately one-third of the value of all exported goods and two-fifths of the value of all imported goods (see Figure A.1). In many respects, intra-firm trade presents potentially fewer security risks as the parties to the transaction are known to each other and trusted.
- **Wholesaler as seller**
  In this case, the shipper is a wholesaler that purchases and keeps an inventory of goods that are sold and shipped from the wholesaler's premises.
- **Manufacturer as assembler**
  The third case arises where the "manufacturer" subcontracts out most, if not all, manufacturing functions to suppliers and only assembles pre-made components into a final product. In this case, many of the pre-assembled components travel to the final manufacturer's site by container as well. From a security perspective, it is important to

Figure A.1. **Intra-firm trade: share of United States imports/exports 1990-2000**



understand how the supply chain extends beyond the manufacturer to the supplier base – especially in the case of large pre-assembled components that could potentially hide a weapon.

- **Wholesaler/broker as seller**

  Another possibility is that the seller is only a broker to a transaction – that is, the goods were purchased from a manufacturer, shipped according to the broker's instructions and, while in-transit, re-sold to a third party. While this type of transaction is more common with bulk goods, where ownership of the contents of a bulk/tank vessel may change hands several times while the ship is en-route, some containerised goods – especially goods that traditionally were handled in bulk – are traded in this manner. In these instances, the final seller can be several steps removed from the original shipper.

There is also a fifth case that will be examined in more detail below. In this case the shipper is a freight consolidator[7] that appears as the originating shipper in all downstream freight documentation.

For the remainder of this section, we will assume that the shipper is either a manufacturer or wholesaler and the seller/exporter.

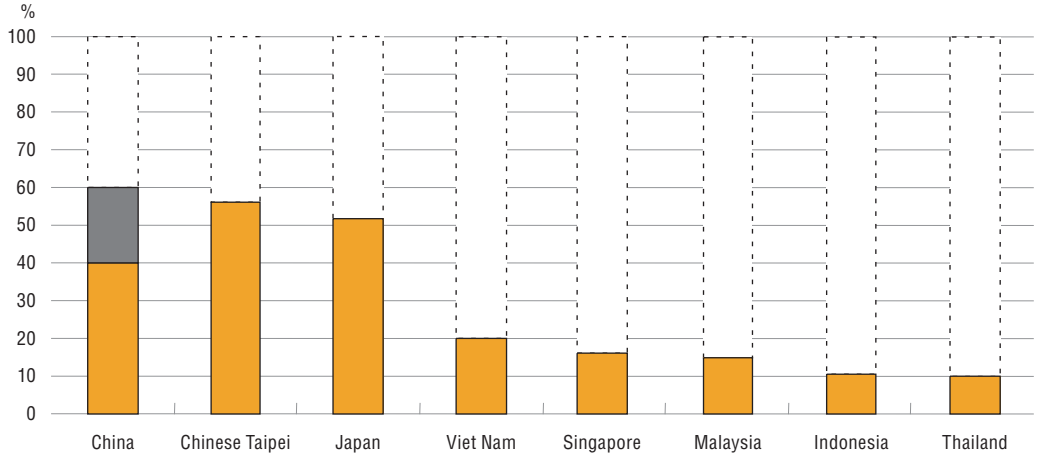
Before the goods can be transported – or at least before they can arrive within the importing country – the shipper has several responsibilities. The shipper must come to an agreement with the buyer/seller and produce the goods to the specification of the latter as specified in contractual documents. These documents also indicate the means by which the goods will be conveyed and the manner in which ownership and liability for the goods will be apportioned among the different parties to the transaction. When necessary, the shipper must also arrange for proper export licensing with the exporting country's administration and provide information enabling the importer to receive appropriate import licenses. In cases where export/import quotas apply to the goods in question, the parties must also ensure they obtain sufficient quota allocations. Finally, the shipper must

ensure that information necessary for passing export/import sanitary controls is made available to authorities in both the exporting country and importing countries (in the case of food, agricultural, timber and wood palletised shipments).

It is important to note that shippers (and buyers) generate considerable information regarding a consignment early on in the container transport chain that is not, at present, communicated directly to those authorities that could use this to better target suspicious consignments.

Shippers (and buyers) are the most numerous actors in international trade. How numerous – while important from a security analysis perspective – is extremely difficult to say with any precision. The reasons are multiple and include the fact that there are no global sources of aggregate data on the numbers of firms trading internationally, that many containerised shipments never cross international borders and that many shippers ship only intermittently. However, from what can be gathered from existing data sources, one can surmise that these numbers range in the hundreds of thousands to millions. In the EU alone, over 4 000 000 firms exported goods in 2001-02 and another 231 420 did so in the United States in 1999.[8] On the import side, the numbers are equally impressive – in the United States approximately 202 800 firms received imports from approximately 178 200 foreign shippers in 2002.[9] What is striking from a closer inspection of the data is the significant participation of small and medium-sized enterprises in export trades – approximately 40% of exporting firms in the EU are SMEs and nearly 97% of all US exporters are SMEs. Indirectly, one can also surmise that SME representation in exporting firms is important in Asia as well by looking at the SME share of exports by value (see Figure A.2) that ranges as high as 50-60% for some large exporting economies.

Figure A.2. **Share of SME exports (by value) in selected Asian economies**



From a security perspective, the large participation of SMEs in containerised trade has repercussions on efforts to secure the container transport chain. Indeed, efforts to extend supply chain security to the originating shipper must take into account these actors' relative lack of resources available to implement security measures.

Role: transaction facilitation

While many shippers, especially large volume shippers, may handle most aspects of their import/export functions in-house, the complexity of international trade leads others to have recourse to one or several intermediaries that seek to facilitate the import/export process. These intermediaries have an important role to play in securing the container transport chain because they often have early and sustained access to information regarding the container and its contents throughout the transaction. In most cases, however, they do not have first hand knowledge of the container contents except in those cases where they stuff the container themselves. Again, as in the case of the shipper, the extent to which they are exposed to commercial liability for the contents of the container are defined in the commercial terms agreed to by the parties to the transaction.

While in the paragraphs that follow, these intermediaries have been treated separately, recent trends in the logistics sector have led to a blurring of lines between these intermediaries and indeed, other actors in the freight transport chain such as transport operators. It is not uncommon today to find freight forwarders that provide custom brokerage services, buying agents that provide some freight forwarding services, carriers providing consolidation services, etc. For this reason, the following sections describe both actors in the transport chain as well as broader functions that are carried out by new hybrid logistics providers.

Buying agents (sourcing)

A buying agent is often used by buyers operating in unfamiliar markets. The agent represents the buyer in dealings with the manufacturer/seller and other important actors such as local carriers, freight forwarders and government agencies. Typical responsibilities may include obtaining quota allocations and the export license, preparing the Letter of Credit and overseeing its compliance, and arranging for and communicating with carriers and freight forwarders/consolidators.

Freight forwarder/consolidator/NVOCC (transport facilitation and load consolidation)

In many cases, buyers require assistance throughout the entire transport chain. Freight-forwarders (and/or other parties such as carriers providing freight forwarding services) respond to that need and facilitate several and/or all aspects of the container move from their point of origin to their destination. Their core functions go beyond those of the buying agent and include preparing and transmitting all necessary documentation, negotiating rates with and arranging for transportation by road, rail and water carriers and arranging for the dispatch of empty containers to the shipper. In addition to ensuring statutory compliance and arranging for transportation, many forwarders have broadened their services to cover trade consulting (*e.g.* route selection, shipment scheduling, etc.) and logistics (supplier network strategies, supply chain configuration, in-house logistics optimisation, etc.) services.

Most forwarders also offer load consolidation services that respond to the fact that many shippers generate less-than-full container loads (LCL as opposed to FCL – or full container load). In these instances the shipper will ship their consignment to a forwarder who will proceed to assemble a full container load with other consignments. In many cases, and in particular where the forwarder has purchased shipping slots from a maritime carrier in advance, the forwarder acts as a shipper and is referenced as such in the

documentation relating to the forwarder-consolidated FCL. In North America, these forwarders are referred to as Non-Vessel Operating Common Carriers (NVOCCs). These forwarders act as contractual carriers for their clients (and thus issue a single bill of lading) while the actual transport task is sub-contracted out to various modal operators for whom the NVOCC is only one shipper among many others.

While the consolidating forwarder may be aware of who the originating shipper is, and may have actually handled the contents of the container, the same can not be said of the carrier who receives a consolidated loads from a forwarder. In this case, all of the documentation available to the carrier points to the forwarder, and not the originating shipper, as the shipper of reference. This situation is further complicated by recent trends towards the use of "Fourth party" service providers. Many small forwarders cannot generate sufficient volumes of trade to leverage favourable enough rates from carriers – in these instances small forwarders may turn to Fourth-party consolidators who purchase large amounts of shipping slots from maritime carriers and in turn sell these to small forwarders. At each step along the way, information regarding the originating shipper becomes more difficult to access and verify.

While freight forwarders have sought to expand the number and scope of services they provide, other actors in the logistics chain – and in particular transport operators – have sought to offer what had been traditional "forwarding" services. It is not uncommon now to find major maritime, road and rail carriers offering the full range of door-to-door freight-forwarding and brokering services that in the past had only been offered by specialised firms.

This blending of roles across the container transport chain makes it difficult to determine the exact number of "freight forwarders" as more and more companies intervening in the logistics chain advertise themselves as "door-to-door logistics providers". At a minimum, one can consider the over 40 000 firms represented by FIATA ("Fédération Internationale des Associations de Transitaires et Assimilés" or "International Federation of Freight Forwarders Associations") as the core representation of the freight forwarding sector to which several other hundreds or thousands of firms offering forwarding services must be added.

Finally, while the use of consolidating forwarders has become quite common throughout the OECD, it should be noted that it is business practice in many developing countries for the shipper to organise and use its own network of carriers and brokers rather than have recourse to a forwarder's services.

Customs broker (customs clearing and regulatory compliance)

These specialised agents deal exclusively with the government agencies that have regulatory oversight over containerised trade in order to facilitate cross-border passage, clearance and release of goods to the buyer. Customs government agencies are the primary counterpart of the customs broker, but it is not uncommon for other agencies such as Agriculture or Trade to be part of the goods release process. Customs brokers have no responsibilities for carriage, cargo condition and do not take custody of the goods being shipped. They have therefore no liability in this respect, whilst they may have limited liabilities as regards their own services. Except in customs matters, they transmit information provided by other parties to the appropriate authorities and their responsibility is generally limited to securing that information is not altered or manipulated by others.

Role: Transport task (physical movement of container)

Road

Aggregate figures for the road carriage of containers are difficult to come by, however most containers are at some point transported by road, often at the beginning and/or the end of the transport chain.

The scale of road container transport can be somewhat approximated by looking at the importance of the road sector in international freight transport. Road transport's overall share of the freight market has been growing constantly, accounting for 63% in Western Europe, 49 % in Central and Eastern Europe, and 38% in total OECD countries in 2000 (Table A.1). Its advantages such as unique flexibility to meet just-in-time delivery at a low price and freedom to carry goods all over the destinations have led to growing road freight transport demand, in spite of the negative environmental consequences of road transport.

Table A.1. **Modal split in 2000 – World freight transport**

%

	Rail	Road	Inland waterways	Pipeline	Sea (national transport)
Total ECMT	**32.2**	**27.0**	**3.5**	**33.6**	**3.7**
Total OECD	**32.0**	**38.2**	**9.6**	**10.8**	**9.3**
Western Europe	13.1	63.4	6.1	6.9	10.5
Central and Eastern Europe	39.2	48.7	2.1	9.9	0.1
CIS	42.0	4.6	2.2	50.9	0.3
EU15	14.1	63.2	7.1	4.9	10.7
USA	39.0	28.6	9.6	15.3	7.5
Japan	3.8	54.2	0.0	0.0	41.9
Russia	39.0	4.3	2.0	54.4	0.2

Note: Data not available for Iceland, Malta, Armenia, and Mexico.

Source: ECMT.

- Operators

There are more than 420 000 road transport enterprises in the EU, many of which are small operators. Road freight transport alone accounts for 56.5% in number of transport enterprises in the EU (Table A.3). Of road transport enterprises in the EU, more than 99% is small firms (with fewer than 50 employees) and less than 0.1% is large enterprises (with more than 250 employees).[10] The small trucking companies face fierce price competition

Table A.2. **Distance classes by mode of transport**

%

Km	Road		Rail		Inland waterways	
	t/km	Tonnes	t/km	Tonnes	t/km	Tonnes
0-49	5.1	53.7	2.3	24.1	5.3	29.2
50-149	16.4	22.8	9.3	22.7	29.0	39.6
150-499	41.9	18.4	49.1	40.4	54.1	28.9
500-	36.5	5.1	39.2	12.8	11.5	2.3
Total	**100**	**100**	**100**	**100**	**100**	**100**

Source: European Commission, *EU Energy and Transport in Figures Statistical Pocket Book* 2003.

Table A.3. **Number of enterprises by mode of transport 2000**

	Railways	Pipelines	Road passenger transport	Road freight transport	Sea transport	Inland water transport	Air transport	Travel agencies and tour operators	Other[1] auxiliary transport activities	Transport total
Belgium	3	10	2 310	7 298	79	248	119	1 332	2 137	13 536
Denmark	17	4	3 917	7 994	422	35	99	564	1 320	14 372
Germany	106	29	21 212	32 885	702	1 121	270	7 400	10 066	73 791
Greece	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.	n.a.
Spain	7	n.a.	67 236	130 141	171	16	51	5 897	12 448	215 967
France	30	33	33 741	44 311	740	1 190	531	4 303	6 471	91 350
Ireland	*2*	n.a.	191	2 919	*41*	*0*	*34*	227	*541*	*4 120*
Italy	139	22	23 360	112 173	591	807	196	8 902	15 672	161 862
Luxembourg	1	1	166	478	n.a.	85	1	111	111	*953*
Netherlands	10	15	3 680	10 290	670	3 690	170	2 245	3 815	*23 510*
Austria	14	2	4 116	5 019	15	51	79	1 253	1 003	11 552
Portugal	*1*	n.a.	11 265	5 906	78	23	23	978	1 417	*19 691*
Finland	4	n.a.	9 066	11 843	223	90	61	745	1 145	23 177
Sweden	27	11	9 637	15 447	478	359	175	2 227	2 454	30 815
United Kingdom	111	28	9 506	36 819	1 020	215	934	6 555	10 062	65 250

1. Cargo handling and storage, other supporting activities, activities of other transport agencies.

Source: European Commission, *EU Energy and Transport in Figures Statistical Pocket Book* 2003.

and therefore lack resources compared with larger companies. It is not easy for them to finance investment in high-tech solutions; as a result, they are unlikely to be enrolled in any voluntary security program that can increase their operational costs.

In addition, trucking operators are probably among the most vulnerable due to the physical openness of road infrastructure. The extensive road network, including critical infrastructure such as tunnels and bridges, is generally accessible and goes through densely populated areas. It would be relatively easy to hijack and use a truck as a weapon. It is also possible for terrorists to obtain commercial driver's license to operate large trucks legitimately.

- Regulating international road transport

A brief examination of how international road transport activities are organised and managed can provide insight into what points of leverage are available to authorities – primarily Transport authorities – to enhance the security of road transport of containers.[11]

International haulage by road is regulated mainly by a system of numerous bilateral agreements in Europe. In the EU, a Community licence is given to transport for hire and reward between member countries, which has a multilateral character and is issued for a period of five years and is renewable. Outside the EU in ECMT areas, transport operations to or from countries that do not belong to the EU require an international transport licence: either a bilateral licence, which may be used both for transport on own account and for transport for hire or reward, or the ECMT multilateral licence, which is only available for transport for hire or reward. The ECMT multilateral licence is distributed based on criteria concerning economic size, trade and transport performance, safety and environment.

Generally speaking, criteria for licensing have increasingly focused on ensuring quality of service. In Europe, qualitative criteria applied include good repute of the transport firm, minimum financial standing, and professional competence.[12] Good repute ensures that the

operator has not been convicted of serious and repeated offences against the rules in force concerning pay and employment conditions, the rules on drivers' driving and rest times, the weights and dimensions of vehicles, and more generally road safety, environmental protection and financial responsibility. The financial standing criterion ensures that the operator has sufficient resources for proper operations without endangering safety and security. The professional competence conditions control for sufficient knowledge on the part of the operator regarding rules for carriage of dangerous materials, vehicle safety and environmental regulations and highway code. In North America, further harmonisation of regulations on truck operations with respect to safety, insurance and customs requirements, etc. are being sought by NAFTA's Land Transportation Standards Subcommittee (LTSS).

Rail

Generally, the trend in rail goods transport has been downward or stable in ECMT and OECD countries over the past decade in favour of road transport. Rail goods transport accounts for about 32% of the total in ECMT and OECD countries in 2000. The share is high in the US and Russia, which account for about 39% of total goods transport in 2000 for both countries (Table A.1). Intermodal traffic on US railroads, the number of international containers, domestic containers, intermodal truck trailers, and road-railers handled by the railroads tripled over the last two decades from 3.0 million to 8.7 million.[13] Because of the relative advantages of rail transport (*e.g.* its environmental and safety benefits relative to road – one train can carry the equivalent of up to 50-60 truckloads), modal shift in favour of rail is promoted by strong government policy in many countries.

Rail freight transport's modal share is particularly strong compared with road where longer distance journeys are concerned (Table A.2). In the EU in general, the trend for rail shows an increase in the share of international transport and a decrease in national transport in 2001 compared to 1990. While road transport dominates most categories of goods transport, rail is dominant for transport of heavy goods like coal and other solid mineral fuels, ores and metal products.[14]

- Operators

Rail operators are generally larger in size and fewer in number than trucking operators. Most rail companies are state-owned and run, though in some countries, an increasing number of operators are privately-owned, with government subsidies and some are state-owned. The openness of infrastructure network is similar to road, however, risk of hijacking seems to be lower than road transport because trains can run less flexibly, *i.e.* only on their rail tracks.

- Regulating international rail transport

For international interoperability of railways in Europe, there are two dominant pieces of EU legislation: Directive 96/48/EC on the interoperability of the trans-European high-speed rail system and Directive 2001/16/EC on the interoperability of the trans-European conventional rail system. The directives stipulate the compliance of subsystems (infrastructure, rolling stock, maintenance, etc.) with the Technical Specifications for Interoperability (TSIs); essential requirements for safety, environmental protection, and other areas; and verification procedure by a notified body, which checks and certifies compliance with the Directives and other regulations.

In North America, there are a number of technical and safety regulations with respect to the operation of rail transport among the three NAFTA countries. The Land Transportation Standards Subcommittee (LTSS) is working on increasing the compatibility of the regulations for smooth cross bordering operations.

Inland waterway

The modal share of inland waterways has decreased overall, falling short of the growth in other modes. Inland navigation's share of goods transport is roughly 6% in Western Europe, 3.5% in ECMT countries, and 10% in OECD countries in 2000 (Table A.1).

While inland waterways are used for both short- and long-distance freight transport, inland navigation tends to cover longer distances than road (Table A.2). In 2000, national and international transport by inland waterways accounted for respectively 48 % and 52% of the total. Crude and manufactured minerals and building material account for almost half of the commodities carried by inland waterway transport.[15]

• Operators

Inland navigation is a sector with many small operators, as is the case withroad transport. The number of enterprises in EU15 countries is about 8 000, nearly half of which are Dutch.

Inland waterway carriers often offer all-in-one packages such as carriage from the seaport to the shipper's loading bay; a sea container inland depot service; and return of empty containers.[16]

• Regulating international inland waterway transport

The Central Commission for Navigation on the Rhine (CCNR) and the Danube Commission are responsible for the safety, effectiveness, efficiency and environmental sustainability of inland waterway transport in Europe. The United Nations Economic Commission for Europe (UN-ECE) is developing the legal and technical aspects of efforts to harmonise the technical, professional, safety and infrastructure-related regulations for inland waterway transport at a Pan-European level.[17]

For navigation on the Rhine, which is by far the most important inland waterway in Europe, the CCNR has adopted a number of regulations ensuring the safety of navigation. The Inspection Regulation for Rhine Vessels settles the technical requirements for the licensing of vessels to navigate on the Rhine, the requirements for safety, emissions, equipment, manoeuvrability as well as crews. If the vessel conforms to the regulations, a so-called "ship's attest for the Rhine" (*i.e.* ship's certificate) is issued by the Inspection Commissions of the CCNR member states (Belgium, France, Germany, the Netherlands and Switzerland). The Regulation of boatmaster's licence for the Rhine (Rhine Patent) settles the requirements to be met by crews. After having finished a training period and an examination, the applicants are issued the Rhine Patent entitling them to steer a vessel on the Rhine. Provisions concerning the Carriage of Dangerous Goods on the Rhine (ADNR) set out the technical and operational safety requirements for the licensing and the operation of inland navigation vessels carrying on board dangerous goods.[18]

• Port/terminal operator

There are approximately 4 600 ports in the world that handle commercial traffic. Only 466 of these, however, regularly handle containerised traffic. Among the latter, the large majority (356 ports) are relatively small and/or medium-sized ports that handled less than 500 000 TEU moves in 2002 (including full, empty and transhipped containers). On the other end of the spectrum, the world's top 20 ports handled 48% of all port container moves in 2002, and the top 40, nearly 63%. As can be seen in Figure A.3 below, the world's megaports are located primarily in Asia and, to a much lesser extent, in Europe and in North America.

Not all these ports serve the same function in the world trading system – even among the larger ports that anchor the principal east-west trade lanes. While many ports serve extensive hinterlands that reach across entire continents (as in the case of the European North Sea ports), others serve local/regional markets only. Furthermore, some ports operate mainly as trade "gateways" while others serve principally as transhipment "hubs". It is estimated that transhipment accounts for approximately one quarter of all container port throughput, although in some specialised ports such as Singapore and Colombo, transhipment may represent up to 70% of port throughput. These movements have grown in importance as liner operators have invested heavily in larger capacity ships on the main trunk routes. These ships are serviced by a number of smaller vessels operating regional feeder routes connecting the main hub ports to their surrounding region. While this "hub and spoke" system remains a dominant feature in many regions, certain global carrier alliances have recently started to offer a blend of main trunk services calling on major ports along with second-level services calling on a string of secondary ports.

While a port authority may represent a single actor, the port area itself may often assemble a number of different actors that may or may not have a direct link to containerised trade. Individual quays and jetties are often operated by independent terminal operators who specialise in servicing a wide range of vessel types. Across a large port, one might find oil and gas terminals, bulk iron ore and chemical terminals, grain and livestock terminals along with container terminals. However, many ports now tend to specialise themselves in one type of operation. While port operations are often (but not always) in the hands of the private sector, in many cases, ownership of the port is not. Depending on local and national arrangements, the port and its infrastructure may be owned either by national, regional or local authorities or by private operators.

Concentration in the terminal operations sector

• Maritime carriers

Maritime carriers are the most visible link in the international movement of containers – principally because they concentrate and move so many containers per voyage. Not all international moves include a maritime leg – especially in the case of North American and trans-European trade – but given the current configuration of world trade, most container moves include at least one sea leg.

There are currently 457 maritime carriers operating vessels that can accommodate containers (CI-online, January 2004). The majority of these vessels (as well as the majority of the available capacity) are fully cellular ships – that is ships designed for the exclusive purpose of transporting containers. 27 of these carriers only operate containers barges and as such do not participate in ocean trade. The remaining vessels are either mixed-used

Figure A.3. **World port container handling in 2002**

TEU's/number of ports

Source: Data from CI-Online, Cartography, Philippe Crist (OECD).

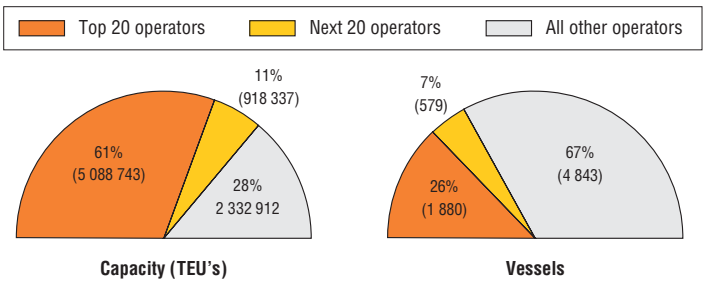
vessels that carry vehicles and cargo containers (roll-on/roll-off) or mixed use general cargo vessels. The world container vessel fleet is dominated by the presence of several large carriers that operate high-capacity vessels (up to 8 000 TEU's) in a few selected trades. The top twenty operators account for 61% of the total fleet capacity and the top 40 operators account for 72% of total capacity. The corresponding figures for the fully cellular fleet are 78% and 92% respectively. Smaller carriers are more likely to be operating in lower-volume trades that service major transhipment centers.

Fully cellular vessels can store containers both above and below deck in a series of racks made to fit standard container sizes. Once stored on-board a fully cellular vessel, crew members have extremely limited access to most containers – especially when these are stored below deck and/or inside full stacks. Generally speaking once a container is lashed down on board a fully cellular vessel, the risk of tampering is nearly inexistent. However, on other vessels, this may not be the case – especially for mixed-use cargo vessels where containers are stored with other break-bulk cargo.

The core role of the maritime carrier in the container transport chain has traditionally been to provide "liner" services – that is, services that are provided on a regularly scheduled basis to pre-determined ports. Recently, however, several major carriers have begun to re-position themselves as door-to-door transport and logistics services providers. These carriers offer door-to-door transport services that are supported by a network of commercial partners and/or wholly-owned subsidiaries on the land side. Furthermore, carriers have also sought to acquire and/or develop expertise in terminal operations.

Figure A.4. **Consolidation in the maritime container-carrying fleet**

1/1/2004



- Shipping line agent (representative)

In order to operate their fleets and carry out essential commercial tasks, ocean carriers have deployed an extensive Web of agents in the ports they service. These essential personnel are in direct contact with shippers/forwarders and have an important role to play in ensuring the security of the container transport chain. A carrier may be represented in its commercial dealings with shippers/forwarders by one of its own staff or by an independent agent that may represent a number of other carriers. Shipping line agents typically perform the following functions:

- Sales and marketing.
- Booking new shipments.
- Ensuring the timeliness and correctness of all documentation regarding the ocean carriage of the container.

- Organising the physical handling of the container.
- Issuing Bills of Lading.
- Receiving and/or releasing containers and collecting related charges.
- Handling cargo claims.
- Managing carrier-owned or leased equipment.
- Handling non-cargo related vessel operations (bunkering, stores, etc.).

Role: authorising/regulatory

While numerous government agencies may intervene either directly or indirectly in the international container transport chain, the main oversight role typically falls onto Customs authorities.

The primacy of Customs in container transport can be easily understood given the hybrid nature of the system. While containers may be transported on or in different types of vehicles and modes (typically the realm of Transport authorities), the container itself is just a recipient for the goods it contains – goods whose control falls under the jurisdiction of Customs. Customs authorities are responsible for establishing national sovereignty over goods when they enter a country, for relinquishing sovereignty when goods exit a country, for collecting revenue generated by international imports and for protecting a country against dangerous and/or illegal imports.

Transport authorities also have a role to play (albeit an indirect one) in the oversight of the international container transport chain through the licensing of vehicles, vehicle operators, and transportation companies. In parallel, ship registers play a role in ensuring that their vessels comply with all international rules relating to maritime transport – including those related to security.

Role: financing

Banks play an integral role in the secure financing of international trade. They facilitate payment between importing and exporting parties once certain documentary requirements regarding a transaction have been made available. In particular, banks ensure the smooth operation of the documentary credit process that allows for successful and secure business transactions between parties in different countries that do not necessarily know each other (see Chapter 2, Section 2).

Flows in the container transport chain

Physical Flows

The first and most obvious flow is that concerning the physical movement of the container and its contents from place to place and from mode to mode. This is the most tangible flow from a security perspective. Knowing where a shipment originated, how it has travelled, where it can be found and whether its integrity has been compromised are key questions for security agencies intent on intercepting threatening cargo. As such, it is important for policy-makers to also be aware of the physical reality of the container logistics chain.

As containers move along the container transport chain they can be in any one of three states:

- They can be empty (in which case they are most likely being repositioned for a new voyage).
- They can be loaded with one single consignment from one single shipper (Full container load or FCL).
- They can be loaded with multiple consignments each from a different shipper (Less-than-full container load or LCL).

While it is feasible that an empty container could be used to transport a CBRN weapon, this is not very likely – principally because these containers are not delivered in any predictable manner and therefore any attempt to target the delivery of a weapon would be extremely difficult. However, empty containers could potentially be used to smuggle materials needed to support terrorist operations. This would not be a risk-free task from the terrorist's perspective as empty containers are often inspected for damage, can be sent for repair and are visually checked for proper condition before they are sent out in use again. There are more risk-free options available for terrorists and it is likely that they would use these (*e.g.* legitimately shipping the necessary components) rather than attempting to smuggle materials via containers.

Finally, there is no single "standard" pathway for containers to move through these nodes and links. The interactions between the various parties cited earlier, unique geographical situations and the multitude of possible commercial and contractual obligations governing container moves give rise to any number of possible transport chains. Generally, however, the network of nodes and links involved in containerised transport can be categorised according to their principal function. These are fourfold:

- Consignment assembly.
- Consignment consolidation.
- Carriage (either local drayage or longer-distance transport).
- Port handling.

These functions are not necessarily sequential – for instance, carriage can occur at many points along the network and consignment consolidation can occur during the port handling process. For illustrative purposes, however, these will each be described below in reference to the following simplified figure representing the container transport chain.

Consignment assembly

This first stage in the physical movement of goods occurs well downstream of the actual start of the commercial transaction giving rise to the container shipment. Beforehand, a buyer and seller will have identified each other, agreed on terms of sale and formalised these through a contract and will have agreed on the manner in which the goods will be shipped. At that point, the actual physical movement of the good(s) will commence.

In most FCL moves, an empty container will be dispatched from an empty container depot to the shipper's premises.[19] Here, the container will be stuffed, the doors shut and a seal affixed. While the shipper premises will most likely be a manufacturing plant or a warehouse – it really could be anywhere. Anecdotal evidence indicates that in some countries, it is not uncommon for containers to be stuffed directly in open courtyards or in the street.

The specific stuffing location is paramount from a security perspective because it represents the last point in the container transport chain where the physical contents of the container can be visually identified and reconciled with the commercial invoice and/or bill of lading. After the doors are shut and sealed and until they are re-opened by Customs or by the consignee at the final destination, all information regarding the contents of the container (*e.g.* such as the export declaration, manifest, the bill of lading and even the commercial invoice) are necessarily unverified. Thus the originating shipper has a critical role to play in the container security by generating a clear, accurate and complete inventory of the physical contents of the container. Proper site security, stuffing procedures and oversight of the stuffing process are necessary for this important link in the chain to be secure.

In many LCL moves, the shipper will assemble the consignment and arrange for it to be delivered as palletised loads to a consolidation centre where actual stuffing will take place. From a security perspective, the initial move of a palletised load onwards to a container stuffing centre may generally be regarded as a less risky operation since the goods loaded onto the palette are easily visible during the move.

Consignment consolidation

The next step in most LCL loads is a freight consolidation facility. These come in various forms and sizes ranging from small freight forwarder warehouses to large, multi-function Container Freight Stations (CFS). Whereas the former may operate with a small network of local clients, the latter may serve thousands of shippers located in an extremely large hinterland. The latter will typically provide several types of value-added logistics activities beyond the simple bundling of consignments, documentary and stuffing/stripping services offered by smaller warehouses. Many consolidation facilities also serve as in-transit consignment/container handling facilities. In these cases, the facility is managed by a bonded operator who can store and/or process consignments without the latter being officially "entered" (for administrative purposes) by the national customs authority.

Just as with the FCL case outlined above, the moment at which the LCL container's doors are shut and sealed by the consolidator is the last point in the container transport chain where the contents of the container can be physically reconciled with the container inventory documents. Accordingly, attention should be paid to consolidation centre site security, stuffing procedures and oversight of the stuffing process. However, consolidation centres pose an additional security challenge in that the operator of the centre is not usually a primary party to the commercial transaction giving rise to the movement of the goods. The consolidation centre thus represents real break in the container's chain of custody and a potential break in the ultimate traceability of the originating shipper's identity.

Carriage

Inland transport of containers involves both links (infrastructure) and nodes (handling centres). The actual physical movement of the container involves the transit from shipper to port (typical for FCL consignments), shipper to consolidation centre (for LCL and some FCL consignments) and/or consolidation centre to port (again, for LCL and some FCL consignments). These transit legs nearly always commence by road and may be single mode (usually road) or include multi-modal moves (involving road and rail or inland waterway).

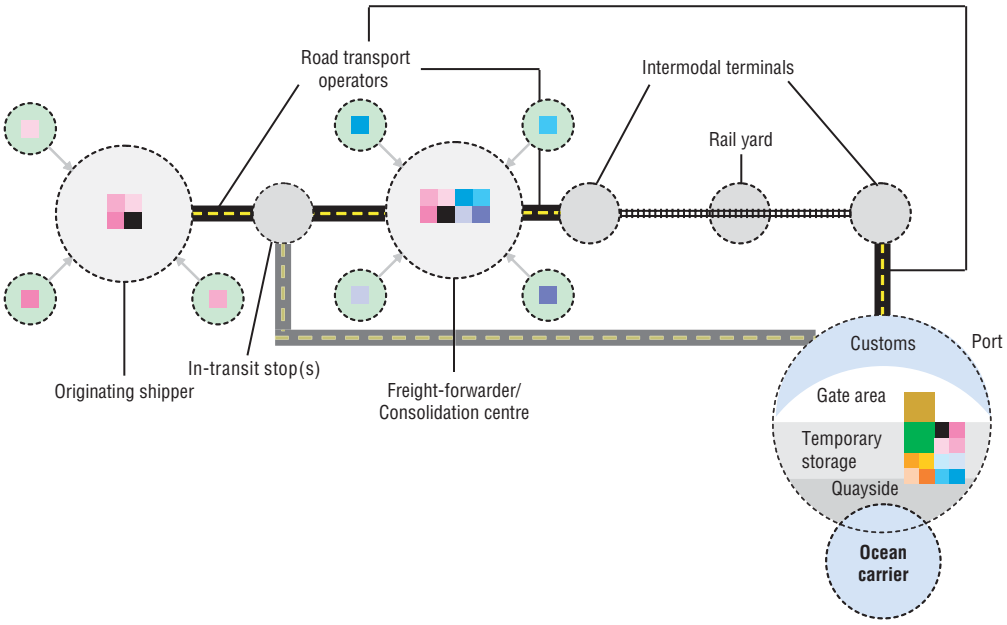
Each mode operates on its own infrastructure (roadway, railway and/or navigable waterways). These links are typically open and easily accessible – there are no fences surrounding most roads, rail tracks and/or waterways. However, the risk of intercepting and/or tampering with a container in movement is relatively low. This risk increases when the container slows and/or stops. Accordingly, most modal/intermodal container handling terminals have some form of security (*e.g.*, in the case of rail switching/staging yards, river container terminals or road-rail interchanges). However, the level of physical security offered varies widely according to mode, operator, location and/or type of goods being handled. Furthermore, not all stops in the container transport chain occur within a dedicated facility. This is especially true in the case of long-distance road transport where the container may be stationary and accessible in open roadside areas while the driver rests.

Intermodal container transport

Intermodal carriage of containers consists of the following operations (Figure A.5):

- Pick-up or initial road leg: transport of containers from the shipper's or forwarder's freight centre to the combined transport terminal.
- Terminal transfer: transfer from road to rail mode in departure terminal.
- Transport by rail: long distance rail transport.
- Terminal transfer: Transfer from rail to road vehicle in arrival terminal.
- Transport by road to the port of the exporting country.
- Departure port terminal: Customs clearance, temporary storage, loading on container vessels.
- Transport by sea.
- Arrival port terminal: Unloading on container vessels, customs clearance, temporary storage.

Figure A.5. **Carriage of containers – Intermodal transport chain**



- Inland transport process in the importing country similar to the one described above.
- Delivery or terminal road leg: transport from arrival terminal to receiver.

Combined transport can take a variety of forms: rolling roads, which allow full road vehicles to be carried on trains comprising low-floor wagons; roll-on-roll-off (Ro-Ro), which enables road vehicles, a wagon or an intermodal transport unit to load and unload straight on or off a vessel; and lift-on-lift off (Lo-Lo), which involves lifting equipment to load and unload transport units on or off a vessel. Containers may be handled and transferred by simple equipment such as a crane at inland intermodal facilities or port terminals. Containers may be interchanged not only among the different modes but also among carriers of the same mode to optimise the operation depending on the destinations. Standardised containers enable cargo to be quickly handled and transferred from ships to trucks and rail wagons with mechanical handling equipment.

Once the container is stuffed and sealed and enters into intermodal transport flow, transport carriers and those physically handling the container do not physically verify the container contents against the commercial documents or bills of lading.

At every interchange point container movements have to be slowed down or stopped for temporary storage. Inefficient transfer creates breaks in the intermodal transit of containers, which can cause higher risk of tampering. Therefore it is important to improve routing operation with fewer stops, to reduce interim storage, to promote interoperability and continuity by reducing differences in locomotives, signalling and electrical systems, and to promote efficient transfer of loading units between road vehicles and rail wagons. Such measures will not only enhance security but also offer economic benefits of more efficient transport and trade.

Container transport by road and border crossings

Road transport is usually involved in either door-to-door, long-distance haulage or during the first/middle/final legs of intermodal carriage. For distances of over 600 km, which a driver can cover in one shift (*i.e.* approximately 8 hours) road transport carriers have either to change drivers doing the journey, break the journey for at least 8 hours, or employ and pay a second driver to take over from the other one.[20]

When road hauliers cross national borders, often the case – particularly in Europe, the haulier presents to border authorities for verification documents containing information on the type and quantity of goods being transported, their origin and destination, and guarantees relating to the import duties or taxes, often a TIR carnet: Among these procedures are more specifically:

- Normal customs formalities (checking of documents, certificates, import/export permits, seals).
- Detailed customs controls (product origin, destination, quantity, value, payment of duties and taxes, inspection of goods, sampling).
- Checking for health and product safety (veterinary and phytosanitary inspections).
- Quality inspection of perishable goods and inspection of dangerous substances.
- Other checking of goods (import and export embargoes, etc.).
- Value-added tax.
- Other taxes.

Vehicles are subjected to a range of procedures, relating to required documentation and licensing, safety and emissions standards, and the many possible taxes and fees payable. Among possible procedures relating to vehicles are:

- Transport authorisations (bilateral, ECMT, etc.).
- Payments for special permits.
- Provision concerning working and driving hours.
- Driving license.
- Vehicle certificate.
- Road worthiness of vehicles and recognition of vehicle licensing.
- Checking of compliance with ADR (European Agreement Concerning the International Carriage of Dangerous Goods by Road) provisions.
- Customs security of transport vehicles.

There are also border controls focusing on the personnel transporting the freight. These include passport and visa verifications, driver's licence control, among others. Extra delays may be caused if visas have to be purchased at the border, or if the vehicles are searched for illegal immigrants.[21]

To the extent that more detailed verification of the vehicle, its contents or identification of its driver are determined to be necessary, the delays at border crossings will be substantially longer.

It should be noted that risk of theft or hijacking of commercial vehicles during road carriage is significant. The percentage change for commercial vehicle thefts over the five-year period between 1995 and 1999 increased in nine out of 11 countries which replied to a 1998 ECMT survey. The average overall increase for the nine countries was 20% over the five-year period.[22]

Container transport by rail

As regards rail transport, containers are carried for a long distance, often across borders particularly in Europe. Freight trains fall into three categories:[23]

- Trainload (or block trains), where a complete train (usually of one type of goods) goes from origin to destination without any re-marshalling on the way.
- Wagonload, where wagons are loaded by different senders at different points and forwarded in ones or two's for different destinations. In the traditional way they may be shunted two or three times during the journey, and will form part of different trains at different stages of their journey. Shunting is a time-consuming process, necessitating very costly marshalling yards, and leading to long journey times.
- A combination of the two (consolidated wagonload) where wagonload traffic is marshalled into a train at as early a stage as possible, and is then run as a full train as far as possible before being split up for final delivery. Where it is necessary to remove or add wagons on the way this is done by adding or removing a block of wagons according to a pre-arranged schedule at a point fixed in advance. The principal sections of the journey are therefore covered without disruption in the manner of a full train. Stops for attaching/detaching are reduced to a minimum and the facilities required for attaching/detaching are reduced to one or two sidings. The benefit is much lower costs and shorter journey times. EurailCargo is an international example of this type of service.

For international rail services, though there are some exceptions, freight trains in general change locomotives and train crew at borders. Locomotives are routinely changed because of technical incompatibility of signalling and electrical systems or lack of personnel qualification for cross-border operation. Changing locomotives and crew involves the risk of delays in scheduling and costs associated with sending locomotives and crews to border-points to await trains, as well as infrastructure to be provided to accommodate the operation.

Container transport by inland waterway

Inland waterway transport mainly involves the carriage of sea containers from and to ports and their hinterland. Container barge operations have to be intermodal, as road and/or rail is always necessary to carry them from and to the hinterland.

The Rhine and the Danube have substantial container transport capacity in Europe, which is determined by the bridge clearances and the width of locks. Since Ro-Ro ships are of limited efficiency over long distances, inland waterway transport primarily uses lift-on/lift-off stackable sea containers. On the Rhine, containers can be stacked four layers-high on a vessel, and four containers each of 2 440 mm can be stowed side-by-side on a Rhine barge. A barge operating on the Rhine can thus easily carry more than 100 TEU, *i.e.* the capacity of two block trains. On the canal and tributary network, bridge clearances are considerably lower so that a vessel can carry only two layers of containers, *i.e.* half its capacity.[24]

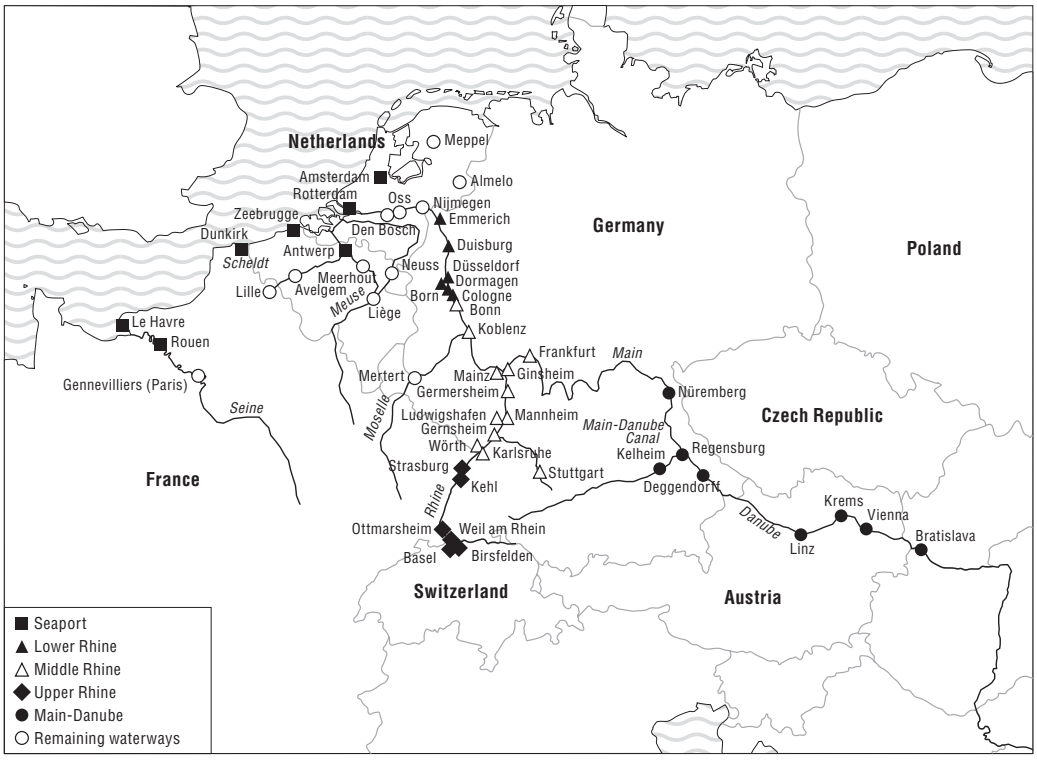
Speed and carriage capacity are being improved in new fleet. Whereas in 1980 mostly 90 TEU ships sailed, 200 TEU ships and motor vessel/pushbarge combination with a capacity of 350 TEU are increasingly being introduced. The inland container ships are suitable for all occurring containers, including deviant sizes, reefer containers, as well as containers with dangerous substances.[25]

Numerous inland port terminals have been established along the waterways (Figure A.6). These terminals are equipped with loading/unloading equipment, maintenance services and road and rail connections to forward the containers to their final destinations.

Major structural changes in the European inland waterway network in recent years include the following:[26]

- In the Rhine Basin, the large barge operators have started to centralise the river-linked container flows in only a few terminals.
- The number of barge terminals in the Rhine basin, however, is still increasing as new operators try to enter the market. The growing awareness of the potential for inland navigation in recent years has also led to the emergence of new intermodal river ports outside the Rhine Basin.
- A substantial number of container barge operators have extended their logistic services to their customers by offering door-to-door transport. The inland terminals function as key nodes in their logistic strategy. For instance, Rhenania Intermodal Transport operates a logistic network built around its five container terminals along the Rhine. As such, a large number of the European river container terminals have become real logistic centres with tri-modal facilities.

Figure A.6. **Location of container barge terminals in the European inland waterway network**



Source: ECMT 2001, *Land Access to Sea Ports*, Round Table 113.

Port handling

Ports represent one of the principal chokepoints in the international container transport chain. As noted earlier, some containers involved in international trade do not voyage by sea and thus do not pass through ports, but most do. The area under the control of a single port authority is typically comprised of a number of dedicated terminals and cargo handling facilities. In addition, many ports harbour other trade-related activities such as multi-modal transfer centres, warehouses, container freight stations, logistics service providers etc. Ports also house some of the trade-related regulatory authorities – such as customs. Finally, while ports are normally associated with a waterfront, tight space constraints have led many ports to develop and/or use inland container depots where many of the main container handling tasks (such as container stacking and staging and customs processing) can be carried out away from the quayside.

Container handling terminals are not usually open areas – access is restricted and the perimeter is usually fenced-in. In order to prevent cargo theft, many terminals have put in place more advanced security systems and procedures that include security patrols, closed-circuit television surveillance, automated intrusion detection systems, etc. However, it is not uncommon for smaller ports to have in place only basic security measures that can be easily bypassed.

Entry into the terminal is usually granted through a gate area where a number of essential functions are concentrated. Here, information on the container, the consignment and the driver (in the case of truck-borne containers) are checked against the booking

information provided by the carrier or his agent. Once the information is checked and cleared, the container is allowed into the port terminal and is unloaded from the truck in a first buffer area. In the case of rail and barge consignments, the gate functions are carried out within dedicated facilities within the container terminal.

After the container is checked in at the gate or at the first buffer area, subsequent container moves are controlled by a container yard management system.[27] This software/hardware system controls where the container is stacked, where it is moved within the yard (including to Customs inspection sites), when and where containers are loaded/unloaded/transhipped, and where on the vessel the container is placed. There are a number of commercial systems on the market that allow either intermittent or real-time tracking of containers. The container is moved from the initial truck/rail/barge buffer area to an outgoing buffer zone where it is stacked with other containers destined for a particular sailing. This outgoing buffer is doubled by an "incoming" buffer zone where containers are unloaded from vessels. Containers are picked from the outgoing buffer and placed onto the vessel according to a pre-determined plan that accounts for further loadings/unloadings and transhipment.[28] The plan also dictates which containers are placed above deck and which are placed below deck according to specific handling directions included in the booking order. The actual loading is supervised by a land-side crane operator and a ship-board stevedore who visually confirm the container number and its physical location on the vessel. Once the vessel is loaded, these systems communicate the loading plan (the "Bay plan") to the next port along with any particular information required for further handling – and in particular, the location of containers carrying hazardous cargoes.[29]

The actual physical handling of the container within the container terminal is carried out by a number of cranes, vehicles and other machinery. Smaller ports tend to operate individual container stacking vehicles ("toplifts", "sidepickers", "reach stackers" and/or "straddle carriers") that stack/unstack containers and manned delivery vehicles that move the latter to the quayside. In larger ports, one tends to find larger gantry cranes (either manned or automatic) that pass over container stacks in order to pick and place containers onto delivery vehicles. In the largest ports, the latter tend to be unmanned automated guided vehicles (AGV's) whose movements are controlled by the container yard management system under supervision from a central "control tower" facility. Finally, quayside cranes vary in sophistication from simple swing units to more sophisticated straddle arm units that extend over the entire vessel bay.

Given that it is extremely difficult to tamper with a container once loaded, the quayside crane represents the last physical checkpoint before the container is dispatched to another country. As such, they represent an important security "chokepoint". In 2003, there were an estimated 3 183 quayside gantry cranes in operation worldwide.[30]

The logistics chain described above is not uniformly secure and the level of protection offered to containers and their contents can vary tremendously from node to node and among modes. The risk of a security breach at any one of its links can compromise the security of the entire chain and imposes additional costs as additional security checks must be put in place to compensate. Also, the level of protection present at different nodes and in transit is often directly related to the value of the goods being shipped. A major electronics manufacturer will invest much more in securing his/her supply chain than will a small low-volume exporter of inexpensive porcelain objects. And even in cases where

relatively high levels of protection are put in place, cargo theft remains a problem. There are literally tens of thousands "entry points" along modern logistics chains that could be exploited by terrorist groups.

Information flows

International trade requires that buyers and sellers – oftentimes completely unknown to each other – be able to conduct business, negotiate contract terms and ensure secure payment across international and jurisdictional lines. These requirements have given rise to a number of international rules and standards, business "languages" and trade procedures that facilitate the movement of goods among commercial partners. All of these are "information-heavy" since it is these exchanges that instil mutual trust among trading partners and replace "face-to-face" business relationships.

The information traded among the actors ensures that the container is quickly and accurately dispatched from shipper to final consignee, that the consignment meets regulatory requirements and adheres to the terms of the commercial contract between buyer and seller. Accordingly, the flow of information in the container transport system can be broken down into three principal categories covering information relating to: *a)* trade contracts; *b)* regulatory compliance; and *c)* operational details. These categories are not mutually exclusive and in some cases they may overlap. One of the principal documents covering container movements – the Bill of Lading – can be both an operational document (it states how the consignment is to be shipped) as well as a commercial one (it serves as a contract of carriage *and* can convey title to the goods shipped). Nonetheless, these information flow components will be discussed separately so as to isolate security-relevant issues.

Information/documentation relating to trade contracts

International trade documentation revolves around four principal types of contracts. These serve to establish the trading relationship between the commercial partners, define the terms of the transaction, its payment and its consignment, and to allocate responsibility for loss among the parties involved. The scope of these, the actors involved and the applicable rules are outlined below:

Table A.4. **Types of contracts**

Scope	Contract name	Parties involved	Applicable laws/rules
Sale	Invoice	Seller (shipper) and buyer (consignee)	INCOTERMS 2000
Finance	Letter of credit	Bank and buyer transferring to seller	UCP500 and eUCP (where applicable)
Carriage	Bill of Lading or Waybill	Carrier and seller transferring to buyer	Hague/Hague-Visby rules or Hamburg rules
Indemnity	Insurance certificate	Insurer(s) and seller and/or buyer	Marine Insurance Act of 1906

Source: Based on P&O Nedloyd, 2003.

Sales contracts (purchase order, invoice, etc.)

These documents establish the terms of the trade. They identify buyer and seller, identify the goods to be traded, their characteristics, their quantity, their prices and the manner in which responsibility for covering consignment-related costs (principally carriage, insurance and liability) are to be allocated. Typically, a first-time trading relationship initiates when a buyer sends a sales inquiry to a seller. The seller responds by sending a detailed

pro forma invoice detailing the terms of the trade. As its name suggests, this is not a binding document but is used by the buyer for making a decision on the transaction and for beginning to arrange the financing and import clearance of the sale. In established trading relationships, the *pro forma* invoice might be replaced by a simple summary quote establishing price and terms. While currently not involved in the security screening process for import goods, the *pro forma* invoice is the first document to emerge in the trading process that provides details on the future consignment and the parties (at least the buyer and seller) involved. After acceptation of the terms set out in the *pro forma* invoice, a formal sales contract or commercial invoice is established on the basis of the information in the *pro forma* invoice. As will be seen further on, a number of data elements outlined in the table below will also be required later on for customs screening and clearing.

Table A.5. **Information typically included in *pro forma* invoices and sales contracts**

Buyer's name and address	Seller's name and address	Buyer's reference number and date of inquiry	Listing of requested products and brief description
Price of each item	Gross and net shipping weight	Total cubic volume and dimensions packed for export	Trade discount, if applicable
Delivery point	Terms of sale	Terms of payment	Insurance and shipping costs
Validity period for quotation	Total charges to be paid by customer	Estimated shipping date and location	Estimated date of shipment arrival

One of the key elements of both the *pro forma* invoice and actual sales contract is the specification of the trading terms agreed upon by both parties. These are codified internationally within the 13 INCOTERMS 2000 rules established by the International Chamber of Commerce (ICC). They are designed to transfer risk from buyer to seller at a mutually agreeable and convenient point in the transport chain (*e.g.* when the container is loaded onto a vessel, or handed to a carrier at an inland CFS, or delivered to a consignee, etc.) They also establish which parties will organise/pay for the different legs of the container transport chain. From a security perspective the relevant INCOTERM of a trade is important in understanding who has oversight over a particular leg of the container transport chain. For instance, it makes little sense to go to a seller for information about a consignment shipped EXW (that is, where the buyer assumes all responsibility for the goods and its transport as soon as the container leaves the seller's premises).

Letter of credit/documentary credit

This contract guides the financial settlement of the trading process. While it is closely linked to the contract of sale, it is a separate contract between slightly different parties and bound by a different set of rules. The parties involved are the seller, the buyer and one (or several) banks under the ICC's Uniform Customs and Practice for Documentary Credits: ICC Brochure 500 (UCP500). The bank(s) typically require a paper-based transaction where *control of the goods is at some point transferred to the bank* (often via a document of title such as the Bill of Lading) as collateral for payment. However, the bank is not a party to the contract of carriage (see below) that may also be the document of title. The contracting bank acts as an agent for the buyer and will pay the seller (either directly or through a partner bank in the seller's country) for the goods against the presentation of documents complying with the sales contract. These documents are required to ensure that the terms of the contract were carried out and typically include a commercial invoice and packing

list, a certificate of origin, a full set of Bills of Lading (either made to order – that is to the party the seller designates – or to consignee), an insurance certificate and possibly a set of export clearance documents if required. The payment cycle is triggered upon acceptance by the contracting bank (or its partner) of the documentary packet. Sellers are often, therefore, eager to ensure that this information is gathered and transmitted as early as possible – in some cases, the *pro forma* invoice will even be used to initiate the documentary credit process. Thus, as with the case of the *pro forma* invoice, a significant quantity of security-relevant data is produced early on in the trading process – but not necessarily evaluated in the security screening process.

The contract of carriage: Bill of Lading

The Bill of Lading[31] has three functions:

1. As a receipt by the carrier to the seller/shipper for the consignment.
2. As a contract of carriage.
3. As a (sometimes transferable) document of title.

The first two functions require detailed information regarding the consignment. This includes the identity of the seller/shipper, description of the goods being shipped, number and type of packages and pick-up/drop-off locations. The document of title function requires perhaps a bit more explanation. In essence, the Bill of Lading is to goods what a cheque is to money where the carrier acts as the "bank" and the shipper/seller acts as the issuing account holder. The party to whom the Bill of Lading is endorsed can exchange the document for the goods much as the bearer of a cheque can receive payment in return for a cheque made to his/her name. These "straight" bills of lading are made out directly to a named party (usually the consignee). However, Bills of Lading can also be transferable documents. In these cases, the Bill is made "to order" (that is, the shipper will designate to whom the Bill should be made at some point in the transaction), "to the order of" (where the named party will designate to whom the Bill should be made) or "to bearer" (where the goods are to be turned over to the party physically holding the Bill – much like a blank cheque).[32, 33]

These distinctions are important from a security perspective since they predicate the relative transparency of the identity of the seller/shipper, buyer/consignee and controlling agent (the party that designates to whom the goods should be released). For instance, the security assessment of a Bill made "to bearer" is rendered extremely difficult since the identity of the consignee is only known when the party physically presents the Bill in exchange for the goods. Likewise, a bill made "to the order of" can potentially mask both the originating shipper and the final consignee.

A further complicating factor is introduced when a freight forwarder or NVOCC enters the picture. As pointed out earlier, these intermediaries often act as "Carriers" even if they only serve to organise the carriage of the goods in question. This means that they issue Bills of Lading to their clients for each individual consignment they collect (House Bills of Lading) in which the forwarder appears as the carrier and the originating shipper as the shipper *and* they appear as shippers on the consolidated Bills of Lading (Master Bills of Lading) they receive from the actual carrier. Any summary security assessment of the parties on such a Master Bill of Lading is rendered extremely difficult insofar as the originating shippers are completely masked.

Nonetheless, many traders feel that both the possibility for forwarders to issue Bills of Lading as well as the negotiability of these Bills remain essential functions in international trade – particularly as they allow for the proper functioning of the documentary credit process outlined above. This is especially true for trade with developing countries where the documentary credit process remains the principal (and in many cases, the only) way in which to protect both buyer and seller from fraudulent non-payment.[34]

Finally, Bills of Lading have been a sometimes unsatisfactory source of information on the contents of the container. In order to understand why this is, one must understand the carrier's legal exposure *vis-à-vis* this document. Once the carrier has issued a Bill of Lading, he/she is legally bound to its contents and terms. This means that the carrier is implicitly accepting the accuracy of all of the Bill's details once it is issued. A carrier who knowingly puts incorrect details on the Bill of Lading may be pursued for fraud. In most cases, however, the *carrier has no first-hand knowledge* of the contents of the container. The carrier must accept the shippers' word as to the type of goods being shipped and their count (a carrier can check weight). In the cases where the shipper is in fact a forwarder handling a FCL shipment for the originating shipper, the named shipper on the Bill of Lading (in this case the forwarder) may not have first-hand knowledge of the contents of the container. Thus, carriers have in the past had recourse to vague or unspecified goods descriptions on Bills of Lading such as "freight all kinds", "said to contain" or "shippers load and count".

The first iterations of the United States "24-Hour rule" (relating to the mandatory advance notification of the contents of a container bound for the United States) dis-allowed these terms for US trades, thus placing carriers in a bind *vis-à-vis* their liability exposure for the boxes they carried but did not stuff. In a subsequent rule-making on the "24-Hour rule", carriers were allowed to retain the clause "Shipper's Load and Count" (added immediately beneath the detailed shipper-provided cargo listing on the Bill of Lading) so as to protect themselves under current liability regimes. Further tightening of Bill of Lading freight descriptions beyond those imposed on the US trades should similarly address carriers' liability exposure relating to Bill of Lading cargo descriptions.

Insurance certificate

The Contract of Carriage informs, but is not, the Contract of indemnity. This function is carried out by the Insurance Certificate, itself linked to a more general Insurance Policy held by the exporter/importer. Depending on INCOTERM in effect for the particular transaction, either the exporter or importer may be obliged to provide proof of insurance (*e.g.* in CIF and CIP terms). However, in some instances, either party may decide to forego cargo insurance and accept the risk of loss. Typically however, the Documentary Credit process requires some proof of insurance and this is a common component of the documentary package presented to banks in the process.

Insurance Policies may be either specific or open. In the former case, insurance is subscribed for a particular case – typically one voyage. In the latter, however, the policy is issued by the Insurer to cover all shipments over a set time period – typically a year. In this instance, the policy holder is required to provide the Insurer with a periodic (typically monthly) listing of all shipments, the carriers involved as well the destinations.

From a security perspective, it is important to keep in mind that insurance providers have sometimes extensive knowledge of both their policy holders and their shipment histories and patterns. As this information is closely linked to the potential risk exposure of the policy holders, one might assume that this is a fairly accurate source of information.

Information required for regulatory compliance

As seen earlier, governments are involved at various levels in the international trading process. In order for traders to ensure compliance with regulatory requirements, specific information must be made available to government agencies before the consignment is cleared either for export or for import.

Information provided to Customs authorities

The principal recipients of trade information on the government side are Customs authorities. They require information from traders in order to fulfil their multiple responsibilities that include import/export control, tariff collection and enforcing regulatory compliance. The latter responsibility covers a wide range of areas and includes ensuring compliance with national criminal laws (*e.g.*, regarding drug and contraband smuggling), carrying out national defence tasks (*e.g.*, securing the country from terrorist misuse of commercial trade) and enforcing international treaties. In the process of carrying out these multiple roles, Customs authorities will require parties to a transaction to provide detailed information regarding the consignment. Most of this information, on the importing Customs side, will be derived from the Bills of Lading, associated manifests and commercial invoices. The degree to which Customs authorities can exercise effective security screening of consignments will depend on the quality of the information with which they are provided. Insofar as these documents/data sources mask the identity of some of the parties involved or are otherwise vague (*e.g.*, originating shipper not identified, final consignee/receiver of goods not identified, buyer and/or seller masked, generic manifest data, etc.), Customs control will be compromised.

Another issue regarding the role of Customs authorities in processing trade data for security purposes is the matter of timing. Historically, Customs authorities withheld the release of goods until all documents were submitted and payments made. In many, if not most cases, documents traveled more slowly than the goods themselves and thus Customs would store goods in their own or external bonded warehouses until the documentary requirements were fulfilled. This posed obvious problems for both Customs authorities (lack of space) and importers (long delays) and thus there has been a general move to allow goods to be entered within countries before the documentary cycle is completed and payment received – or at a minimum, to allow goods to be entered into countries with a provision allowing for shipping documents to be updated and corrected after the goods are released to the consignee. In many instances, this has meant that containers have been released before final descriptions of their contents have been made available to Customs. This has important security repercussions and several Customs administrations are now enforcing stricter compliance with documentary requirements before goods are released to the consignee and/or are allowed to reach the border.

The moment at which Customs authorities receive information on a consignment is important from a security perspective. Traditionally, Customs authorities have exercised their control at national points of entry (*e.g.*, border posts, ports, airports, etc.). This was generally regarded as a satisfactory situation since Customs could intercept illegal and/or non-compliant consignments before they "entered" (in an administrative sense) the country. Since Customs depend heavily on the Bill of Lading for their screening needs, it is the carrier operating the final leg of the international voyage that generally transmits this information to Customs. In many cases, this information was not known by the carrier

until after the vessel was loaded and thus the transmission to Customs in the importing country took place once the vessel was on its way. Following the September 11th attacks in the United States and under the perceived threat of CBRN weapons, US Customs rightly pointed out that if once a CBRN weapon-containing container is en-route to a port of entry, it is too late for effective Customs control. Thus, the United States has implemented new advanced notification guidelines, requiring that US Customs receive detailed information about the contents of a US-bound (either for import or for transshipment) before the container is loaded on the vessel at the last port of call. Similar provisions, albeit with different timelines, have been put in place for other modes of transport (see Annex II on the US Advance Manifest Rule or "24-hour rule") and have been envisioned for the European Union.

Customs do not only exercise their control on the importing side, they also have responsibility to ensure compliance with export regulations. Historically, however, Customs have focused more on imports than on exports. Most countries have in place some form of export licensing that enables national governments to exercise control over the types of goods that leave the country. Many of these systems have been simplified and generally include an "automatic" class of export licenses for a large category of goods alongside a more restrictive licensing process for exports the government wishes to monitor and/or control. In the latter case, detailed information must be provided to the exporting Customs administration and/or Trade administration relatively early on in the trading cycle. Given that many of the items requiring export licensing are items that governments would not want falling into the hands of terrorist organisations (*e.g.* weapons, weapons-manufacturing technology, chemical pre-cursers, radioactive materials, etc.), early access to this information in the importing country would allow for more effective security screening.

The TIR[35] Carnet is an internationally accepted Customs transit document facilitating international trade, which accompanies goods transported from Customs offices of departure to customs offices of destination under the TIR procedure. The TIR Carnet is currently paper-based and centrally printed and distributed to national associations by The International Road Transport Union (IRU). The TIR Carnet can reduce the risk of pressing inaccurate information to customs administrations as well as the time for customs transit by simplifying the procedure.

The Customs office of departure checks the load on the basis of information supplied in the TIR Carnet (goods manifest) completed by the transport operator. Customs seals the load compartment, reports it in the TIR Carnet. The TIR Carnet is handed back to the transport operator, who starts the transport operation. When crossing the outgoing border of that country, Customs checks the seals, and fills-in the corresponding counterfoil of the TIR Carnet. This process is repeated until the goods reach the Customs of destination. If the customs office suspects fraud, finds seals faulty or fears the TIR Carnet has been tampered with, it will check the goods and it may interrupt the TIR operation.

Each individual TIR carnet can be used for one TIR transport. Once the TIR operation has been terminated at the Customs office of destination of the goods, the driver is handed back the TIR carnet duly endorsed by the Customs authorities of destination and may proceed with the goods' delivery. The TIR carnet is returned to the IRU for control and archiving.[36]

Other information provided to Governments

Various other branches of government require information regarding international imports and exports. Unlike Customs information, however, there are no generalised international requirements that are applicable to all goods. Specific sanitary and/or veterinary information regarding certain exports of food, plant matter or animals may be required depending on the destination. Some countries still require consular invoices that must be obtained in the exporting country from the consulate of the destination country. Some countries and/or importers may require inspection certificates certifying that the goods being shipped are in conformity with the goods description in the commercial invoice. Most of these communication channels with governments are activated early on in the trading process and could, theoretically, serve as a useful compliment to more traditional Customs data. At present, however, these data streams are typically not very well integrated with Customs administrations (if at all) and are therefore not available for security screening of incoming goods.

Information pertaining to operational details

The actual physical movement of a container from actor to actor and from node to node in the container transport chain requires the transmission of numerous operational messages. These govern the sourcing of the empty container, its dispatch to a point of loading, its stuffing, its carriage by a transport operator, its hand-off to a different transport operator, its movement within different transport nodes (*e.g.* rail yards, ports, etc.), its passage at various checkpoints and its final delivery to a consignee and/or its stripping/emptying. The systems supporting the operational management of container moves are equally numerous. These include:

- In-house shipper/buyer inventory and order tracking systems.
- Shipment information systems.
- Security systems.
- Railcar planning systems.
- Motor carrier routing and dispatching systems.
- Customs clearance systems.
- Gate clearance systems.
- Container terminal management systems.
- Terminal inventory management systems.
- Asset location and management systems.
- Ship stowage management systems.

At present, the stream of data related to the movement of the container throughout the supply chain is neither harmonised in its content nor in the supporting media used to transmit this information. The latter include paper files, faxes, phone and oral messages, proprietary data networks and messaging standards, Internet-based systems and open messaging standards, etc. When looking at the entire container transport chain, lack of messaging interoperability is still the rule and not the exception.

However, it is important to note that this lack of interoperability is not uniform along the entire container transport chain. Incompatible message structures and messaging systems are most likely to be found at the outer bounds of the container transport chain,

especially among SMEs providing drayage services. On the other hand, considerable progress has been made to develop uniform messaging standards and systems for the core/central part of the transport chain covering forwarders, large land carriers, ports and maritime operators. Accordingly, when Customs have in place electronic filing systems, they are oriented mostly towards these actors, and not necessarily those in the container transport chains that are the first to have knowledge of a consignment or its initial movements (*e.g.* most small shippers and small road carriers). From a practical standpoint, this means that data submitted to Customs by the former are often re-keyed from data supplied by the latter – raising the possibility of re-transcription errors.

One of the principal explanations of the emergence of these interoperable systems at the "core" of the container transport chain has been the uptake of common Electronic Data Interchange[37] standards. These standards allow for the transmission of harmonised trade messages irrespective of computer platform. They are, in effect, common trade "languages" that allow different actors operating different systems to communicate amongst themselves regarding the movement of shipping containers. There are three broad categories of these trade "languages" or "syntaxes": EDIFACT (promoted by the United Nations), ANSI X12 (in use in the United States) and the emerging set of standards based on Internet XML (Extensible Mark-up Language) syntax.

EDIFACT and ANSI X12 have been the principal standards used for the transmission of international trade-related information. However, because of the relative complexity of their use and the need to pass through a paying third-party value-added network (VAN), rather than an open network such as the Internet, the use of these standards has been limited to large shippers and major actors in the container trade network[38] – thus explaining their use at the "core" (dominated by large actors) rather than at the outlying reaches of the container transport chain (dominated by SMEs). Because it is truly cross-platform and requires no VAN, Internet-based XML trade messaging will likely reduce costs linked to EDI implementation for SMEs. This has important security ramifications as harmonised container-related messaging among trade partners will also allow for earlier and more robust security management practices – especially through the creation of an electronic "audit-trail".

At present, efforts are underway to seek to harmonise these messaging standards in the International Standards Organization Technical Committee 204 and UNCEFACT Trade and Business Group (TBG) 3. The principal thrust of this work has been to develop E-Business MOU between the ISO, the UN-ECE, the International Telecommunications Union (ITU), and the International Electro-technical Commission. This agreement sets the foundation for more uniformity in electronic communications between all business elements on a global basis.

Financial flows

The financial flows supporting international trade operate primarily through some form of the documentary credit process. This process allows for banks to serve as neutral intermediaries in international transactions involving parties that may or may not know each other.

Notes

1. For instance, one 40-foot container (a very common size in the trans-Pacific trades) counts as two TEUs.
2. BIC, personal communication 2003.
3. World Shipping Council, 2003 ("Liner Shipping: Facts and Figures").
4. These numbers combine a four-character code identifying the owner of the container and a seven-digit code individually identifying the container.
5. ISL, 2003.
6. A notable exception is the case where the "shipper" is in fact a freight forwarder/consolidator that is only re-shipping a full container load for the originating shipper's account.
7. Also known as a Non Vessel-Operating Common Carrier in North America, or NVOCC, when they assume contractual responsibility for the transportation of cargo by issuing a Bill of Lading or other transport contract in their own name.
8. Data sources Observatory of European SMEs 2001 (p. 14) and 2002 and US Office of Trade and Economic Analysis "Export America 2001" and "Small and Medium sized Exporting Companies: a Statistical Profile" 1999 – These numbers most likely under-report the actual number of exporting firms since they also include freight forwarders and consolidators that assemble and export other firms' goods.
9. World Shipping Council, 2003 ("Liner Shipping Facts and Figures").
10. Calculated from the data "number of enterprises by employment size class in 1999" in Panorama of Transport, 2002, Eurostat.
11. Chapter 4 examines current measures specifically pertinent to improving container security. However, as is pointed out in Chapter 5, the permitting and licencing systems that make up the regulatory context for national and international road haulage may provide the points of greatest leverage for Transport authorities to mitigate security risks in road transport of containers. It should be noted that ECMT has examined the licensing and permitting criteria and processes for other aspects of road transport crime – notably theft of goods and goods vehicles, and transport of illegal drugs and illegal immigrants.
12. These criteria are set out in the ECMT Resolution adopted in Prague in 2000, and EU Directive 96/26 and 98/76.
13. Association of American Railroads, *www.aar.org*.
14. Trends in rail goods transport 1990-2001, Eurostat.
15. Inland Waterways Freight Transport in 1990-2001 in the European Union and the candidate countries, Eurostat.
16. ECMT 1998, Report on the *Current State of Combined Transport in Europe*.
17. Declaration adopted by Pan-European Conference on Inland Waterway Transport, Rotterdam, September 2001.
18. CCNR, *http://ccr-zkr.org/*.
19. In some cases, a FCL shipper may wish to use the services of a freight forwarder/NVOCC in order to enjoy more advantageous freight rates. In these cases the FCL shipper may ship full containers to the Consolidation centre rather than directly to the port.
20. ECMT 1998, *Report on the Current State of Combined Transport in Europe*.
21. ECMT 2000, *Integration of European Inland Transport Markets*.
22. ECMT 2002, *Crime in Road Freight Transport*.
23. ECMT 1998, *Report on the Current State of Combined Transport in Europe*.
24. *Ibid*.
25. ECMT 1999, *What Markets Are There For Transport By Inland Waterways?*, Round Table 108.
26. ECMT 2001, *Land Access to Sea Ports*, Round Table 113.
27. Some smaller, low volume ports still operate with paper-based systems.

28. In some cases, the loading/unloading operation may be carried out directly from the rail/truck chassis (or barge) to the vessel. Such "wheeled operations" principally concern ports operating in geographically constrained sites where land values are high.

29. According to IMO rules, the Carrier must also establish a Dangerous Cargo Manifest detailing the type and placement of hazardous cargoes on the vessel.

30. Inventory and estimates from Containerisation Yearbook, 2001.

31. The Marine Bill of Lading is a bill covering shipment by sea. The Bill of Lading is the most widely used form of contract of carriage for containerised shipments where at least one part of the door-to-door voyage is by sea (UNCTAD, 2003). Where not all of (but the majority of) the journey of the container is by sea, the carrier issues a Combined Transport Bill of Lading, which covers the full journey across modes of transport. Other transport documents, such as road and/or rail waybills, may be issued when the container does not travel by sea. It should be noted, however, that the importance to banks of negotiable Bills of Lading in the documentary credit process renders this form of contract extremely popular.

32. In keeping with the reality of today's multimodal transport chains, there has been a move to develop and use truly Multimodal Transport Documents. While initial efforts at creating such an instrument met with limited success, several operators now routinely issue these documents based on the UNCTAD/ICC Rules for Multimodal Transport Documents. The Multimodal Transport Operator issuing this document is the party assuming responsibility for the door-to-door carriage of the goods. Unlike single mode Bills of Lading, Multimodal Transport Documents have been structured in such a way as to facilitate their transmission via electronic means.

33. For inland transport, the road consignment note (road waybill) and the rail consignment note (rail waybill) are issued by the carriers. The consignment note is not a document of title, but serves as the evidence of the contract of carriage and the receipt of the goods by the carrier. The consignment note has a standard form in each transport mode, regulated respectively by the Convention on the Contract for International Carriage of Goods by Road (CMR, 1956) and by the Uniform Rules concerning the Contract for International Carriage of Goods by Rail (CIM), part of the Convention concerning International Carriage by Rail (COTIF, 1980).

34. In some cases, a transport document that limits itself to the first two functions of the Bill of Lading may be used. Known as "waybills", these are often used in cases of intra-firm trade or in cases where alternative secure payment arrangements have been made. Because it is not a document of title, there is no need for the actual paper document to be transmitted from one party to another. Further uptake of the waybill as the principal contract of carriage would likely lead to more electronic transmission of carriage-related information among trading parties.

35. See also Annex B.

36. UN-ECE, TIR Handbook and IRU Website *www.iru.org/TIR/TirSystem.E.htm*.

37. Electronic data Interchange (EDI) can be defined as: "The automated, electronic exchange of standardised, structured and normalised messages from computer to computer between different organisations in commercial or administrative transactions" (UN, 1993).

38. For instance, it has been estimated that 95% of the Fortune 1000 companies use some form of VAN-based EDI, whereas only 2% of SMEs do so – and in many cases only because their business partners have imposed its use (Virtuele Haven, Messaging: State of the Art EDI XML, 2001).

ANNEX B

International, National and Industry Container Security-Related Initiatives

International measures

International Maritime Organisation (IMO)

International Ship and Port Facility Security (ISPS) code

Sets out detailed security-related requirements relating to the security of the ship and the immediate ship/port interface. Adopted in December 2002, the ISPS Code establishes an international framework for co-operation among Governments and their agencies, local administrations, shipping companies and port authorities to detect security threats and take measures to prevent security incidents affecting ships or port facilities used in international trade. It is centred on the designation of security officers at the company, port and ship levels, the development of comprehensive ship and port security plans and the elaboration by port states of three security levels. Ship and Port security plans must specify increasingly stringent security measures to be implemented in each of the security levels. The ISPS enters into force on July 1, 2004 and non-compliance by either ports and/or vessels will preclude these from participating in international trade.

Other amendments to 1974 Safety of Life at Sea Convention (SOLAS)

Adopted in 2002 and effective 1 January 2004, these amendments rendered *inter alia* the International Maritime Dangerous Goods (IMDG) Code mandatory. The IMDG Code sets forth basic principles and offers detailed recommendations for the packing, marking, labelling and stowage of dangerous goods, as well as the necessary segregation and handling of substances, materials and articles and their transport by sea.

International Labour Organisation (ILO)

Seafarers' Identity Documents Convention (Revised) 2003

Adopted in 2003, this Convention revises the 1958 Convention of the same name. The objective of this revised convention is to improve the security of seafarers' identification, thereby heightening passenger and crew security and safety of ships while maintaining seafarers' necessary access to shore facilities/shore leave. The revised Convention specifies in particular guidelines for the composition and issuance of seafarers' identity documents.

World Customs Organisation (WCO)

Revised WCO Kyoto Convention

The 1974 WCO International Convention on the Simplification and Harmonization of Customs procedures, otherwise known as the Kyoto Convention, was revised and then adopted in June 1999 by the WCO Council to ensure modern and efficient Customs procedures in the 21st century. A key aspect of the revised Convention is its focus on the transparency and predictability along the supply chain. Principal elements of the revised Convention include:

- The use of pre-arrival information to drive programmes of selectivity.
- Risk management techniques (including risk assessment and selectivity of controls).
- Maximum use of automated systems.
- Co-ordinated interventions with other agencies.
- Readily available information on Customs requirements, laws, rules and regulations.

WCO Customs Data Model, Unique Consignment Reference (UCR) and Advance Cargo Information (ACI) Guidelines

The **WCO Customs Data Model** v. 1 establishes a standard, international, harmonized data set that will meet governments' requirements for international cross-border trade and represents a step towards harmonisation of customs information for inter-alia security purposes. The model is designed to deal exclusively with the requirements of an automated environment.

The Data Model will provide Contracting Parties to the revised Kyoto Convention with a global standard for implementing provisions for reduced data requirements and electronic submission of declarations and supporting documents.

The proposed WCO **Unique Consignment Reference** – an internationally managed universal number/reference – would serve as the unique identification for a consignment, and would allow the collection of information on a consignment from various sources as early as possible in the supply chain.

The WCO **Advance Cargo Information** guidelines, in accordance with the revised Kyoto Convention, identifies security-relevant data elements and offers guidelines for their early collection by Customs.

Finally, the 1972 **Customs Convention on Containers** (administered by the WCO on behalf of the United Nations) contains technical specifications for containers used in international transport under Customs seal as well as procedures for the approval of such containers. The Convention is currently under review from a security perspective, in particular as concerns the use of high security seals.

International Standards Organisation (ISO)

Adopted in 2003, the ISO guidelines ISO/PAS 17712:2003 *Freight containers – Mechanical seals*, set out specifications for mechanical seals used to protect the contents of freight containers. The recommendations establish uniform procedures for the classification of mechanical seal types and their requirements, as well as the acceptance and withdrawal of mechanical freight container seals based on a series of testing methods. ISO has also developed working draft standard for the use of Radio Frequency Identification Tags (RFID) in conjunction with freight containers (ISO/WD 17363) as well as a draft standard outlining common communication protocols for RFID-enabled e-seals (ISO/DIS 18185).

European Union (EU)[1]

Maritime and port security

On 2 May 2003, the Commission proposed a Parliament and Council Regulation on enhancing ship and port facility security [*COM (2003)229 final*, European Parliament First Reading on 19/11/2003]. This proposal is the IMO ISPS implementing legislation and presents rules on ship security assessment, security plans, introduction of security officers on ships and fitting ships with security equipment (*i.e.* alarms, marking, Automatic Identification System, etc.). The proposed regulation also addresses port security assessments and consequent measures, a distinction of security levels based on the concentration of threat, and establishment of security officers and committees who will train staff and control the implementation of security measures in ports.

On 10 February 2004, the Commission proposed a Parliament and Council Directive on enhancing port security [*DIR COM(2004)76*]. This proposal complements the regulation on ship and port facility security. In particular, whereas *COM(2003)229 final* only extends its coverage to "port facilities" (*i.e.* terminals – reflecting the limited land-side reach of the IMO), *COM(2004)76* extends the ISPS measures to the entire port area as well as to adjacent areas where these have a direct or indirect impact on the port (*e.g.* rail yard, container depots, warehouses, etc.). It presents rules on port-wide security assessment, security plans, introduction of port-wide security officers and security committees. The security assessment will be the basic instrument to identify the risks to port security and the appropriate measures to reduce this risk appropriately.

Intermodal

The consultation paper "Freight Transport Security" (December 2003) discusses:

- Securing key transport infrastructure.
- Minimum security standards for transport service providers.
- Ensuring proper functioning of the system.

The EU also supports projects such as:

- Safe Intermodal Transport Thematic Network (SIT-TN) – a networking activity for international cooperation and information exchange regarding safety and security for intermodal freight transport.
- Safe and Secure Intermodal Transport Across the Globe (SIMTAG) – a demonstration project to develop technology, processes and methods that improve the security, safety and efficiency of intermodal transportation.

External border

On 24 July 2003, the European Commission published a Communication and a proposal for a Regulation to modify the Community Customs Code. This proposal was intended to enhance the role of customs in the security management of the EU's external borders. The new implementing rules will establish compatible security standards for the transportation of EU imports and exports.

Eight EU countries have adhered to the United States Customs Security Initiative (CSI – see below). After having launched infringement procedures against these bilateral agreements, the European Commission has signed an agreement with the US in April 2004 to intensify

container security cooperation, including expansion of the CSI to all ports in the European Community.[2] Further accords of the same type may be negotiated with Canada and countries in Asia.

Secure Trade in APEC Region (STAR)

The STAR initiative, proposed by the United States and adopted by APEC Leaders in Los Cabos in October 2002, commits APEC economies to accelerate action on screening people and cargo for security before transit; increasing security on ships and airplanes while en route; and enhancing security in airports and seaports.

United Nations Economic Commission for Europe (UN-ECE)[3]

Transports Internationaux Routiers system (TIR)

The TIR system, as defined by the UN-ECE TIR Convention (1975), has been devised to ensure that goods may travel with a minimum interference "en route" and yet offer maximum safeguards to Customs administrations. Security elements of the TIR procedures include the following:

- The TIR Convention sets out technical requirements on secure vehicles, containers and sealing.
- The TIR Carnet, an internationally accepted Customs document, reduces the risk of pressing inaccurate information to Customs administrations.
- The access to the TIR system by transport operators and national associations to issue TIR Carnets is controlled. The requirements stipulated in the Convention include sound financial standing and absence of serious or repeated offences against Customs or tax legislation. Information on all transport operators authorized to use TIR Carnets is centrally stored in the International TIR Data Bank.

In February 2004, UN-ECE's Working Party on Customs Questions affecting Transport (WP.30) and the TIR Administrative Committee have agreed on a step-by-step approach for the computerization of the TIR procedure which is currently paper-based. Through the use of modern and secure information technology, it is envisaged that the TIR procedure will be able to facilitate the transmission of advanced cargo information and additional data related to security controls which are not already in the TIR procedure. The Working Party has also initiated a review of the use of sealing devices in the TIR procedure with a view to further enhancing the security and integrity of loading units approved for TIR transports. This process is being carried out in parallel to a process in the WCO on reviewing sealing procedures prescribed in the Kyoto Convention and the Customs Convention on Containers.

International carriage of dangerous goods

International carriage of dangerous goods by rail, road, and inland waterways is regulated respectively by Regulations concerning the International Carriage of Dangerous Goods by Rail (RID), European Agreement concerning the International Carriage of Dangerous Goods by Road (ADR), and European Agreement concerning the International Carriage of Dangerous Goods by Inland Waterways (ADN). The RID/ADR/ADN Joint Meeting is considering new security provisions including:

- Proper identification of carriers before shipment.

- Securing areas of temporary storage sites, vehicle depots, marshalling yards, etc. used for dangerous goods.
- Means of identification with photography carried by all crew members.
- Existing safety inspections to be extended to security.
- Existing mandatory training of staff involved in transport of dangerous goods to be extended to security.
- For the "high-consequence" dangerous goods (which include gasoline in tank-vehicles), security plan to be developed by consignor, carrier and all other participants in the transport operation, and application of measures to prevent theft.

Vehicle regulations

The Working Party on General Safety Provisions is considering an amendment to Regulation in order to introduce a "vehicle degradation system", a device which, after previous activation, is intended to prevent or to restrict a vehicle being driven away by its own engine after standstill of the vehicle.

US national and bilateral measures

Container Security Initiative (CSI)

CSI is a reciprocal government-to-government program based on the idea of extending the zone of security outward to the port of origin. This programme places US Customs officers in foreign ports to assess the security risk of containers before they depart for the United States. Their principal role is to apply US targeting matrices in order to single out containers for inspection before they are loaded onto vessels. Actual scanning and/or inspection of the selected containers are carried out by Customs officers of the port country. While the United States has declared that CSI is a reciprocal programme – that is that CSI-participating countries can place Customs officers in US ports – relatively few countries have done so.

Customs-Trade Partnership against Terrorism (C-TPAT)

C-TPAT is a voluntary joint government-business initiative, which encompasses manufacturers, importers, brokers, warehouse operators and carriers (air, rail, sea). The premise of the programme is that existing security practices among certain participants of the container transport chain (such as those implemented under the BASC programme, for example) should be validated and extended to all participating companies. Through this initiative, participants must conduct a comprehensive self-assessment of supply chain security using the C-TPAT security guidelines jointly developed by Customs and the trade community. Once participants are vetted by Customs, they will be subject to a reduced number of inspections and oversight. The programme is not yet designed to be extended to all elements in the supply chain, and in particular, the question of participation by small, non-US shippers, carriers and forwarders has yet to be addressed.

24 Hour Advance Manifest Rule

Effective December 2, 2002, maritime carriers and electronically-enabled NVOCCs must submit a cargo declaration 24 hours before cargo is laden aboard a vessel at a foreign port outside the United States. The cargo declaration must be submitted for containers destined

for the United States as well as for non-US destination containers loaded onto vessels calling at US ports. US Customs uses the cargo information to assess potential terrorist threats before a vessel sails from a foreign port to US seaports, rather than after a vessel and its cargo arrives in the United States. For other modes, manifests are required 30 minutes or an hour before trucks arrive in the US, two hours for rail, and four hours for air.

Bio-Terrorism Act

The Bioterrorism Act (BTA), which was signed into law June 12, 2002, is intended to protect the health and safety of the US population from an intended or actual terrorist attack on the nation's food supply. With few exceptions, all domestic and foreign food facilities that manufacture/process, pack, or hold food for human or animal consumption in the United States must register with the US Food and Drug Administration (FDA), so that the FDA can quickly identify and locate affected food processors and other establishments in the event of deliberate or accidental contamination of food. Also, prior notice must be submitted for any shipment of human or animal food imported or offered for import subject to the Act. The intent is to provide advance information to target potentially high-risk shipments that could threaten public health and the security of the food chain by an act of bioterrorism.

Industry and joint industry government initiatives

Business Anti-Smuggling Coalition (BASC)

BASC is a voluntary cooperation program between the private sector, governments, and international organisations. BASC consists of national and regional chapters, while central management is carried out by the World BASC Organization (WBO), with participation by Colombia, Costa Rica, Ecuador, Mexico, Panama, Peru, United States of America and Venezuela. BASC promotes the strengthening of supply chain security standards and procedures. The main goal is to encourage the development and implementation of voluntary steps to address the risks of narcotics and merchandise smuggling through legitimate trade, as well as the threat of a disruption in the global economy brought about by terrorism. The companies that form BASC are periodically audited and assured that their products and services are produced and delivered under strict security controls.

Memorandum of Understanding on Electronic Business

Aiming at establishing a coherent set of information and communication technology standards which are open, interoperable, and internationally accepted among consumers, industry and government, a Memorandum of Understanding (MoU) on electronic business has been signed by the four main organisations: the International Electrotechnical Commission (IEC), the International Organization for Standardization (ISO), the International Telecommunication Union (ITU), and the United Nations Economic Commission for Europe (UN-ECE). The MoU establishes a coordination mechanism to produce mutually supportive standards required in business transactions (data interchange and interoperability) as well as products design and manufacturing to meet the urgent needs of both the industry and the end-users.

International Road Transport Union (IRU)

The IRU General Assembly approved on 8 November 2002 the Resolution on Security in Road Transport calling for measures which strengthen protection against crime and terrorism while facilitating international transport and trade. The IRU calls on governments to work with the industry to combat all forms of crime, whilst preserving trade facilitation measures like customs transit systems. At the same time, it asks the road transport industry to implement modern risk management procedures, internal security measures and anti-fraud practices.

The IRU has also developed "Guidelines for Road Transport Security" which explain how the UN's revised ADR rules will affect safety advisors, records, operations, employees, reporting and confidentiality. The IRU is also developing a "Standard Security Plan", to help transport operators to fulfil the new rules' requirement for them to develop a security plan when transporting "high consequence dangerous goods".[4]

Operation Safe Commerce (OSC)

OSC is a public-private partnership program with 18 projects designed to improve container supply chain security. These projects identify and explore commercially viable business processes, technologies and initiatives that protect commercial shipments from threats of terrorist attack, weapons of mass destruction, smuggling and contraband throughout supply chains. These projects analyze existing practices and test security solutions in an operational environment and scrutinize supply chain security through container tracking and tracing technology, non-intrusive detection strategies, and improved seal concepts. The projects are conducted at the 3 largest container load centers in the United States: New York/New Jersey, Los Angeles/Long Beach, and Seattle/Tacoma.

As part of the US Department of Homeland Security's effort to secure cargo moving through the ports of the United States, the US Congress provided funding for Operation Safe Commerce, a pilot program and collaborative effort between the federal government, business interests, and the maritime industry to enhance containerized supply chain security. The program's objective is to thwart the use of containers as a vehicle for terrorism by identifying and addressing security risks in an operational environment.

An Executive Steering Committee (ESC) provides organisational oversight for OSC and its membership is comprised of senior officials from the US Transportation Security Administration, the US Department of Transportation, and the US Customs and Border Protection Agency. In addition to representatives from these agencies, an OSC Program Review Panel comprised of members from the United States Coast Guard, and the US Departments of State, Justice and Commerce provides oversight for the actual technology deployments under the OSC program.

The OSC Executive Steering Committee selected eighteen container security projects proposed by these Load Centers that focus on supply chain security shortcomings from point of origin to point of destination. These projects provide a test bed for security techniques and practices that have the potential to enhance container security. They identify vulnerabilities and scrutinize supply chain security through container tracking and tracing technology, non-intrusive detection strategies, and improved security and business practices.

In an effort to create synergy with other US initiatives, many of the OSC projects integrate other federal container security programs such as US Customs and Border Protection's Customs Trade Partnership Against Terrorism (C-TPAT) and their Container Security Initiative (CSI), and the US Department of Transportation's Intelligent Transportation System.

Smart and Secure Tradelanes (SST)

SST is an industry-driven, supply chain security initiative in the United States created by the world's three largest seaport operators. SST uses wireless identification and detection technologies, including Radio Frequency Identification (RFID), satellite tracking systems, sensors, and biometrics. The objective of SST is to rapidly deploy a baseline infrastructure that provides real-time visibility, physical security through non-intrusive, automated inspection and detection alerts, as well as a complete audit trail of a container's journey from origin to final destination.

Table B.1. **Coverage of current and proposed container security measures**

	Container scanning	Container integrity	Container environment	Container tracking	Container doc. and intelligence
International					
IMO	X		X		X
ILO			X		X
WCO	X		X	X	X
ISO	X	X			
EU		X	X		X
APEC/STAR	X			X	X
UN-ECE/TIR	X	X			X
UN-ECE/International carriage of dangerous goods	X	X	X		
National and bilateral					
CSI (US)	X				
C-TPAT (US)		X	X		X
24 Hour Rule (US)	X				X
Bio-Terrorism Act (US)	X				X
Industry and Industry Government					
BASC		X	X		X
E-Business MoU					X
IRU	X	X	X	X	X
OSC (US)	X	X		X	
SST (US)	X			X	

Notes

1. European Commission, Consultation paper – *Freight Transport Security*, December 2003.
2. European Commission, *http://europa.eu.int/comm/taxation_customs/customs/information_notes/containers_en.htm*.
3. UN-ECE, Transport and Security, Note by the Secretariat, 16 February 2004.
4. IRU, Transport Security in the EU, Electronic Pre-Notification of Export and Import Movements by Authorised Transport Operators? – Draft IRU Position on a "Consultation Paper on Freight Transport Security" issued by the European Commission DG Energy and Transport on 23 December 2003 and a "Proposal for a regulation of the European Parliament and of the Council amending Council Regulation (EEC) No. 2913/92 establishing the Community Customs Code (2003/0167 (COD)".

Bibliography

Abt, C. *et al.* (2003), "The Economic Impacts of Bioterrorist Attacks on Freight Transport Systems in an Age of Vulnerability", Prepared by Abt Associates for US DOT/RSPA/Volpe (Contract DTRS57-03-P-80130), Cambridge (MA).

Association of American Railroads, *www.aar.org*.

Australian Ministry of Foreign Trade and Economic Co-operation (2001), "Paperless Trading: Benefits to APEC", Canberra.

Barletta, M. (ed.) (2002), "After 9/11: Preventing Mass-Destruction Terrorism and Weapons Proliferation", Center for Nonproliferation Studies at the Monterey Institute of International Studies, Monterey.

Bolkestein, F. (2003), "EU Customs Policy – Boosting Security and Modernising Procedures" (EU SPEECH/03/584).

Business Anti-Smuggling Coalition (2002), "BASC Standards", World BASC Organization, Cartagena.

Carl, H. and United Nations Economic Commission for Europe (UNECE) (2003), "Proposal for Standards Development in Support of Trade Facilitation and Security: A Collaborative Approach" (TRADE/2003/22), Geneva.

Central Commission for Navigation on the Rhine (CCNR), *http://ccr-zkr.org*.

Dae, J. *et al.* (2002), "2002 China Logistics Provider Survey: Results and Findings (Summary)", The Logistics Institute at Georgia Tech University and the the National University of Singapore.

Damas, P. (2003), "Global Security Controls on Supply Chains", *American Shipper*, Vol. 45, No. 8 (August), Jacksonville, pp. 20-26.

Damas, P. and R. Mottley (2003), "Shippers only Flirt with E-Commerce", *American Shipper*, Vol. 45, No. 8 (August), Jacksonville, pp. 10-18.

DeVrede, M., J.W. Koolwaaij, M. Oosterhout, Y.H. Tan, R. Lee and M. Zielinski (2001), "Rotterdam Virtuele Haven: Messaging – State of the Art EDI XML", Erasmus University, Rotterdam.

Dulbecco, P. and B. Laporte (2003), "How can the Security of the International Supply Chain be Financed? A Global Good Approach", Centre d'études et de recherches sur le développement international, CNRS Université d'Auvergne on behalf of the World Customs Organization, Clermont Ferrand.

European Commission (2003), "Consultation Paper: Freight Transport Security", Directorate General for Energy and Transport, Brussels.

European Commission (2003), *EU Energy and Transport in Figures Statistical Pocket Book*, Brussels.

European Commission, *http://europa.eu.int/comm/taxation_customs/customs/information_notes/containers_en.htm*.

European Conference of Ministers of Transport (1997), Resolution No. 97/2 on Crime in International Transport.

European Conference of Ministers of Transport (1998), *Report on the Current State of Combined Transport in Europe*, OECD, Paris.

European Conference of Ministers of Transport (1999), *What Markets Are There For Transport By Inland Waterways?*, Round Table 108, OECD, Paris.

European Conference of Ministers of Transport (2000), *Integration of European Inland Transport Markets*, OECD, Paris.

European Conference of Ministers of Transport (2001), *Land Access to Sea Ports*, Round Table 113, OECD, Paris.

European Conference of Ministers of Transport (2001), *Crime in Road Freight Transport*, OECD, Paris.

European Conference of Ministers of Transport (2002), *Ministerial Declaration on Combating Terrorism in Transport*, CEMT/CM(2002)18.

European Conference of Ministers of Transport (2002), *Regulatory Reform in Road Freight Transport*, OECD, Paris.

European Conference of Ministers of Transport (2004), *Policy Note and Declaration on Security and Terrorism in the Transport Sector*, CEMT/CM(2004)5/Final.

European Conference of Ministers of Transport and International Road Transport Union (2003), *Truck Parking Areas in Europe, ECMT/IRU*, Paris.

European Conference of Ministers of Transport (2004), *Report on Removal of Obstacles at Border Crossings*, CEMT/CM(2004)23.

Eurostat, *Trends in Rail Goods Transport*, 1990-2001, Brussels.

Eurostat, *Inland Waterways Freight Transport in 1990-2001 in the European Union and the Candidate Countries*, Brussels.

Eurostat (2002), *Panorama of Transport*, Brussels.

Export 911, *Online Shipping and Logistics Guide* (*www.export911.com*).

FIA International Ltd. (2001), "Contraband, Organized Crime and the Threat to the Transportation and Supply Chain Function", FIA International.

Ghazarian, J. (Loran Technologies) and L. Trebasch (Savi Technologies) (2002), "Report on Asset Tracking Technologies", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 3, June 14.

Goedvolk, E.J., B. Hulsebosch, W. Janssen and P. Maclaine (2001), "Rotterdam Virtuele Haven: Risk Analysis of Container Import processes", Telematica Institute, Rotterdam.

Goldman, A. and K. Crawford (Tech Center) (2003), "Five RFID Myths Exposed", Wi-Fi Planet (*www.wi-fiplanet.com/tutorials/article.php/3296031*).

Hoffman, B. (2003), "Al Qaeda, Trends in Terrorism and Future Potentialities", The Rand Corporation, Washington, D.C.

Huddlestone, James C. (2002), "Supply Chain Visibility and Valuation" (*www.eyefortransport.com*).

Institute of International Container Lessors (2003), "2003 IICL Annual Leased Container Fleet Survey", New York (*www.iicl.org*).

Institute of Shipping Economics and Logistics (ISL) (2002), "Executive Summary – SSMR Market Analysis", No. 6, Institute of Shipping Economics and Logistics, Bremen.

International Road Transport Union (IRU), *www.iru.org/TIR/TirSystem.E.htm*.

International Road Transport Union (IRU) (2004), Draft Position Paper, *Transport Security in the EU, Electronic Pre-Notification of Export and Import Movements by Authorised Transport Operators?*.

International Transport Implementation Guidelines Group (ITIGG) (1997), *Guide to UN/EDIFACT Container Messages Version 1.3* (JM4/ITIGG/103/v.13).

Ioannou, E.B. *et al*. (2000), "Cargo Handling Technologies Final Report" (Task 1.2.3.2 – Commercial Deployment of Transportation Technologies), Center for Advanced Transportation Technologies at the University of Southern California and August Design, Inc., Los Angeles.

ISO (International Standards Organisation) (2002), "Freight Containers – Radio-frequency Communication Protocol for Electronic Seal", ISO Technical Committee 104 SC4, Working Document ISO/DIS 18185.

ISO (International Standards Organisation) (2003), "Supply Chain Applications of RFID – Freight Containers", ISO Technical Committee Joint Working Group 122/104, Working Document ISO/WD 17363.

ISO (International Standards Organisation) (2004), "Freight Containers – Mechanical Seal", ISO Technical Committee 104 N 940, Publicly Available Specification (PAS) 17712.

Lewis, B. (2002), "Port Security: Container Targeting and Inspection Procedures of the United States and Singapore", The Logistics Institutes of Georgia Tech University and the National University of Singapore.

Lin, J. (US Customs) and P. Talley (Vigilos, Inc.) (2002), "Report on Asset Control and Integrations", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 2, June 14.

Meyer, A. and D. Meyer (2002), "Supply Chain Response to terrorism – Planning for the Unexpected", Center for Transportation and logistics, Massachusetts Institute of Technology, Boston.

National Academy of Sciences (United States) (2003), "Cybersecurity of Freight Information Systems: A Scoping Study", Computer Science and Telecomunications Board of the Transportation Research Board, Washington, D.C.

O'Brian, K. and M. van de Voort (2003), "Seacurity: Improving the Security of the Global Sea-Container Shipping System", RAND Corporation, Santa Monica.

O'Brien, G. and R. Stuart (2003), Non-intrusive Container Inspection, *Port Technology International*.

OECD (2001), "Behind the Corporate Veil: Using Corporate Entities for Illicit Purposes", Organisation for Economic Co-operation and Development, Paris.

OECD (2002), "The Economic Consequences of Terrorism", Economics Working Papers No. 334, Organisation for Economic Co-operation and Development, Paris.

OECD (2003), "Quantitative Assessment of the Benefits of Trade Facilitation: Progress Report" [TD/TC/WP(2003)20], Organisation for Economic Co-operation and Development, Paris.

OECD (2003), "Role of Automation in Trade Facilitation" [TD/TC/WP/(2003)21], Working Party of the Trade Committee, Organisation for Economic Co-operation and Development, Paris.

Oosterhout, M. and Y.H. Tan (2001), "Rotterdam Virtuele Haven: Detailed Process-Description Containerscan Showcase", Erasmus University, Rotterdam.

Oosterhout, M., Y.H. Tan and M. Zielinski (2000), "Rotterdam Virtuele Haven: Inventory of Flows and Processes in the Port", Erasmus University, Rotterdam.

P&O Nedlloyd (2003), "The Merchants Guide: 2003 Edition", P&O Nedlloyd, London.

Pan-European *Conference on Inland Waterway Transport* (2001), Rotterdam Declaration.

Quartel, R. (Freightdesk technologies) (2002), "Report Information Application Technologies", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 8, June 14.

Science Applications International Corporation (SAIC) (2003), "Final Report: Container Seal Technologies and Processes", Cargo Handling Co-operative Program of the US Department of Defense Space and Naval Warfare Systems Center, San Diego.

Sheridan, R. (American Sciences and engineering) (2002), "Report on Non-intrusive Inspection Technologies", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 6, June 14.

Sinclair Knight Merz Consulting and the State Government of Victoria, Department of Infrastructure (2003), "Melbourne Port Container Origin and Destination Process Mapping", Sinclair Knight Merz Pty Ltd., Malvern (Australia).

Smith, S. (Harrison Consulting Group, LLC) (2002), "Report on Seal Technologies", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 7, June 14.

Spencer, C. (IMS Worldwide) (2002), "Report on Intrusion Detection Technologies", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 5, June 14.

Spurgeon, K., J. Prozzi and H. Harrison (2003), "The Secret Life of the Container: Evidence from Texas", University of Texas Center for Transportation Research (prepared for the 2003 Transportation Research Board Annual Meeting), Austin.

Stanford Study Group (2003), "Container Security Report", Center for International Security and Cooperation (CISAC – Stanford University), Stanford.

Talley, P. (Vigilos, Inc.) (2002), "Report Closed Circuit Television Technologies", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 4, June 14.

US Customs and Border Protection (2003), *C-TPAT Validation Process Guidelines*, Washington, D.C.

US Customs and Border Protection, *www.cbp.gov*.

US Office of Trade and Economic Analysis (1999), *Small and Medium sized Exporting Companies: a Statistical Profile*, US Office of Trade and Economic Analysis, Washington, D.C.

US Office of Trade and Economic Analysis (2001), *Export America 2001*, US Office of Trade and Economic Analysis.

UNECE (2002), "Trade Facilitation: The Challenges for Growth and Development", United Nations Economic Council for Europe, Geneva.

United Kingdom Parliamentary Office of Science and Technology (2002), "Nuclear Terrorism", *Postnote*, No. 179 (July), London.

United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT) (2003), The International Shippers and Freight Forwarders Security Code – Draft (Security-management Systems for the supply chain), International Trade Procedures Working Group (ITPWG).

United Nations Conference on Trade and Development (UNCTAD) (2001), "Study on the Use of Information Technology in Small Ports" (UNCTAD/SDTE/TLB/1), Geneva.

United Nations Conference on Trade and Development (UNCTAD) (2003), "Development of Multimodal Transport and Logistics Services" (TD/B/COM.3/EM.20/2), Geneva.

United Nations Conference on Trade and Development (UNCTAD) (2003), "The Use of Transport Documents in International Trade" (UNCTAD/SDTE/TLB/2003/3), Geneva.

United Nations Conference on Trade and Development (UNCTAD) (2004), *Container Security: Major Inititiatives and Related International Developments* (UNCTAD/SDTE/TLB/2004/1), Geneva.

United Nations Economic and Social Council for Asia and the Pacific (2001), "Emerging Issues in Transport, Communications and Infrastructure Development: Globalisation and Integration of Transport" [E/ESCAP/SGO/MCI(2)/3], Seoul.

United Nations Economic Commission for Europe (UN-ECE) (2002), *TIR Handbook*, UNECE, Geneva.

United Nations Economic Commission for Europe (UN-ECE) (2004), *Transport and Security*, Note by the Secretariat, 16 February.

United States Customs and Border Protection (2001-04), Frequently Asked Questions (FAQ): 24-Hour Rule, Container Security Initiative, Trade Act of 2002, C-TPAT, ACE, *www.cbp.gov*.

United States Interagency Commission on Crime and Security in US Seaports (2000), "Report of the Interagency Commission on Crime and Security in US Seaports", Washington, D.C.

United States Senate Committee on Foreign Relations (2002), "Dirty Bombs and Basement Nukes: The Terrorist Nuclear Threat", Transcript of Hearing held on March 6, Washington, D.C.

USGAO (1998), "Combating Terrorism:Threat and Risk Assessments can Help Prioritize and Target Program Investments" (GAO/NSIAD-98-74), Washington, D.C.

USGAO (2003), "Container Security: Expansion of Key Customs Programs will Require Greater Attention to Critical Success Factors" (GAO-03-770), Washington, D.C.

USGAO (2003), "Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers" (GAO-04-325T), Washington, D.C.

USGAO (2003), "Maritime Security: Progress Made in Implementing Maritime Security Act but Concerns Remain" (GAO-03-1155T), Washington, D.C.

USGAO (United States Government Accounting Office) (1999), "Combating Terrorism: Need for Comprehensive Threat and Risk Assessments of Chemical and Biological Attacks" (GAO/NSIAD-99-163), Washington.

USGAO (United States Government Accounting Office) (2003), "Homeland Security: Preliminary Observations on Efforts to Target Security Inspections of Cargo Containers (Statement of Richard M. Stana, Director USGAO Homeland Security and Justice)" (GAO-04-325T), Washington, D.C.

Wilkins, B. (National Cargo Security Council) (2002), "Executive Summary", COAC (United States Treasury Advisory Committee on Commercial Operations of the United States Customs Service), Vol. 1, June 14.

Wolfe, M. (North River Consulting Group) (2001), "Freight Transport Productivity and Security", Fifth EU/US Forum on Intermodal Freight Transport, Jacksonville, April 11-13.

Wolfe, M. (North River Consulting Group) (2002), "Electronic Cargo Seals: Context, Technologies and Marketplace", Intelligent Transportation Systems Joint Program Office, FHWA, USDOT, July 12.

World Customs Organization (WCO) (2002), "WCO Recommendation on the Unique Consignment Reference Number (UCR)", World Customs Organization, Brussels.

World Customs Organization (WCO) (2003), "Draft Guidelines on Advanced Cargo Information (ACI Guidelines)", World Customs Organization, Brussels.

World Shipping Council, International Mass Retail Association and the National Industrial Transportation League (2003), "In-Transit Container Security Enhancement" (*www.worldshipping.org*), Washington, D.C.

World Shipping Council, National Industrial Transportation League, National Customs Brokers and Forwarders Association of America, Inc. and the Retail Industry Leaders Association (2004), Petition before the United States Department of Homeland Security, Bureau of Customs and Border Protection for reconsideration of final rule: Required Advance Electronic Presentation of Cargo Information (RIN 1651-AA49) (*www.worldshipping.org*), Washington, D.C.

OECD PUBLICATIONS, 2, rue André-Pascal, 75775 PARIS CEDEX 16
PRINTED IN FRANCE
(75 2005 01 1 P) ISBN 92-821-0331-5 – No. 53893 2005