

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", *OSCE Ministerial Council Decision No.9/04*

Contents

GOVERNMENTS

Stephen Caldwell, U.S. Government
Accountability Office (**GAO**), [LINK](#)

Russian Federation, [LINK](#)

INTERGOVERNMENTAL BODIES

Stefan Aniszewski, World Customs
Organization (**WCO**), [LINK](#)

Halina Biernacki, International Civil Aviation
Organization (**ICAO**), [LINK](#)

Gustav Kafka, Intergovernmental
Organisation for International Carriage by Rail
(**OTIF**), [LINK](#)

Mehdi Knani, **OSCE** Secretariat, [LINK](#)

Gabriel Leonte and Roel Janssens, **OSCE**
Secretariat, [LINK](#)

Graham Mapplebeck, International Maritime
Organization (**IMO**), [LINK](#)

Marios Meletiou, International Labour
Organization (**ILO**), [LINK](#)

PRIVATE SECTOR

Jacques Colliard, International Union of
Railways (**UIC**), [LINK](#)

Mark Miller and Moureen Schobert, European
Organisation for Security (**EOS**), [LINK](#)

Charles H. Piersall, International Standard
Organization (**ISO**), [LINK](#)

Umberto de Pretto, International Road
Transport Union (**IRU**), [LINK](#)

Marco Sorgetti and Niels Beuck, European
Association for Forwarding, Transport,
Logistic and Customs Services (**CLECAT**), [LINK](#)

Tim Watson, International Chamber of
Shipping (**ICS**), [LINK](#)

➔ Contact

Mehdi Knani
Editor
Mehdi.Knani@osce.org

The CTN Electronic Journal is available online, free of charge, in English and Russian, to any interested reader, at www.osce.org/atu
Inquiries regarding reproduction and adaptation rights, for all or parts of this issue, should be addressed to atu@osce.org
Contributors to this issue can be contacted through the OSCE Action against Terrorism Unit.

Tel: +43 1 514 36 6702
Fax: +43 1 514 36 6687
E-mail: atu@osce.org
www.osce.org/atu

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No. 9/04

Editorial

There is no doubt over how critical the container transport system is to the world economy, as a core component of the international supply chain. More than 90 per cent of global freight moves by containers and more than 400 million container shipments occur annually.

There is no doubt also over how daunting a challenge it is for governments to secure containers and the supply chain. Containers are potentially easy to tamper with and therefore vulnerable to criminal abuses such as theft and illicit trafficking. But the ubiquity and sheer volume of containerized trade make it practically impossible to ensure full access control to containers at all times in all places, and to ascertain the content of every containers through physical inspection.

The complexity and fragmentation of the container transport system makes oversight and security enforcement particularly challenging. Multiple private operators are involved in, and state authorities concerned with, the handling of containers across borders and jurisdictions, by sea, air, rail and road. Add to this the economic imperative of facilitating rather than disrupting trade and a rough sketch of the issue of container security starts to emerge.

With the 9/11 terrorist attacks against the United States, governments around the world became increasingly concerned over possible terrorist targeting or misuse of the container transport system. Terrorist attacks against major container ports or other choke points in the container system have the potential to disrupt the supply chain and wreak havoc in the global economy. Terrorists could seek to deliver a chemical, biological, radiological or nuclear (CBRN) weapon by means of a container shipment to inflict human, environmental and economic damage of catastrophic proportions.

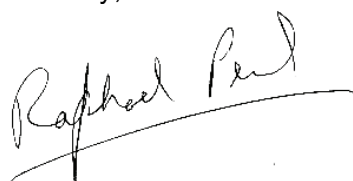
The threat of terrorism became the driving force behind the mobilization of the international community to secure the container transport system and the supply chain. Several national initiatives were launched with the dual goal of securing and facilitating trade and transportation. Specialized intergovernmental organizations, such as the World Customs Organization (WCO), the International Maritime Organization (IMO) and the International Civil Aviation Organization (ICAO) were called upon to develop international standards on their pieces of the container transport security puzzle.

Five years ago, the OSCE rallied to support these ongoing efforts. Participating States pledged in December 2004 to act urgently to enhance container security based on best practices and standards agreed internationally. The following year, they committed to implement WCO's Framework of Standards to Secure and Facilitate Global Trade (SAFE). Concurrently, the OSCE Secretariat was mandated to promote the exchange of information and best practices on container security, as well as to facilitate technical assistance and awareness raising efforts in this field by the WCO and other relevant international organizations.

Five years on, the ATU is publishing this CTN Special Bulletin to give an overview of efforts undertaken by the international community and the private sector to enhance container and supply chain security, and the challenges ahead. The ATU invited OSCE participating States, through their CTN contact points, as well as a number of international structures and private sector stakeholders to contribute articles presenting their work and views.

I hope that you will enjoy reading this Special Bulletin,

Sincerely,



Raphael F. Perl
Head on Anti-Terrorism Issues
OSCE Action against Terrorism Unit

CTN Newsletter Special Bulletin

Enhancing Container and Supply Chain Security

July 2010

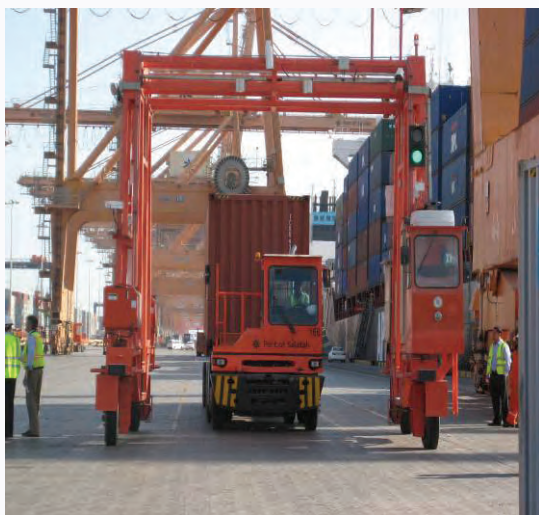
“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

Supply Chain Security: More Economic Analysis Needed Before Proceeding with U.S. Requirement to Scan 100% of Containers

*Stephen L. Caldwell, Director of Maritime Security Issues
U.S. Government Accountability Office (GAO)*

Few changes in supply chain security have the potential worldwide economic impact of the U.S. statutory requirement that 100% of U.S.-bound cargo containers be scanned before being loaded on ships. This requirement was put in place through two pieces of legislation—the SAFE Port Act and the 9/11 Act—which directed U.S. Customs and Border Protection (CBP) to establish pilot ports for testing the proposal and to then implement the requirement by July 2012. Yet relatively little of the international discussion and controversy over the requirement has focused on economic issues.

Much of the discussion surrounding the scanning requirement has been focused on the technological maturity of equipment, particularly the difficulties of scanning containers quickly and scanning containers that are transshipped (moved from one ship to another ship without ever leaving the port). There has also been much discussion of the layout and logistics of various ports that make it challenging to separate and scan all U.S.-bound containers. On the political front, various nations have discussed or threatened to implement reciprocal scanning requirements on U.S. origin containers exported to their ports. As a matter of principle, several nations and other observers have questioned whether the 100% scanning requirement is consistent with risk management as endorsed in the World Customs Organization’s SAFE Framework. And finally, experts have raised concerns that 100% scanning may hinder implementation of existing programs in the CBP layered security regime.



Mobile RPM equipment in Salalah, 100% scanning pilot port in Pakistan (GAO)

One possible reason for the focus on these other factors and the lack of economic analysis is the uncertainty over who will pay the costs associated with the 100% scanning requirement. While the U.S. government has purchased cargo container scanning equipment thus far for foreign ports that have participated in the SFI pilot program (see cost estimates below), it is unclear who will pay for additional costs—including additional infrastructure, construction, equipment, installation, and people—to continue operating and advancing the program. Neither the SAFE Port Act nor 9/11 Act specifies who is to pay for scanning U.S.-bound cargo containers at foreign ports.

While some cost information has been gathered to date, the costs gathered and estimated by the U.S. government have been limited to U.S. program implementation costs. The SAFE Port Act requires CBP to report on U.S. government costs of deploying integrated scanning equipment at foreign ports as part of the SFI program, and CBP and the Department of Energy have identified \$100 million in costs borne by the United States. CBP estimates that establishing

a single lane for 100% scanning costs about \$10 million for construction, equipment and installation. Given the number of ports worldwide (each with multiple lanes) exporting containers to the United States, CBP has developed a rough estimate of \$20 billion. These are initial construction, equipment installation costs, not the longer term “life cycle” costs (which would also include operations and maintenance over a period of years). GAO recently made recommendations for improving the accuracy and validity of CBP cost estimates related to the 100% scanning program.

In addition to not identifying complete estimates of U.S. program costs, CBP has not developed estimates of economic costs to other maritime shipping stakeholders. While governments from Europe, Asia and the Middle East are generally unwilling to pay for what they see as a U.S.-centric security initiative, some of them have borne some of the costs for personnel, infrastructure and other costs at pilot ports. In addition, private terminal operators have borne additional costs for control centers and moving containers to scanners.

CTN Electronic Journal Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

Such non-U.S. costs could be substantial and a recent European Commission study estimated European costs as € 430 million for infrastructure, construction and equipment costs, and € 200 million in operations costs per year, including 2,200 additional people. In addition to these specific costs, there may be systemic costs through lower terminal efficiency. The European Commission study estimated these systematic worldwide economic costs—referred to as welfare loss—as € 150 billion per year.



**Mobile RPM equipment in Southampton
100% scanning pilot port in the United
Kingdom (GAO)**

The additional costs of scanning may vary considerably by country or port, according to World Bank and World Customs Organization officials. For example, U.S.-bound cargo may have to be funneled through large hub ports that could accommodate and operate the scanning equipment. According to the European Commission study, these large hub ports would experience increased congestion and environmental damage. The additional shipping costs would also have a disproportionately negative impact on developing economies and countries with comparatively small ports. Similar differences by country or port might also arise if CBP grants extensions (as allowed by the law) on a port-by-port basis, potentially giving a competitive advantage to some ports and leading to trade disruptions. For example, one port that invests in scanning equipment would be able to meet the scanning requirement, but another port that does not invest in scanning equipment could not meet the requirement. If the latter port gets an extension, it could have a temporary competitive advantage over the former port because its costs of operations do not include the costs of investments in scanning equipment.

Furthermore, CBP has not performed a cost-benefit analysis to assess alternatives to achieve 100% scanning or other alternatives to enhance container security. Cost-benefit analysis is designed to identify the superior economic solution amongst competing alternatives and is a proven management support tool to support planning and managing costs and risks. Federal guidance on cost-benefit analysis indicates it should identify and measure overall costs and benefits (such as impact on international maritime stakeholders), not solely the costs related to the U.S. government. Development of a systematic cost-benefit analysis, which incorporates more complete cost estimates, could better inform CBP and the Congress of the relative costs and benefits of different alternatives, including alternatives short of scanning 100% of U.S.-bound containers. In its recent report, GAO has recommended that CBP conduct such a cost-benefit analysis.

In conclusion, more analysis should be done to analyze the economics of the U.S. legal requirement that 100% of U.S.-bound containers be scanned by July 2012. Much of the discussion surrounding this requirement has been focused on the technological maturity of scanning equipment, logistical challenges with terminal layout and operations, political considerations for reciprocity, and the consistency of this approach with risk management principles and existing elements of the layered security regime. One possible reason for the lack of economic analysis is the uncertainties of the law itself in that it does not specify who will pay the costs associated with the requirement. Some cost information has been gathered to date, and a recent European Commission study includes economic analysis. However, the economic costs estimated by the U.S. government (by CBP and others) have been limited to U.S. program implementation costs, and have excluded the costs to other stakeholders such as foreign governments and terminal operators. There has not been a cost-benefit analysis by the U.S. side to more fully examine and explore total costs. To remedy this lack of economic analysis, GAO has recommended that CBP improve its costs estimates and conduct a cost-benefit analysis.

NOTE

The article is based on the report: Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers (GAO-10-12). See www.gao.gov/cgi-bin/getrpt?GAO-10-12

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

Ensuring Container Security/Supply Chain Security and Laws of the Russian Federation on Transport Security

Russian Federation (unofficial translation from Russian)

Ensuring transportable cargo security, preventing accidents and accident-related losses, countering terrorism in transport, and other security-related global measures are becoming increasingly significant issues, particularly with regard to securing continued, standard operation of all types of transportation and above all of railroads.

“Transportation security” is a multifaceted notion that requires the implementation of a solid set of measures. These measures ought to take into account and include two central aspects: forecasting and preventing potential threats; and establishing the most technically and economically efficient mechanisms to deal with consequences of emergency situations.

The flow of goods in the supply chain is inevitably accompanied by a wide array of risks. This applies to transportation via various types of cargo transport, warehousing and temporary storage, as well as loading and unloading operations. The supply chain is a high-risk area with an inherent emergency risk. In the wake of heightened terrorist threats in recent years, transportation has increasingly become a target of terrorist attacks, in Russia as well as abroad.

In order to ensure compliance with the laws and the security of railway freight transportation, the primary objectives consist in protecting cargo and preventing access to freight wagons and containers by unauthorized persons. Agreements were signed between the Federal State Enterprise Security of Railway Transport of the Russian Federation and the Joint Stock Company (JSC) TransContainer to protect railway cargo for which security escort *en route* is compulsory, as well as to secure container transportation. Issues pertaining to railway container security enforcement are controlled by the Department for Traffic Safety of the Russian Railways JSC. Stations where “loading-unloading” operations and the shipment of containers take place are equipped with video surveillance systems.

With the aim of supporting a seamless container transportation process and to prevent tampering with containers, agencies from the Federal Ministry of Internal Affairs are patrolling railroad hauls, the areas of goods stations, as well as shunting stations. These patrols are conducted on vehicles by joint specialized teams consisting of transport and security police.

Customs bodies functioning and working efficiently is a prerequisite in preventing the flow of illicit goods. These bodies have to ensure that the legislative requirements of the Russian Federation for the regulation of foreign trade are fulfilled. In compliance with existing laws, controls over the traffic of goods imported in containers are performed upon arrival at checkpoints. Controls are carried out on the basis of a risk management system and inspections

are jointly conducted by authorized personnel from the Border Guards of the Federal Security Service and the Customs Administration of the Russian Federation, using mobile inspection systems. Controls are also performed when containers are opened during operations for temporary storage.

Various technical customs control devices are used. One of the most efficient and all-encompassing forms of customs control is the use of sophisticated inspection systems (SIS). The X-ray images obtained through these systems allow to screen the goods transported and parts of the vehicles, in order to find objects transported in violation of customs regulations, all without opening the containers and vehicles. Almost all customs posts are now equipped with SIS, in line with the Concept for Customs Development in the Russian Federation and the Concept for customs control of large-scale cargo and vehicles within the framework of the Federal Programme “The state border of the Russian Federation (2003-2010)”.



Mobile X Ray Unit, Copyright © Federal Customs Service of the Russian Federation

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

As a direct result of container examination by customs using SIS, between 2009 and 2010 within the jurisdiction of the Southern Customs Regional Office alone, 17 criminal cases and over 340 administrative cases for illegal transportation of goods have been initiated. Furthermore, 480 kg of narcotics and 192 units of weapons and ammunition were seized.



Copyright © Federal Customs Service of the Russian Federation

The customs authorities are mandated to exercise control over the import of dangerous cargoes. All goods and vehicles crossing customs checkpoints should pass through radiation detection equipment to detect fissile and radioactive materials.

In identifying and preventing offences and crimes that relate to the transportation of goods, including by container, through customs control, the regional customs authorities co-operate with the Federal Security Service, the Internal Affairs Department and the Federal Drug Trafficking Control Service, by exchanging operational information, involving their personnel in the examination of goods and vehicles and in investigations, and conducting forensic analyses.

The overall objective of the measures in the area of transport security is to reduce the risk of transport accidents, and, consequently, investments to improve the security of transportation are always a priority. However, no matter how high these expenses may be, it is impossible to eliminate these threats entirely. There comes a tipping point at which increasing expenses becomes relatively ineffective, and, consequently, the cost begins to outweigh the benefit. Therefore, reliable consequence management mechanism and damage compensation arrangement should be incorporated in the security system; for instance risk insurance is one of the most efficient forms of protection against possible damage.

Ensuring security and integrity of the cargo is a central problem of any country's transport system. For the Russian Federation, it is especially important at the present stage of the development of its market economy, as the active growth in production and consumption sets new requirements in terms of quality of the transport services.

According to the Ministry of Transport of the Russian Federation, 20% of all cargo transported in Russia is considered “dangerous”. These figures are increasing in Russia and in international transportation as a whole. Such developments are thus not limited to our country. According to the UN, this sector of the market is developing all over the world. With the increase in transportation of dangerous goods, transport-related incidents are also increasing. And these figures grow at faster rates. These disturbing statistics demonstrate the necessity for state authorities and business communities to focus on this problem.

The most problematic challenge in the transportation of dangerous cargo is, without a doubt, decreasing the rate of incidents. Indicators suggest that in this respect Russia is at par with other economically developed countries. However, in many respects the situation becomes more complex because a significant segment of the transportation of dangerous goods, especially by rail or mixed transport, occurs in close proximity to industrial and residential areas, which increases the risk of incidents with particularly devastating consequences.

Besides the risk of incidents during the transportation of dangerous goods connected with infringements of vehicle regulations and transportation rules, there is an increasing urgency to protect transport from threats of a terrorist nature. The rolling stock transporting dangerous cargo may become an object of interest for terrorists and turn into a terrible weapon in their hands. In countering such threats the condition and design of the relevant infrastructure come into question.

The fight against terrorism and transnational crime, in particular with respect to international transportation, requires coordinated efforts among the law-enforcement authorities of all countries, with unconditional support of their activities by international organizations and the international community. The analysis of how

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No. 9/04

structures involved in smuggling and illegal economic activities operate at borders of the Russian Federation show that these groups are constantly improving their methods and often unite their efforts across several countries.

Increase in flow of cargo across the borders of a country raises the likelihood of attempts at smuggling weapons, ammunition, explosives and other means to carry out a terrorist attack. One of the basic ways of smuggling weapons, drugs and other objects and forbidden materials is transportation in containers carried by sea, railway and road.

In working to identify and prevent infringements upon the customs legislation, the State Customs Committee of the Russian Federation has gained experience in carrying out joint operations with customs and other law enforcement agencies from both the states of the Commonwealth of Independent States (CIS) and other countries. The Committee is responsible for inspecting containers moved through the customs border of the Russian Federation. Special attention is given to the containers the senders of which are registered in countries of the Near and Middle East, as well as to so-called high-risk containers.

To date, there is no internationally agreed definition for containers that are considered high-risk. Therefore the following criteria are used to define high risk:

- ◆ Presence in the container of explosive, radioactive, poisoning and strong substances; weapons, ammunition, drugs and other contents of high danger;
- ◆ Presence in the container of objects of considerable material, cultural or scientific value;
- ◆ The operational environment, including the possible criminal situation which has developed in zones of transportation.

A major problem the international trade system has to face is ensuring the security of the global supply chain. According to the ISO 28000 standards developed by the International Standardization Organization, the security of a supply chain is directed, first of all, at the security of people, cargo, transport infrastructure and vehicles, protection against accidents and prevention of negative consequences.

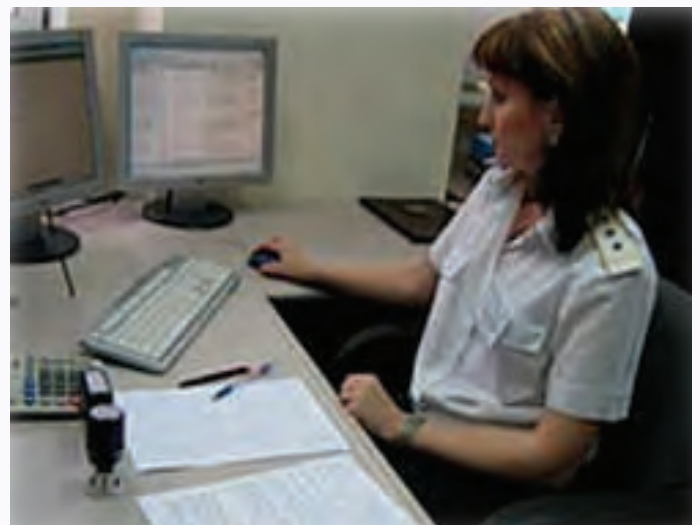
Therefore, it is reasonable to consider the security of the supply chain as consisting of a variety of countermeasures against deliberate unauthorized actions against any aspect of the delivery process. This includes planning, realization, control and improvement of measures, encompassing legal, organizational, technical, technological and economic aspects, in order to decrease loss, prevent and identify offences, and prosecute responsible individuals.

According to international statistics over the past five years, there is a growing trend of financial losses in supply chains because of criminal abuses. For example, in 2008 alone in the United States, this cost over US\$ 100 billion.

Experts note that the financial proceeds from these abuses are mostly used by criminal groups to further finance trafficking in drugs and human beings, acquire weapons, and perpetrate acts of terrorism.

Additionally, the lack of security of supply chains causes economic damage, harms those involved in trade and causes consumers to become victims of unsatisfactory quality. There are not only losses in quantity but also in quality for merchandise going through insecure supply chains.

An effective solution to secure the supply chain consists in establishing a system which includes not only law enforcement controls but also tools to identify and monitor "critical points", as well as to assess risks and efficiency in the use of resources. Such a model covers the whole supply chain from the manufacturer, the shippers to the end-users.



Copyright © Federal Customs Service of the Russian Federation

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

This concept requires the implementation of a new logistical approach to the problems of security which will promote the alignment of transport security arrangements in Russia with international practice, along the use of the common criteria and technologies. This direction has already been developed to a certain extent, first of all in the areas of sea transportation and civil aviation; therefore a systematic analysis of the application of the methodology and specialized logistic standards to other types of transport is required.

It is obvious that an essential part of the supply chain consists in transport logistics. On 22 November 2008, the Government of the Russian Federation approved the Transport Strategy of the Russian Federation for the period until 2030. The main task of the State in the area of transport is defined as creating the conditions for economic development, increasing the competitiveness of the national economy and improving quality of life of the population by providing access to safe and high-quality transport services and using the geographical features of Russia as a competitive advantage.

According to the Transport Strategy, the aims of developing the Russian transport system are to create a unified transport space, based on the balanced development of an effective transport infrastructure and integration into the world transport system, and to increase the level of its security. An important element of the Strategy's practical implementation with regard to securing supply chains is the adoption of a set of regulations to execute the Federal Law on Transport Security, adopted in the beginning of 2007. This federal law provides for the creation of a complex transport security system based on a unified approach to risk assessment, planning and implementation of measures to make transport infrastructure and vehicles safe and secure, which, in our opinion, is essential to the security of supply chains.

Transport security in the Russian Federation is understood as protection of transport infrastructure and vehicles from unlawful acts, including those of terrorist nature. Transport security is aimed at ensuring continuous and safe functioning of the transport system, and protecting the interests of individuals, society and the State. Therefore, the work currently conducted by the Russian Federation to develop a system of transport security is also aimed at achieving the appropriate level of intermodal transportation security.

Transport security in the Russian Federation is provided by means of implementing a set of legal, economic, organizational and other measures defined by the state against the background of unlawful acts threatening the transport sector.

The Transport Ministry, the Federal Security Service and the Ministry of Internal Affairs of the Russian Federation have jointly approved a list of such potential threats of unlawful acts against transport infrastructure and vehicles, which serve as basis for the organization of practical measures to secure transportation.

The primary goals of transport security, along with defining the threats of unlawful acts, are:

1. Legal regulation in the field of transport security;
2. Assessment of the vulnerability of transport infrastructure and vehicles;
3. Categorization of transport infrastructure and vehicles;
4. Identification and implementation of requirements for transport security;
5. Identification and implementation of measures for transport security;
6. Training specialists in the field of transport security;
7. Control and supervision in the field of transport security;
8. Informational, material, scientific and technical support of transport security.

The ultimate responsibility for setting transport security requirements rests with state authorities. However, within the framework of the federal legal principle of shared responsibility of individuals, society and the State in the field of transport security, users and operators of transport infrastructure and the supply chain also contribute directly to planning, information-exchange and formulation of suggestions related to transport security.

CTN Electronic Journal Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No. 9/04

The WCO SAFE Framework of Standards and Supply Chain Security

*Stefan Aniszewski, Technical Officer, Compliance and Facilitation Directorate
World Customs Organization (WCO)*

BACKGROUND

In the aftermath of the tragic events of 9/11 the world took another look at the security vulnerabilities associated with critical infrastructure and international supply chains. These concerns lead governments to seek global solutions and the assistance of international organizations such as the World Customs Organization (WCO) to come up with strategies to address these vulnerabilities in order to allay international concerns.

The response of the Customs community to this challenge was the development of the SAFE Framework of Standards (SAFE Framework). The Framework is a global supply chain security initiative, developed at the WCO by WCO Member Customs administrations in partnership with the international trade community, which incorporates the dual aim of both securing and facilitating global trade. The SAFE Framework was also designed to align the strategies of the Customs community to United Nations security resolutions and the work being undertaken in other international institutions such as the International Maritime Organization (IMO) and the International Civil Aviation Organization (ICAO).

The purpose of this article is to briefly explain the SAFE Framework's approach to supply chain security and facilitation; to outline the contribution of the approach, to shed more light on where the international Customs community currently is with its implementation, and to touch upon what challenges remain outstanding to attain full implementation by the 161 WCO Members who have committed to implement the Framework to date.

ABOUT THE SAFE FRAMEWORK

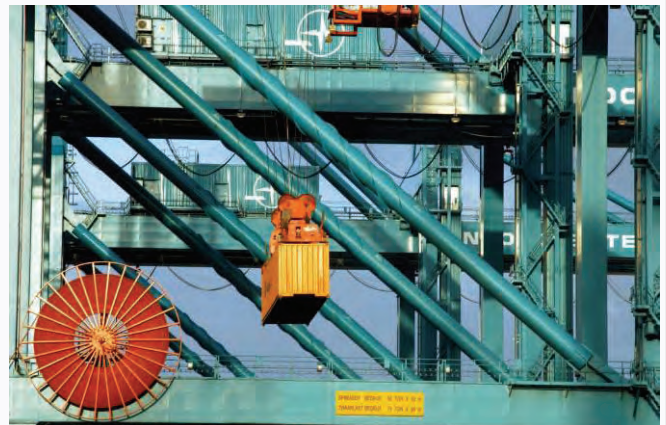
The SAFE Framework has its genesis in another key WCO instrument - the revised Kyoto Convention on the simplification and harmonization of Customs procedures (RKC). This convention contains the legal text, standards and guidelines that define the principles for a modern Customs administration. The Framework applies the RKC principles but then provides additional guidance on the end-to-end management of international supply chains, both to enhance security and improve facilitation. Today these two documents are the framework around which WCO Members develop both international and national policy and procedures that govern international cross-border trade.

Most importantly, the Framework is designed to provide additional benefits to businesses that work voluntarily with Customs to secure their supply chains from the point of packing for export until goods are cleared from Customs control on importation.

The SAFE Framework approach builds around two key pillars (Customs-to-Customs and Customs-to-Business cooperation) and consists of five core elements: the use of advance electronic cargo information; the application of consistent risk assessment; outbound security inspections; the use of non-intrusive inspection technologies based on the application of risk assessment; and benefits to businesses that meet minimum supply chain security standards and best practices.

THE CHANGE BROUGHT ABOUT BY THE SAFE FRAMEWORK

The approach outlined in the SAFE Framework has meant a fundamental change of mindset in the way Customs goes about its business. The traditional import focused business process model for border



Copyright © Antwerp Port Authority

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

control has been challenged. The Framework proposes more emphasis on control prior to exportation or pre-arrival to address security related concerns as early as possible. This new approach enables Customs administrations to “push back the border” beyond the territorial limits of countries.

To achieve the desired level of security within the supply chain, Customs must increase their levels of cooperation with one another particularly with respect to the exchange of information, risk profiles, and examination results. This collaboration has seen the development of, for example, centres to co-ordinate both exchanges of information and examination activities by the exporting administration at the request of an importing administration.

Likewise, the SAFE Framework places additional reporting requirements on carriers for the pre-arrival notification of cargo for risk assessment purposes. Risk assessment on pre-arrival information incorporates facilitation benefits as in many parts of the world it has enabled countries to make admissibility decisions earlier in the supply chain leading to the separation of physical movement and release of goods from clearance procedures. This has had a significant effect on supply chain logistics and inventory management, and has led to faster delivery of goods and cost savings.

Taking into account the long-term growth in goods and passenger flows and bearing in mind the fact that Customs administrations usually have to undertake their tasks in an environment of static or even declining resources, the risk management based approach outlined in the SAFE Framework enables Customs to act more efficiently and effectively. This approach coupled with early and accurate pre-arrival information allows Customs to allocate scarce control resources to shipments and actors in the supply chain which pose the highest risk to security and compliance while at the same time hastening the flows of legitimate and compliant trade.

Another critically important change brought about by the Framework relates to the role of and relationship with trade. Traditionally the cross-border movement of goods was seen as a compliance issue, however, the second pillar of the Framework introduces a fundamental change to how Customs and the trade community interact. It recognizes the importance of the role of trade in enhancing supply chain security and acknowledges the fact that cooperation between governmental authorities and the trading community will lead to benefits and best results for both parties.



Copyright © French Customs

SURVEY FINDINGS OF THE IMPLEMENTATION OF THE SAFE FRAMEWORK

In mid 2009, four years after the adoption of the instrument, the WCO Secretariat initiated a survey to take stock of the implementation of the SAFE Framework. The survey was based on a self-assessment exercise by WCO Members and focused on the first pillar of the Framework. Seventy-four WCO Members responded to the survey questionnaire.

The findings of the survey showed that WCO Members are clearly mobilized towards implementation of the SAFE Framework. It also confirmed that since the adoption of the

Framework there has been a shift in the approach of Customs administrations to border control. The traditional focus on imports had changed to an increased awareness of the need to focus attention on exports.

Another key finding indicated that a high percentage of WCO Members receive advance electronic information on their imports. Nearly all WCO Members indicated that they had some sort of an automated risk management system in place and that this system could be used for both threat assessment and targeting. The survey further showed that most responding Customs administrations were conducting outbound security inspections. In relation to the use of the latest inspection technologies, the results indicated that there have been significant investments in non-intrusive inspection technologies by responding Customs administrations.

The survey results also indicated that on-going capacity building through the WCO Columbus Programme and

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

the support provided by other international organizations is a prerequisite to achieve further implementation for many countries.

OUTSTANDING CHALLENGES

While the survey showed that WCO Members have been active in implementing the SAFE Framework, more still needs to be done.

In June 2008 the Customs community adopted a new strategic policy covering “Customs in the 21st Century” (C21). The 10 building blocks that form the basis of C21 draw from both the trade security and trade facilitation objectives of the SAFE Framework, and enshrine these concepts into the future working methods of Customs. One of the initiatives of the C21 strategy, namely, “Globally Networked Customs” (GNC) has direct linkages to the first pillar of the Framework, as one of its goals is to provide WCO Members with better capacity to collect, collate and exchange reliable information with each other for risk management purposes as early as possible in the supply chain.

Another challenge for Customs internationally has been the *ad hoc* approach to the application of risk management. To overcome this challenge the WCO is currently drafting a new Customs Risk Management Compendium, which will enable WCO Members to adopt a common methodology and approach for managing risks at all organizational levels.

In the field of outbound security filing and cargo examinations, there is a need to continue to modernize working methods. Likewise, there is an on-going need to further integrate technology solutions at all stages of the supply chain. In this regard, the WCO has developed tools such as the WCO Databank on Advance Technology and the WCO X-Ray Scanning Guidelines aimed at assisting WCO Members to build capacity in these areas. These tools are complemented by the yearly WCO Technology and Innovation Forum which provides a platform for the exchange of ideas to further increase the capacity of Customs administrations.

In relation to the second pillar of the SAFE Framework, the creation or on-going development of Authorized Economic Operator (AEO) programmes remains a priority with the development of Mutual Recognition Arrangements between WCO Members in the middle to longer term. However, providing tangible benefits to businesses at all stages in the supply chain remains a challenging goal. The WCO will continue to engage its Members on this issue and encourage them to offer such benefits as an incentive to the trade to play their part in securing the supply chain. This is now even more significant as 2010 is the WCO Year of the Customs-Business Partnership.

THE WAY FORWARD

Customs administrations are under mounting pressure as governments and citizens seek both economic and physical security from them through the rigorous application of the law. At the same time the international trade community looks for uniformity, predictability, transparency and efficiency in their dealings with Customs.

Through the full implementation of programmes such as the SAFE Framework of Standards and the wide scale adoption of standardized risk management techniques, Customs will be able to rise to the challenges posed by supply chain security and the wider border management environment.

The WCO has mapped out its path and is determined to ensure the security of international trade whilst facilitating the movement of legitimate goods based on the application of intelligence-driven risk management in partnership with its business stakeholders.

NOTE: Pictures courtesy of the World Customs Organization



Copyright © New Zealand Customs

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No.9/04

Supply Chain Security in the context of Aviation Security and Facilitation

*Halina M. Biernacki, Aviation Security and Facilitation Policy Section, Air Transport Bureau
International Civil Aviation Organization (ICAO)*

The world of transport today is truly a multimodal system and there is a definite need for an integrated, harmonized and comprehensive approach to ensuring the secure transport of persons and goods worldwide. Air transport has become an attractive target for various terrorist groups, as demonstrated by dramatic hijackings over the past several decades, the bombing of Pan Am flight 103 in December 1988, and the horrific terrorist attacks of 11 September 2001.



**Manas International Airport, Kyrgyzstan, July 2008
(OSCE/Eric Gourlan)**

Since then, the world community has made remarkable progress, through global cooperation, in containing acts of terrorism against civil aviation. ICAO initiated immediate action, including the review of existing security Standards contained in Annex 17 to the *Convention on International Civil Aviation*. The Organization also convened a High-level, Ministerial Conference on Aviation Security in February 2002, with an overall objective of preventing, combating and eradicating terrorism involving civil aviation, restoring public confidence in air travel and promoting the health of the air transport industry.

This historic Conference unanimously endorsed an ICAO Plan of Action for Strengthening Aviation Security, which was later approved by the Council of ICAO. The Plan includes a Universal Security Audit

Programme (USAP) and is complemented by a series of programmes and activities designed to help States comply with the Standards and Recommended Practices (SARPs) contained in Annex 17. One of the programmes involves the assessment of new and emerging threats to aviation security, in order to develop security measures for airports, aircraft and air traffic control systems.

Another serious threat to civil aviation is the use by terrorists of man-portable air defence systems (MANPADS). ICAO accords the highest priority to this particular threat. In light of the latest developments in the United Nations, as well as regional and national initiatives, the 36th Session of the ICAO Assembly adopted a Resolution on the threat to civil aviation posed by MANPADS.

The threat on an alleged terrorist plot involving liquid explosives to be carried on board civil aircraft flying across the North Atlantic, reported by United Kingdom authorities on 10 August 2006, once again emphasized the vulnerability of the global air transport system. This plot revealed a new modus operandi, calling for immediate action.

In response, the Council of ICAO adopted security control guidelines for screening liquids, aerosols and gels (LAGs), and these were conveyed to States for implementation. While security is the overriding priority, ICAO was also concerned with mitigating any adverse impact on the travelling public, airlines and airports, including duty-free and on board aircraft sales. A Secretariat Study Group on the Carriage and Screening of Liquids, Gels and Aerosols was convened to agree on specifications for tamper-evident bags (STEBs) that could be used to transport larger quantities of LAGs purchased at the airport or on board an aircraft. The Study Group developed detailed guidance material, to assist States in the implementation of the guidelines.

In order to develop multiple technological solutions for screening LAGs, a workshop was convened in Brussels in November 2009 to exchange information on possible new procedures and detection technologies under development. The workshop examined the likely consequences of various screening technologies on airport

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

operations and facilitation, mindful of the eventual need to remove volumetric restrictions in a coordinated manner.

Most recently, on 25 December 2009, a passenger on board Northwest Airlines flight 253 attempted to detonate an explosive device containing pentaerythritol tetranitrate (known as PETN) while the aircraft was in flight from Amsterdam to Detroit, in an attempt to bring down the aircraft. Following the incident, Ministerial-level regional conferences on aviation security were held in Mexico City (16 to 17 February), Tokyo (13 March), Abuja (11 to 13 April) and Abu Dhabi (1 to 2 June). These regional conferences resulted in the adoption of Joint Declarations on Aviation Security, representing each Region’s response to the latest attack on the air transport system.

In their Joint Declarations, States affirmed their commitment to prevent acts of unlawful interference with civil aviation in all its forms, with particular attention to countering terrorist threats posed to civil aviation. The conferences underscored the need to enhance international aviation security standards and measures in order to respond more effectively to new and existing threats. The Declarations recognized: the need to strengthen international cooperation in various efforts to enhance aviation security worldwide; the critical importance of sharing information on passengers, with due respect to their civil rights; and the role of technology in addressing the evolving threat.



Copyright © ICAO

Over time, the ICAO Aviation Security Programme has evolved and expanded in cooperation with member States and concerned international organizations. With regard to the judicial aspect of the Programme, there are five aviation security legal instruments, namely, the Tokyo Convention, The Hague Convention, the Montréal Convention and its Supplementary Protocol, and the *Convention on the Marking of Plastic Explosives for the Purpose of Detection*. These instruments have become the basis for international law and continue to rank among the most widely accepted multilateral international legal instruments. However, given new types of threats such as the acts committed on 11 September 2001, gaps and inadequacies appear to exist in the instruments. A Secretariat Study Group was appointed in 2006 to review existing air law instruments to determine whether they should be updated to address new and emerging threats to civil aviation such as the

use of aircraft as weapons of destruction and the spread of biological, chemical or nuclear substances, and to develop amendments as appropriate.

The Council of ICAO, at the sixth meeting of its 188th Session, on 30 October 2009, agreed to convene a Diplomatic Conference to finalize and adopt two draft instruments to amend The Hague and Montréal Conventions as recommended by the Legal Committee. The Conference is scheduled to be held in Beijing from 30 August to 10 September 2010.

The principal document giving direction on the establishment of security measures is Annex 17. Because this document sets the Standards for international aviation security worldwide, it is constantly evolving and is subjected to scrutiny before undergoing any changes. This document contains SARPs addressing air cargo security in order to prevent the placement of explosives on board aircraft, either through concealment in otherwise legitimate shipments or through gaining access to aircraft via cargo handling areas. To this effect, States are required to ensure the protection of cargo, baggage, mail and operator’s supplies being moved within an airport. In addition, States



Copyright © ICAO

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

are required to subject cargo, courier and mail intended for carriage on passenger flights to appropriate security controls, and to ensure that operators do not accept consignments of cargo on passenger flights unless their security has been accounted for by a “regulated agent” or they are subjected to other security controls.

The Council of ICAO, at the first meeting of its 190th Session on 17 May 2010, considered proposals for Amendment 12 to Annex 17. These proposals arise from the review of Annex 17 provisions conducted by the Aviation Security Panel related to, inter alia: security equipment; air traffic service providers; the application of random and unpredictable security measures; security measures for cyber threats; and cargo supply chain security. The proposed Amendment was conveyed to States for their comments. Amendment 12 to Annex 17, if adopted by the Council, will become applicable on 1 July 2011.



Copyright © ICAO Journal Vol.64 No.01

In order to assist States with the implementation of provisions contained in Annex 17, the seventh edition of the *Security Manual for Safeguarding Civil Aviation Against Acts of Unlawful Interference* (Doc 8973) has been and is available for distribution to all member States. The manual now comprises five volumes, each addressing a specific aviation security concern: Volume I – National organization and administration; Volume II – Recruitment, selection and training; Volume III – Airport security organization, programme and design requirements; Volume IV – Preventive security measures (which contains detailed material on the security of cargo); and Volume V – Crisis management and response to acts of unlawful interference.

Due to increased market demands in recent years, the volume of air cargo has grown significantly and is expected to continue to grow at a pace that will surpass the growth of passenger air travel. In this context, vulnerabilities in air cargo security place all air transport operations at risk. Since the Lockerbie incident and the terrorist acts of 11 September 2001, emphasis on enhancing the security of passenger flights has made the air cargo system more vulnerable and a likely target for terrorists. Today, air cargo is confronted by entirely new security threats, such as the placement of explosives in air cargo shipments or the use of aircraft as weapons of destruction. The security of air cargo has become one of the major global security concerns given the recognized vulnerabilities that make air cargo possibly the easiest target for terrorists.

In recent years, a variety of national, regional and international initiatives have taken place to counter threats to and vulnerabilities in air cargo. As the screening of all air cargo is not currently feasible due to limited technology and infrastructure, the most practical approach would be an application of risk management, which would enable the identification of high-risk shipments on which to concentrate controls. Among other procedural initiatives are the requirements for advance cargo information, expanding the use of authorized operators, and supply chain security.

In order to provide guidance to States in implementing effective national aviation security programmes, ICAO has developed air cargo security procedures that reflect a cost-effective and pragmatic approach, based on three main principles; first, that aircraft must operate from within a secure environment; second, that every consignment must be subjected to security control, with a maximum focus on the screening of cargo whose security cannot be readily assessed before being placed on board a passenger aircraft; and third, that once cargo has received security clearance, it must be protected from interference. It should be noted that the main rationale for preventive security measures is that if the consignment was packed in a secure environment and is kept secure thereafter, there is no need to search it.

ICAO recommends that both the aircraft operator and the regulated agent perform random checks on cargo

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

declared as secure in order to determine that the information provided in the accompanying documentation is accurate. The proportion of cargo randomly inspected should depend on the perceived level of threat. ICAO also recommends that regulated agents be subjected to inspection and supervision by appropriate national authorities.

With regard to cargo, more work is needed on the development of internationally strengthened and harmonized measures and best practices for air cargo security, taking into account the need to protect the entire cargo supply chain. Solutions should be developed with due consideration for their impact upon air transport and trade. Future security measures should be effective, affordable and practical. Only such measures, together with a workable authorized operator and a secure supply chain mechanism, can provide reliable guarantees of effective security in the air cargo system.

A Secretariat Study Group composed of members of the Aviation Security Panel and Facilitation Panel has been established to examine the possibility of developing security standards by which air cargo operators, agents, airports and ground handlers may be certified as authorized entities or regulated agents. The first meeting of the Study Group was held in St. Julian's, Malta on 15 December 2009 and made proposals for new Standards for inclusion in Amendment 12 to Annex 17, and defined its future work. The report of the Study Group was considered by the Facilitation Panel at its sixth meeting, held in May 2010. It was stressed that the World Customs Organization's "Framework of Standards to Secure and Facilitate Global Trade" (June 2005) is important for the work of the Study Group. To further the work on this subject, cooperation between the Aviation Security and Facilitation Panels is essential. The Facilitation Panel thus recommended that the Study Group identify elements common to both customs and supply chain security. The second meeting of the Study Group is planned to be held later this year.

The 37th Session of the ICAO Assembly, to be held from 28 September to 8 October 2010, is expected to adopt amended Assembly Resolution A36-20 — *Consolidated statement of continuing ICAO policies related to the safeguarding of international civil aviation against acts of unlawful interference*, revised in light of new developments in the field of aviation security, including the incident of 25 December 2009. This Resolution would reaffirm the critical importance of aviation security as one of the programmes being accorded the highest priority in the ICAO work programme.

The Assembly is also expected to adopt the ICAO Comprehensive Aviation Security Strategy for the next two triennia, to succeed the Aviation Security Plan of Action adopted following the events of 11 September 2001 to address challenges posed to aviation security. The proposed strategy comprises the following seven focus areas: addressing new and existing threats; promoting innovative, effective and efficient security approaches; promoting the sharing of information amongst and within member States to raise awareness of threats and aviation security trends; promoting global compliance and establishing sustainable aviation security oversight capability of States; improving human factors and security culture; promoting the development of mutual recognition for aviation security processes; and emphasizing the importance of security amongst States and stakeholders.



CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

Security Provisions Related to the Carriage of Dangerous Goods

*Gustav Kafka, Deputy to the Secretary General
Intergovernmental Organisation for International Carriage by Rail (OTIF)*

INTRODUCTION

The aim of the international system of regulations for the carriage of dangerous goods, the most important basis of which are the UN Recommendations on the Transport of Dangerous Goods - Model Regulations, which apply to all the modes, is to ensure the safety of people, property and the environment (1). In this system of transport safety, security provisions, which are part of the system for maintaining international and national public order and safety, really constitute a *lex fugitive* (2).

The reason provisions concerning security were nevertheless included in the UN Model Regulations following the events of 11 September 2001 was mainly that these Regulations

- ◆ are adapted to ongoing developments, particularly in the technical field, every two years, i.e. relatively quickly for international regulations,
- ◆ are designed for all transport modes so that, unlike the general transport sector, there can be no gaps or loopholes in terms of requirements in the supply chain between air and sea transport on the one hand and inland transport on the other,
- ◆ are recommendations and so are not directly legally binding, but as they are conceived as model regulations, in principle they are worded in such a way that they can be transposed into legally binding regulations virtually unchanged, and
- ◆ are transposed with exemplary discipline and in active cooperation with the organizations concerned into mandatory regulations at governmental level, mostly word for word and using the latest version in each case.



*Tank truck to transport dangerous liquid loads, Batumi International Container Terminal, Georgia May 2010
(OSCE/Mehdi Knani)*

This is done by means of separate international conventions between States for the various modes. The UNECE deals with the conventions for transport by road – **ADR** (3) and inland waterways – **AND** (4), OTIF for transport by rail – **COTIF RID** (5), ICAO for air transport – **ICAO TI** (6) and IMO for maritime transport – **IMDG Code** (7).

Probably to deal with the concerns about inappropriately placing the security provisions in with the safety provisions, almost all the security provisions have been put together in one chapter of the regulations; in the UN Model Regulations and the IMDG Code, this is Chapter 1.4, in the ICAO TI it is Part 1, Chapter 5, and in ADR, RID and ADN it is Chapter 1.10.

It has also been deemed appropriate to consider transport security as a sub-set of safety provisions, which is given expression in the definition of (dangerous goods) security: according to the definition, security means “measures or precautions to be taken to minimize theft or misuse of dangerous goods that may endanger persons, property or the environment”.

HIGH CONSEQUENCE DANGEROUS GOODS

As international opinion was that in the carriage of dangerous goods safety provisions, classifying goods in “classes” on the basis of physical, chemical or otherwise determined hazardous properties were insufficient for the purposes of security, which has other protective aims and threat scenarios, as mentioned above, the proposed security measures were sub-divided into those applicable to all dangerous goods in quantities above a very small amount and those for which special additional security measures must be taken.

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

The goods subject to such special measures were called “high consequence dangerous goods” (HCDG) and they were defined as those which have the potential for misuse in a terrorist incident and which may, as a result, produce serious consequences such as mass casualties or mass destruction. The particular goods concerned from each Class have been listed in a table. Typical HCDG are explosives, toxic gases, and highly infectious, toxic, acid or radioactive substances.

Security provisions applicable to all dangerous goods

1. Personal responsibility

All persons engaged in the carriage of dangerous goods must consider the security requirements set out in the Chapter on security commensurate with their responsibilities. In this context, the term “persons” means every individual physical person with his/her personal responsibility.

2. Reliability of partners

Although the provisions only refer to reliability in relation to carriers, to whom dangerous goods must only be offered for carriage if they have been properly identified and that for this purpose, each crew member of a train (vehicle, vessel) carrying dangerous goods must carry with them means of identification, which includes their photograph, during carriage, in practice this measure must be extended to cover all partners. In the interest of security, carriers for example might also have to assure themselves that the persons from whom they receive a job or load are reliable.

3. Secured infrastructure

As these provisions, which require that areas within temporary storage terminals, temporary storage sites, vehicle depots, berthing areas and marshalling yards used for temporary storage during carriage of dangerous goods must be properly secured, well lit and, where possible and appropriate, not accessible to the general public, may entail not insignificant costs for those operating such infrastructure, the word “appropriate” is important here. As for other security measures, a risk analysis must also form the basis here.



Copyright © Port of Rotterdam

Security provisions applicable to high consequence dangerous goods

1. Security plan

Such a plan applies to participants (consignor, packer, loader, carrier etc.) engaged in the carriage of high consequence dangerous goods and shall address *inter alia* the following tasks:

- list all dangerous goods concerned,
- allocate responsibilities for security to competent and qualified persons with appropriate authority,
- review current operations and assess security risks,
- reduce security risks (by training, policies, operating practices, equipment, resources),
- report on and deal with security threats, breaches of security or incidents,
- evaluate, test and update security plan,
- ensure physical security of the transport information contained in the security plan and
- limit distribution of information relating to the transport operation contained in the security plan to those who need to have it. Such measures shall not preclude the provision of information required elsewhere in the provisions of ADR, RID or ADN.

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

2. Theft prevention

This measure includes the following tasks:

- apply devices/equipment/arrangements to prevent theft of train/vehicle carrying high consequence dangerous goods and its cargo,
- ensure that these devices etc. are operational and effective at all times. The application must not jeopardize emergency response. It might be a problem in this respect to load containers to avoid opening the doors “back to back”, because the emergency services find it much harder to deal with this than removing a seal, and
- use when appropriate and already fitted, transport telemetry or other tracking methods or devices to monitor the movement of high consequence dangerous goods.

Role of the safety adviser

The safety adviser must be appointed by undertakings, the activities of which include the carriage, or the related packing, loading, filling or unloading of dangerous goods and is responsible for helping to prevent the risks inherent in such activities with regard to persons, property and the environment. In so doing, in connection with his obligation to monitor a number of practices and procedures relating to the relevant activities of the undertaking, he must also ensure, *inter alia*, that if a security plan is prescribed within the undertaking, it is available. However, it is not the safety adviser who is responsible for the content of the security plan, but the management of the undertaking.

Official checks

1. Spot checks

The checks during transport prescribed in the provisions on the transport of dangerous goods to be carried out by independent official bodies must cover appropriate security measures. This has the advantage that such checks imply the right to stop such traffic routinely, i.e. without any specific suspicions.

2. Checks within undertakings

The competent authorities for the carriage of dangerous goods may also, for the purposes of carrying out checks on the premises of the enterprises participating in the carriage of dangerous goods as consignors, packers, loaders, carriers etc., make inspections, consult the necessary documents and remove samples of dangerous goods or packagings for examination, provided that safety is not jeopardized thereby. The authorities may, if they deem necessary, designate a person from the enterprise to accompany the representative of the competent authority. A check on security concerns can also be incorporated into the dangerous goods checks in this case.



A specialized railway tank holding toxic rocket fuel component mélange, Ukraine, November 2009 (OSCE/Susanna Lööf)

Role of the railway infrastructure manager

1. Emergency plans for marshalling yards

The aim of these emergency plans prescribed for the carriage of dangerous goods is that in the event of an accident or incident in marshalling yards, all those involved must co-operate in a co-ordinated way and the consequences of the accident or incident for human life or for the environment must be minimized to the greatest possible extent. Obvious security threats or infringements must be included in the emergency situations covered by the plans.

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

2. Exchange of information between railway infrastructure manager and carrier

The railway infrastructure manager must ensure that he has rapid and unrestricted access to the following information at any time during carriage:

- composition of the train,
- UN numbers of the dangerous goods being carried,
- position of these wagons in the train,
- mass of the load.

In order that the railway infrastructure manager can fulfil this obligation, the carrier must ensure that the manager of the railway infrastructure being used is able to obtain at any time during carriage rapid and unrestricted access to the information mentioned above. This information must only be disclosed to those parties that require it for safety, security or emergency response purposes. This addresses the issue that the requisite transparency of dangerous goods information for security purposes, which also serve the markings, labels and documentation, can at the same time lead to vulnerability in relation to security, a conflict of interests which needs to be balanced out.

Training

Persons employed by consignors, packers, loaders, carriers etc., whose duties concern the carriage of dangerous goods, must receive training in the requirements governing the carriage of such goods appropriate to their responsibilities and duties. Training requirements specific to the security of dangerous goods must also be addressed.

CONCLUDING REMARK

Despite the advantages in some respects of incorporating security provisions into the established system of dangerous goods transport safety provisions in this special case, it should not be forgotten that with regard to responsibilities at the national level, the carriage of dangerous goods and security can be widely separated. Thus at the international level, consideration still needs to be given to establishing a system of mandatory regulations comprising all these responsibilities.

NOTES

(1) see http://www.unece.org/trans/danger/publi/unrec/rev16/English/00E_Recommendations.pdf

(2) Literally: escaped law, i.e. a statutory rule concealed within a law which deals with other matters in terms of content and its description

(3) European Agreement concerning the International Carriage of Dangerous Goods by Road, see: <http://www.unece.org/trans/danger/publi/adr/adr2009/09ContentsE.html>

(4) European agreement concerning the international carriage of dangerous goods by inland waterways, see: http://www.unece.org/trans/danger/publi/adn/adn2009/09files_e.html

(5) Regulation concerning the International Carriage of Dangerous Goods by Rail, see: http://www.otif.org/fileadmin/user_upload/otif_verlinkte_files/07_veroeff/02_COTIF_99/RID-1999-e.PDF
<http://www.otif.org/en/navi-top/login/publications/rid-2009.html>

(6) Technical Instructions for the Safe Transport of Dangerous Goods by Air, see: <http://www.icao.int/icaonet/dcs/9284.html>

(7) International Maritime Dangerous Goods (IMDG) Code, see: http://www.imo.org/Safety/mainframe.asp?topic_id=158

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", *OSCE Ministerial Council Decision No. 9/04*

Container Security: How the OSCE engages with International Partners to Prevent Terrorism

Mehdi Knani, Action against Terrorism Unit
OSCE Secretariat, Vienna

In the wake of the 9/11 terrorist attacks against the United States, governments around the world became increasingly concerned over possible targeting or misuse of the container transport system by terrorists, for instance to deliver a weapon of mass destruction. This mobilized the international community to better secure the system. Several countries launched national programmes with the dual goal of securing container transport and at the same time making it more efficient, the United States taking the lead with its *Customs-Trade Partnership against Terrorism*. Specialized global organizations, such as the World Customs Organization (WCO), the International Maritime Organization (IMO) and the International Civil Aviation Organization began addressing the issue and developed international standards on their pieces of the container transport security puzzle.

The OSCE, for its part, rallied to build political will in support of these initiatives. Participating States mandated the Secretariat to promote the exchange of information and best practices on container security, and to lend support to efforts in this field by international organizations. In 2005, the OSCE became one of the first organizations to endorse the *WCO Framework of Standards to Secure and Facilitate Global Trade (SAFE)*.

OSCE commitments on container and supply chain security

Sofia, 2004: Ministerial Council Decision No. 9/04

"[The Ministerial Council] decides that OSCE participating States will act without delay in accordance with their domestic legislation, and necessary resources available, to enhance container security, based on best practices and on norms and standards to be agreed internationally."

Ljubljana, 2005: Ministerial Council Decision No. 6/05

"All OSCE participating States should take measures recommended in the *WCO Framework of Standards to Secure and Facilitate Global Trade* as soon as possible. [...]"

Madrid, 2007: Ministerial Statement on Supporting the United Nations Global Counter-Terrorism Strategy

"The OSCE will continue its activities aimed at promoting supply chain security, especially by supporting and facilitating the capacity-building work of the World Customs Organization in implementation of the *Framework of Standards to Secure and Facilitate Global Trade* and will endeavour to serve as a platform for co-ordination and co-operation between relevant international organizations and national authorities for the development and application of an integrated approach to supply chain security."

Madrid, 2007: Ministerial Council Decision No. 5/07

"[The Ministerial Council] decides to task the Secretary General and OSCE institutions to continue to promote the involvement of the private sector (civil society and the business community) in their counter-terrorist activities, where relevant and appropriate."



THE OSCE AS A TRANSMISSION BELT

The OSCE's role in promoting container security is typical of how a regional organization can add value to global counter terrorism efforts. This may be best described by the concept of a 'transmission belt' between the global and national levels. Regional organizations can help channel downwards objectives, approaches and measures agreed upon at the global level. They can serve as a multiplying force by supporting the outreach and capacity building activities of specialized global organizations within their respective regions.

The ATU's close collaboration with the WCO in support of the *SAFE Framework* is a case in point. Under the *WCO Columbus Programme*, the ATU has helped to organize national *SAFE* workshops for five OSCE participating States, enabling the countries to draw up strategic action plans for implementing the *SAFE Framework*.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

The OSCE is now considering how it could provide assistance for specific actions under these national plans, such as providing equipment and supporting cross-border co-operation.

Another track followed by the ATU has been to promote the *Code of Practice on Security of Ports*, developed jointly by the International Labour Organization (ILO) and the IMO. ILO first engaged with the ATU at an OSCE Technical Expert Workshop on Container Security organized in Vienna in 2005. ILO asked the ATU to help promote the *Code of Practice* and the ATU suggested to expand the related training package to also cover the work of other organizations. A modified package, that included information on the WCO, the European Commission, the International Atomic Energy Agency and the United States government was tested a year later at a joint OSCE/ILO training workshop in Istanbul.

PLATFORM FOR CO-OPERATION

The global supply chain is complex and securing it requires a comprehensive vision and coherent action. In 2007, participating States encouraged the OSCE to serve as a platform where international organizations and national authorities could join forces to develop an integrated approach to supply chain security. They also gave the Organization a mandate to promote co-operation between state authorities and the private sector in countering terrorism.

The ATU put this into practice for the first time by organizing the *Workshop on an Integrated Approach to Supply Chain Security for the Mediterranean Region* in December 2009 in Malta. In addition to experts from 17 countries, including five OSCE Mediterranean Partners for Co-operation, 20 international organizations and private sector associations attended the workshop. A review of the full picture of current international, regional and key national initiatives on supply chain security stimulated reflection on the best way forward to make it as cost-effective and consistent across the different modes of transportation as possible. Building on the workshop's success, the ATU is now offering to organize similar events for other sub-regions of the OSCE.

LOOKING AHEAD

The workshop in Malta also opened a new door for co-operation with the United Nations Office on Drugs and Crime (UNODC), which manages a Container Control Programme (CCP) jointly with WCO. The CCP helps developing countries train law enforcement officials to identify and inspect high-risk freight containers, in order to prevent illicit trafficking. The CCP started with a focus on key ports in Latin America and Africa and as its implementation is now moving east, UNODC decided to engage with the OSCE.

To begin with UNODC and ATU have agreed to work together in response to an assistance request from Georgia. The ATU facilitated a needs assessment visit to Georgia by a team of UNODC and WCO experts in May 2010. The team held several meetings with law enforcement agencies in Tbilisi and visited the ports of Batumi and Poti on the Black Sea. The findings of the mission now serve as a basis to define modalities for implementing the CCP in Georgia, and deciding how the OSCE can help further.

ATU co-operation with the WCO is also expanding. The ATU was recently granted observer status to the *SAFE Working Group*, which meets twice a year at the WCO to discuss implementation progress and possible improvements of the *SAFE Framework*. The ATU has also started supporting WCO workshops for the European region on key *SAFE* standards. In June 2010, it co-sponsored a workshop at the St. Petersburg branch of the Russian Customs Academy, on the use of non-intrusive inspection technologies by customs to scan suspicious containers.

Securing container shipments to deter illicit trafficking remains a priority for the international community. Significant progress has been achieved, but there is still much work ahead. The ATU's engagement with international partners to make sure that existing tools are used and countries receive the assistance they need to enhance container security is typical of the Unit's approach in all its eight thematic programmes.

NOTE: this article is an adaptation of a contribution to the OSCE Magazine, [Issue Number 2/2010](#), which focused on the OSCE's external co-operation with other organizations and institutions.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No. 9/04

Land Transport Security Challenges. How can the OSCE Respond?

*Gabriel Leonte and Roel Janssens, Economic and Environmental Advisers
OSCE Secretariat, Vienna*

Producers, consumers, transport operators and ultimately national economies rely on the constant and predictable flow of goods. Therefore, it is of crucial importance to reduce obstacles to legitimate trade flows and at the same time minimize risks. With globalization, strengthening transport security becomes a stringent necessity.

THE OSCE'S MANDATE

As early as 1975 when the *Helsinki Final Act* was adopted, the CSCE (later on OSCE) participating States considered that the improvement of the transport conditions constitutes one of the factors essential to the development of their co-operation.

The OSCE's attention to transport received strong emphasis in 2003 with the *OSCE Strategy Document for the Economic and Environmental Dimension* adopted at the Maastricht Ministerial Council. In this document, the OSCE participating States identified transport as a priority area for co-operation and encouraged the "development of transport networks in the OSCE region which are efficient and integrated, free of avoidable safety and security risks and sensitive to the environment."



A session of the 18th OSCE Economic and Environmental Forum in Prague focused on Transport Security Aspects and the Role of the OSCE, 26 May 2010 (OSCE/OCEEA)

In recent years, transport-related themes have been quite high on the agenda of the annual OSCE Economic and Environmental Forum. Through its annual Forum process, the OSCE aims at offering an inclusive platform for political dialogue, for networking between stakeholders, for discussing relevant issues and suggesting solutions and follow up actions.

In 2006, 2008 and 2010, the respective Forums were dedicated to "Transportation in the OSCE area: Secure transportation networks and transport development to enhance regional economic co-operation and stability", "Maritime and inland waterways co-operation in the OSCE area: Increasing security and protecting the environment" and "Promoting good governance at border crossings, improving the security of land transportation and facilitating international transport by road and rail in the OSCE region".

Based on the recommendations of the Forums, Ministerial Council Decisions were adopted in Brussels in 2006 and Helsinki in 2008.

In the Brussels *Ministerial Council Decision No. 11/06 on Future Transport Dialogue in the OSCE*, the participating States considered that, within its comprehensive approach to security, the OSCE could make contributions in the field of transport inter alia: "by encouraging the development of stronger partnerships between participating States and with relevant international bodies that focus on transport, in particular transport development and transport security" and "by promoting a wide dissemination and implementation of best practices and standards developed by relevant organizations in the field of transport security".

Through the adoption in Helsinki of the *Ministerial Council Decision No. 9/08 on Follow-Up to the Sixteenth Economic and Environmental Forum on Maritime and Inland Waterways Co-operation* OSCE participating States acknowledged "the growing challenges related to the environment and security aspects of maritime and inland waterways co-operation, and the need to step up regional, subregional and inter-regional efforts, among others in addressing the challenges and opportunities related to the development of efficient

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

multimodal transport corridors” as well as “the multifaceted aspects of maritime security, including supply chain security”. Additionally the Ministerial Council Decision called upon participating States to apply and share best practices and technological solutions in this field.

THE OSCE’S WORK

The OSCE has sought, in close co-operation with partners such as the UNECE, to address these issues by **promoting good governance in customs and in other border agencies** and by facilitating the exchange of good practices between our participating States. As transport and border crossing comprise a wide range of aspects, the OSCE's approach has been based on multiple pillars, such as supporting the implementation of relevant regulatory documents, the promotion of good governance, transit transportation development, regional co-operation, public-private dialogue and co-operation as well as the need to involve the private sector as an equal partner thereby fostering cross-border trade.

There are various economic and governance issues related to border crossing procedures such as the high economic costs of non-physical barriers to trade and transport, the need to reduce border crossing delays by harmonizing border and customs formalities and stimulating cross-border co-operation measures while at the same time increasing the efficiency-level of security measures and adopt **risk management based approaches** including profiling and selectivity etc.

The OSCE has organized regional seminars to discuss the implementation in South Eastern and Eastern Europe and the South Caucasus and Central Asia of the following international legal instruments, designed to tackle these issues:

- ◆ UNECE International Convention on the Harmonization of Frontier Control of Goods ('Harmonization Convention')
- ◆ World Customs Organization revised Kyoto Convention on the Simplification and Harmonization of Customs Procedures
- ◆ World Customs Organization (WCO) SAFE Framework of Standards to Secure and Facilitate Global Trade

In close co-operation with the Transport Division of the UNECE and the World Customs Organization (WCO) the OSCE offers national, tailor-made technical assistance. Such assistance seminars have recently been organized in Kazakhstan, Turkmenistan and Uzbekistan. Requests for similar activities have been received from other countries and are currently under preparation.



As part of preparations for a handbook of best practices, the OSCE conducted an assessment visit at the Ak-Jol/Korday border crossing point between Kazakhstan and Kyrgyzstan on 22 October 2008. (OSCE/Roel Janssens)

THE 2010 OSCE ECONOMIC AND ENVIRONMENTAL FORUM PROCESS

Recently, the transportation sector has been facing challenges from all sides. The sector has been hit hard by the global economic downturn. In many countries and regions, physical and non-physical barriers continue to hamper transport and trade, causing delays and unnecessary costs.

Reacting to that, the Forum's theme under the Chairmanship of Kazakhstan in 2010 was once again related to transport - "Promoting good governance at border crossings, improving the security of land transportation and facilitating international transport by road and rail in the OSCE region".

The concluding meeting of the Forum process took place in Prague in May, following the first part of the Forum, in February in Vienna. The process also included two preparatory Conferences in Astana and Minsk, in October 2009 and March 2010 respectively.

The security of the international transport circuit has been one of the main building blocks of this year's Forum process. In trying to address this complex and challenging task the OSCE strongly relied on the

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

expertise and co-operation of organizations such as the United Nations Economic Commission for Europe (UNECE), the World Customs Organization (WCO), the UN Conference on Trade and Development, the Transport Asset Protection Association (TAPA), the International Road Transport Union (IRU) and the International Union of Railways (UIC) to name just a few. Experts and policy makers, representing different transport sectors and various disciplinary fields including private sector, have been invited to share their views along the meetings of the Forum process.

At the outset, a number of key questions were identified:

- What are the vulnerabilities of land transport from a security perspective?
- What are the preconditions to ensure secure and sustainable transport operations?
- How can transport be more secure while remaining cost-efficient and competitive?
- What should be the responsibilities and roles of all those involved in transport operations – both public authorities and private sector?
- How can the commonly agreed standards or instruments be implemented more effectively?
- How could the OSCE contribute to strengthening co-operation at all levels?

TRANSPORT SECURITY: CARVING OUT THE OSCE’S ROLE

In addition to the challenges described above international terrorism and transnational organized crime also pose serious threats to the transport sector. Recent years have seen ruthless terror attacks on trains and urban transport means – in Madrid, London and the Russian Federation, with tragic results. Many more -- *fortunately unsuccessful* -- attempts have not made the headlines, but the risk is ever present.

Furthermore, the complex range of security risks facing inland transport include thefts of vehicles and of high-value goods, illegal border crossings, smuggling people and/or weapons, the trafficking of dangerous substances and/or hazardous waste, attacks on critical transport infrastructure such as tunnels and bridges causing disruptions in the distribution and supply chain networks.



*A train speeds across the dry land of southern Tajikistan.
(OSCE/Astrid Evrensel)*

Through the increasing amounts of hazardous waste, the global economy has witnessed a flourishing waste-trade, which has raised a number of questions with regard to the security repercussions, both human and environmental, of such transactions.

The possibility of associating such illegal activities with money laundering and using such revenue to fund further organized crime or even terrorist activities deserves probably more attention.

Transport systems are interconnected in today’s global economy and often referred to as the global supply chain. A common wisdom is that this supply chain is as vulnerable as its weakest link.

Relative to maritime ports and airports, inland transportation strikes many as being under-protected. Land-based transport (covering road and railways) is considered by many to be the **weakest link in securing the international supply chain** while at the same time it is both a *vehicle* (often in the literal sense) as well as a *target* for terrorist attacks.

When looking a bit deeper into the issue, the following observations can be made:

There seems to be a **lack of inter-governmental bodies** dealing specifically with **land transport security**. While the security arrangements of civil aviation and maritime transport are regulated by ICAO and IMO respectively, inland transport remains largely a national policy matter. Whereas the security rules and standards in maritime and aviation sectors are clearly defined and decided within the respective intergovernmental regulatory bodies, such a harmonized and cooperative approach seems to be lacking in the land transport sector.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

In addition, security in the land transport sector, as opposed to in other segments of the supply chain, is highly fragmented in terms of number and nature of actors involved (transport authorities, customs, police, as well as the private sector to name just a few). Improving collaboration between these actors is therefore an absolute necessity.

As well, the lack of a unified, co-ordinated approach can also be explained by the fact that there are no harmonized regulatory frameworks, legal instruments and conventions available that cover land transport security in its entirety. **The OSCE as a political organization could be well placed to support UNECE and others in their endeavours to create a harmonized set of rules and regulations that could possibly fill this gap.**

While security measures need to be tailored to specific situations and/or transport modes, a number of key general conclusions can be drawn, as they emerged from the 18th OSCE Economic and Environmental Forum process, such as:

- The need for adopting a comprehensive and integrated approach to supply chain security;
- The need for further balancing security and facilitation as the key to sustainability;
- The importance of putting a stronger emphasis on preparedness and resilience;
- The importance of information-sharing and the necessity of ensuring multi-stakeholder co-operation including public-private partnerships and interagency co-ordination, nationally as well as across borders;
- Fostering national implementation of existing international standards while considering the incorporation of new security provisions in existing legally binding instruments.

THE WAY AHEAD

One thing is for sure, there is a need for further dialogue on these issues at both expert and political levels. In this regard, a key recommendation for continued OSCE involvement is included in the 2010 *UNECE Review of the implementation of OSCE commitments in the economic and environmental dimension* which was presented on the occasion of the Concluding Part of this year’s Forum process in Prague from 24-26 May 2010. The UNECE Transport Division called upon the OSCE to establish jointly an **Inland Transport Security Discussion Forum** that would meet annually.

In this context it is important to note that the UNECE has been administering for a number of years an inland transport security expert group and organized a number of conferences in this sphere. Given the fact that a lot remains to be done in order to make inland transport security more effective it now reaches out to the OSCE to join forces.

Among others, the participants in the expert group deliberations identified the following key transport security issues as those that are most pressing and those that require further discussion and elaboration:

- In the transport security sphere the division of responsibilities between the public and private sector, consequently it is unclear who should pay for increased security!?
- Transport security norms, standards, procedures and rules need to be further developed and knowledge on the tools that already exist should be enhanced.
- Risk assessment techniques, allowing for a balance between security and facilitation, are insufficiently known and/or underutilized.
- Best practice sharing is one of the best ways to enhance transport security, countries can learn from each other. The OSCE jointly with the UNECE could play a role in providing a forum for exchange.

IN CONCLUSION

With its membership of 56 participating States and its broad security mandate, the OSCE is well placed to identify and address political problems and contribute to the ongoing international efforts in this field. Our aim should be to promote a comprehensive, integrated approach that would involve the public and the private sector, along with relevant international organizations. In doing so, the OSCE would not duplicate existing efforts and initiatives. On the contrary. In this regard, the 2010 Economic and Environmental Forum process is a good example, as it has been designed to provide an opportunity to strengthen points of synergy and deepen co-operation.

With this in mind, the OSCE should stand ready to continue contributing to the issue of inland transport security, including in a more systematic and institutionalized format as proposed for by the UNECE.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

Maritime Supply Chain Security, IMO's perspective

*Graham Mapplebeck, Head Facilitation Section, Maritime Safety Division
International Maritime Organization (IMO)*

“The mission of the International Maritime Organization (IMO) as a United Nations specialized agency is to promote safe, secure, environmentally sound, efficient and sustainable shipping through co-operation. This will be accomplished by adopting the highest practicable standards of maritime safety and security, efficiency of navigation and prevention and control of pollution from ships, as well as through consideration of the related legal matters and effective implementation of IMO's instruments with a view to their universal and uniform application.”

IMO presently consists of 169 Member States and three Associate Members, plus some 61 Inter-Governmental Organizations and 75 Non-Governmental Organizations with Observer status who provide valuable expert input to the Organization. IMO's main task has been to develop and maintain a comprehensive regulatory framework for international shipping and its remit today includes safety, environmental concerns, legal matters, technical co-operation, maritime security and the efficiency of shipping. The result is a comprehensive body of international conventions, supported by hundreds of recommendations governing every facet of shipping.



Poti Seaport, Georgia, May 2010 (OSCE/Mehdi Knani)

There is a high priority given by IMO both to the security of ships and port facilities, and to the complementary issue of facilitating international maritime traffic; reflecting the continuing need for the Organization, and the maritime community as a whole, to sustain efforts to enhance and improve security in all aspects of ship and port operations while, at the same time, ensuring that the flow of seaborne trade continues to be smooth and efficient, and that the movement by sea of persons is not unduly impeded.

MARITIME SECURITY

Since the 1980s IMO has developed international treaties, guidelines and recommendations on measures to prevent unlawful acts against passengers and crew on board ships. Whilst the

protection of international shipping was raised first, within IMO, in the context of the enhancement of security, the safety of navigation and the protection of the environment are integral parts of the process and the work of IMO, intertwined and inseparable. None of them can exist without the simultaneous co-existence of the others. Ships need a climate of security in order to conduct their trade safely and, in doing so, not to present any unnecessary threat to the marine environment.

In December 2002, an International Diplomatic Conference under the auspices of IMO adopted amendments to the International Convention for the Safety of Life at Sea, 1974 (SOLAS) and the International Ship and Port Facility Code (ISPS), the first step in establishing an international framework through which maritime security would henceforth be addressed. These special measures to enhance maritime security (i.e. chapter XI-2 of the 1974 SOLAS Convention and the ISPS Code) entered into force on 1 July 2004. Today the IMO measures apply to 159 States, the combined merchant fleets of which constitute over 99 % of the gross tonnage of the world's merchant fleet and the number of port facilities involved is in excess of 10,000.

The measures adopted by IMO aim towards establishing a security conscious culture amongst seafarers, ship owners, ship operators, maritime sector services providers and port facility operators, users and services providers and focus on enhancing awareness and vigilance.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

The maritime security provisions of SOLAS chapter XI-2 and the ISPS Code are part of a wider initiative to counter terrorism, including action by the Counter Terrorist Committee of the UN Security Council, co-operation with the World Customs Organization (WCO) on container security, joint initiatives with the ILO on port security and identification documents etc.

The 2002 SOLAS Conference resolution 9, which recognized the inter-modal and international nature of the movement of closed cargo transport units (closed CTU) and the need to ensure security throughout the supply chain also invited the WCO to consider urgently measures to enhance security throughout international movements of closed CTUs. The WCO Council subsequently adopted in June 2005 the Framework of Standards to Secure and Facilitate Global Trade (Framework of Standards), and then ultimately the SAFE Framework of Standards in June 2007.

The overall objectives of the ISPS Code are to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade. It establishes their respective roles and responsibilities and ensure the early and efficient collection and exchange of security-related information.

IMO has also established co-operation with the International Labour Organization on the issue of seafarer identification, and has signed a Memorandum of Understanding with the World Customs Organization, mainly aimed at strengthening co-operation in the fields of container examination and integrity in multimodal transport and matters relating to the ship/port interface.

The IMO Maritime Safety Committee (MSC), its 82nd session in November 2006, and the Facilitation Committee (FAL), established a Joint MSC/FAL Working Group which began work on container and supply chain security, with a view to ensuring that the right balance is struck between enhanced security and the facilitation of maritime traffic. In its work, the Group took into account the aforementioned WCO SAFE Framework of Standards to secure and facilitate global trade. The Joint Working Group identified the following guidance for IMO Member States.



Cargo port of Tukmenbashi on the Caspian Sea, Turkmenistan, July 2009 (OSCE/Martina Gadotti)

Member States, either as SOLAS Contracting Governments or as FAL Contracting Governments, or both, developing guidance on the implementation of the FAL Convention and SOLAS chapter XI-2 and the ISPS Code, in the context of the SAFE Framework of Standards, should include statements to the effect that:

1. SOLAS chapter XI-2 and the ISPS Code sufficiently set out the requirements on ships and port facilities with respect to the security and facilitation of the movement of closed cargo transport units and of freight containers transported by ships, taking into account the appropriate references in the ISPS Code;
2. The WCO has primacy over supply chain security, with IMO's role being limited to those aspects related to ships and port facilities;
3. Port facilities and ships are not responsible for maintaining the physical integrity of closed cargo transport units and of freight containers other than those in their custody;
4. The SAFE Framework of Standards, including the risk-based cargo security strategy set out therein, should be taken into account in policies and practices with respect to the FAL Convention, SOLAS chapter XI-2 and the ISPS Code; and
5. Communication, co-ordination and co-operation at both national and local levels, between ships, port facilities, Customs and other competent authorities are of the utmost importance.

IMO through the Maritime Safety Committee and its subsidiary bodies are continuously working on additional elements of and guidance for the mandatory requirements, i.e. Ship Security Alert Systems, long range

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

identification and tracking of ships, control and compliance measures, training and certification of security officers, etc.

Although the global security net, which chapter XI-2 and the ISPS Code aim at, has been established, there is a need to strengthen it further and to ensure its continued robustness on a long-term basis. With a view of addressing difficulties and practical issues relating to the implementation of the provisions of SOLAS chapter XI-2 and of the ISPS Code and so as to ensure the uniform, harmonized and consistent implementation of their requirements, between May 2003 and May 2010, the IMO Maritime Safety Committee, in some cases jointly with the Facilitation Committee, has adopted, and updated, some 40 pieces of amendments to existing mandatory, performance standards, guidance and recommendations which are still in effect.



Rotterdam Port Key: access key for dedicated Port Businesses and Port Officials, based on a security declaration, with visual, electronic and biometrical identification.
Copyright © Port of Rotterdam

IMO has also undertaken several technical co-operation activities in the field of maritime security and missions to developing countries to improve the level of implementation of the security measures, particularly in ports.

In September 2010, the IMO Facilitation Committee will also start a comprehensive revision of the Convention on Facilitation of International Maritime Traffic, 1965, as amended. The purpose of the revision is to modernize the Convention, so as to adequately respond to the current and emerging needs of international trade, including the use of state of the art technology in the clearance of ships and cargoes. In addition, the intention is to start building closer links between measures to enhance maritime security and the facilitation of maritime traffic.

As an integral part of maritime security and recognizing the importance of an early implementation of Long-range identification and tracking of ships (LRIT), the 2002 SOLAS Conference, also invited IMO to develop and adopt appropriate performance standards and guidelines for such global systems. The maritime LRIT system is now at an advanced stage of development, with ships on international voyages reporting their position automatically to data centres every six hours while on voyage. Flag States, Coastal States, Port States and SAR authorities have access to these reports under various conditions, defined under the regulations.

In relation to piracy, IMO has been addressing piracy and armed robbery against ships for some considerable time, developing guidance for dealing with the threat as long ago as the 1980s and in 1998 embarked on a long-term anti-piracy project. Since then, IMO's principal, although by no means exclusive, strategy has been to foster the development of regional agreements on the implementation of counter-piracy measures. IMO has worked closely with the United Nations Security Council and other relevant organizations in matters relating to counter-piracy. IMO's approach is to promote regional capacity building and the development of strong infrastructures that would enable countries in the region to join forces to repress piracy and armed robbery against ships in seas adjacent to their coast. IMO has played, and will continue to play, a pivotal role in all efforts to promote an appropriate, coordinated international response to the situation.

The Strategic Plan for the Organization, adopted by the IMO Assembly in December 2009 for the six year period 2010 to 2015 (resolution A.1011(26) states in relation to maritime security: “The challenge for IMO is to promote the effective implementation of the security measures, and to instill a security consciousness in ship and port facility operations, at the same time ensuring that the right balance is struck in trade facilitation and that the flow of seaborne trade continues to be smooth and efficient.”

IMO will continue to seek to enhance the security of the maritime transport network, including vital shipping lanes, and to reduce piracy and armed robbery against ships, by promoting a comprehensive and cooperative approach, both among Member States within the Organization and between IMO and other intergovernmental and non-governmental organizations, while raising awareness of IMO security measures and promoting their effective implementation.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No. 9/04

The ILO/IMO Code of Practice on Security in Ports

*Marios Meletiou, Transport and Ports Specialist
International Labour Organization (ILO)*

Copyright © 2010 International Labour Organization

A Tripartite Meeting of experts on Security, Safety and Health in Ports was held in Geneva from 8 to 17 December 2003. The experts unanimously adopted a draft ILO/IMO code of practice on security in ports (a report on their discussion may be downloaded at the following ILO web link:

<http://www.ilo.org/public/english/dialogue/sector/techmeet/messhp03/messhp-n-a.pdf>).

At its 289th (March 2004) Session, the Governing Body took note of the report of the Tripartite Meeting of Experts and authorized the Director-General of the ILO to publish the ILO/IMO code of practice on security in ports.

The ILO/IMO code of practice on security in ports (it may be downloaded from the following ILO web link: <http://www.ilo.org/public/english/dialogue/sector/techmeet/messhp03/messhp-cp-a.pdf>) was published in print form on 15 June 2004 in English, French and Spanish and may be purchased by sending an e-mail to pubvente@ilo.org.

It has therefore been made available on time before the IMO International Ship and Port Facility Security Code (ISPS Code) would take effect upon entry into force on 1 July 2004 of the new chapter XI-2 of the International Convention for Safety of Life at Sea, 1974, as amended.

The ILO/IMO code of practice on security in ports has also been translated into Russian but it is only available in an electronic format (see attached document).

The practical recommendations in the ILO/IMO Code of Practice on Security in Ports are intended to provide relevant guidance to ILO constituents and all those responsible for or involved in the management, operation, maintenance and development of ports.

The objective of the ILO/IMO Code of Practice on Security in Ports is to enable governments, employers, workers and other stakeholders to reduce the risk to ports from the threat posed by unlawful acts. It provides a guidance framework to develop and implement a port security strategy appropriate to identified threats to security. Security had always been a factor in maritime transport and a number of mechanisms and procedures already exist to address this issue.

However, recent and serious security incidents have prompted new initiatives at international, national and company level, which would reflect the new realities. These new realities touch both the nature of the security threat and, importantly, the perception of the nature of that threat, which have changed since the September 11 events in the United States. Effectively, the focus has shifted from the relatively minor threat to trade and transport (from theft, hijackings, terrorist interventions, etc.) to the much more alarming threat from trade and transport, where the mechanisms and processes of transport could be used as weapons.

This Code falls within the framework of the new international level initiatives, which are complementary to other recent maritime security related work by the ILO and the IMO (International Maritime Organization). In the case of the ILO, it relates to the ILO [Seafarers' Identity Documents Convention, 2003 \(Revised\) No. 185](#) adopted in June 2003 by the International Labour Conference. In the case of the IMO, it is a follow up to the adoption of the 2002 amendments to the International Convention on Safety of Life at Sea (SOLAS), which includes the adoption of the International Ship and Port Facility Security Code (ISPS Code).

The Code of Practice on Security in Ports extends the consideration of port security beyond the area of port facility into the whole port. It is intended to be compatible with the provisions of the IMO's ISPS Code, which contains requirements that relate only to security of the ship and the immediate ship/port interface (i.e. the port facility). This Code of Practice addresses inter alia, port security policy, assessment and plans as well as related tasks and roles. It also addresses the issue of security awareness and training, which are vital for a successful implementation of an appropriate port security strategy. The table of contents of ILO/IMO Code of Practice on Security in Ports (2004) is presented on the next page.

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

Table of Contents of the ILO/IMO Code of Practice on Security in Ports (2004)

Heading	Page
Preface	V
Abbreviations	XVI
1. Introduction	1
2. Scope and definitions	4
3. Aim of security measures	7
4. Security policy	8
5. Roles and tasks	9
6. Security level	12
7. The port security assessment	13
8. The port security plan	14
9. Physical security of the port	16
10. Security awareness and training	18
11. Confidentiality and non-disclosure of information	19
Appendix A. The port security assessment	21
Appendix B. The port security plan	37
Appendix C. Selected references	44



Port of Istanbul, Turkey, during a joint ILO-OSCE Workshop on Port and Supply Chain Security in December 2006 (OSCE)

The provisions in the Code of Practice on Security in Ports may be represented as **activity flow-chart**, reflecting steps defined in the COP towards attainment of an acceptable level of risk in port security. Such a flow chart is presented **on the next page**.

The ILO in collaboration with the International Maritime Organization (IMO) and Col (Ret) Michael Chen (Chief Executive Officer of ST. Education & Training Pvt. Ltd. of Singapore, IMO & ILO consultant), has developed training material for a three/four-day course on the implementation of the ILO/IMO Code of Practice on Security in Ports (2004), which is complementary to the IMO International Ship and Port Facility Security (ISPS) Code. This training material was validated at an international tripartite workshop that was held in March 2004 in Singapore. In this respect, the ILO is since 2004 in a position to offer training courses / workshops to all those that would be interested in the use of the ILO/IMO Code of Practice on Security in Ports.

The curriculum of a standard course / workshop has been tailor-made for the following participants:

- Policy makers and senior executives responsible for port security issues particularly those from “Designated Authorities” or Recognized Security Organizations;
- Senior officials and Representatives from the Maritime and Port Administrations, industries, private enterprises and training institutions in the port sector.
- Maritime/Port workers’ representatives responsible for port security issues. Representatives from law enforcement agencies.

Upon completion of a standard course / workshop, the participants will be able to:

- Describe the ILO/IMO Code of Practice on Security in Ports (2004) and its link with the IMO/ISPS Code and with the ILO Seafarers’ Identity Documents Convention (Revised), 2003 (No. 185).
- Analyze the institutional and organizational arrangements necessary for the implementation of the ILO/IMO Code of Practice on Security in Ports (2004).
- Identify the roles and responsibilities of governments, employers and workers in the implementation of the ILO/IMO Code of Practice on Security in Ports.
- Undertake a port security assessment (PSA) and understand the format and content of a port security plan (PSP).
- Provide general advice to their organizations on the implementation of the ILO/IMO Code of Practice on Security in Ports (2004).

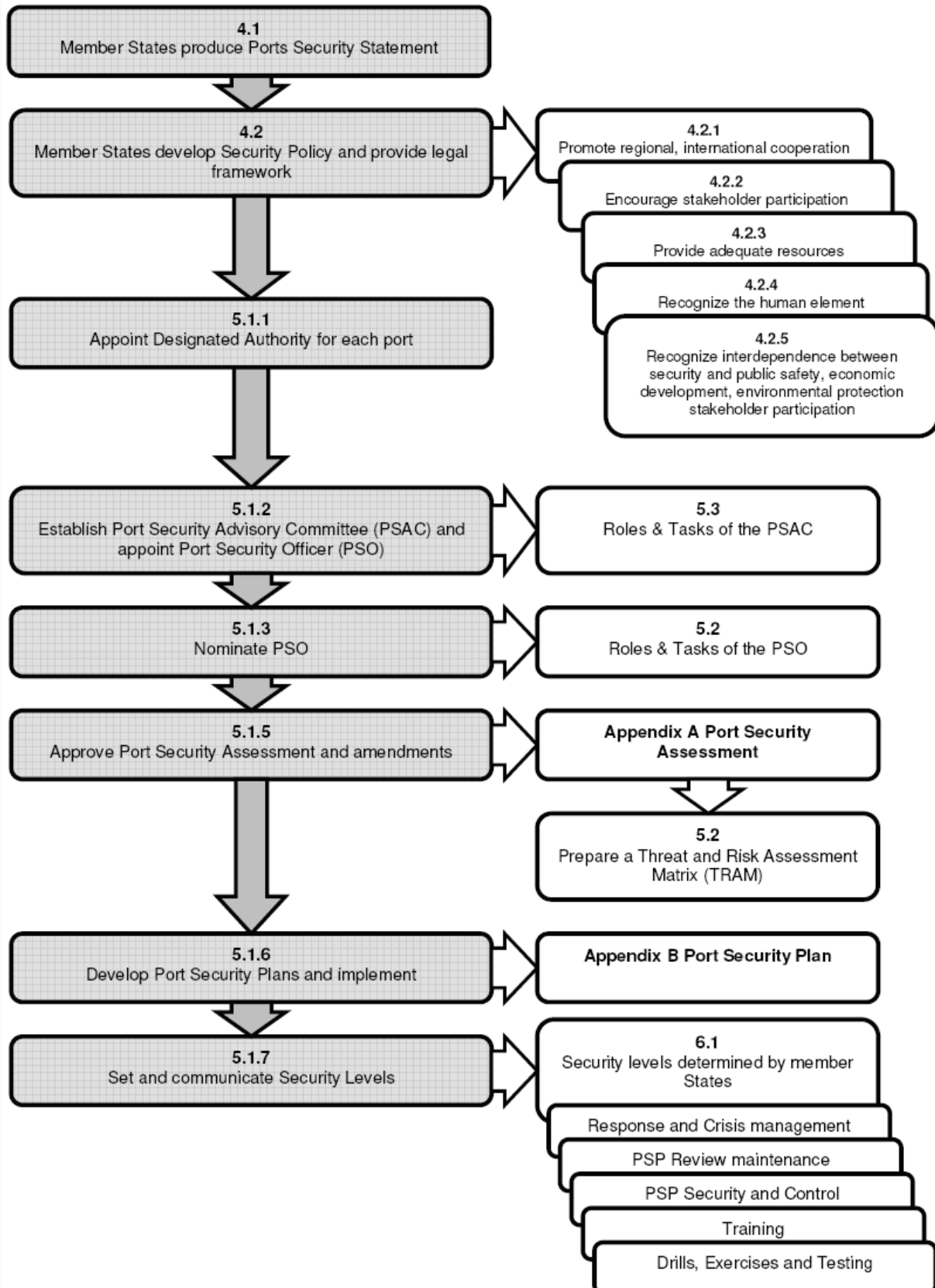
CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, *OSCE Ministerial Council Decision No.9/04*

Activity flow-chart reflecting steps defined in the ILO/IMO Code of Practice on Security in Ports towards attainment of an acceptable level of risk in port security.



CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

Security of the Supply Chain and Efficiency of Rail Transport

*Jacques Colliard, Head of Security Division
International Union of Railways (UIC)*

Improving the security of the supply chain is a permanent issue between the railways, their national authorities and the relevant international bodies.

The opening of the European market increases the number of involved companies and structures that needs to develop some coherence between them.

Some texts define the responsibilities for various members of the supply chain and confer on the parties with the contract of carriage the responsibility for deciding who has to load the goods. For the European railways it is essentially the consignor who loads the wagons in wagonload traffic. This means that the consignor is responsible for the proper loading of the wagons and the quality of the information contained in the consignment note. But as a result, the railways undertakings are unable to guarantee the accuracy of this information.

Therefore the necessity to ensure an appropriate level of security along the whole logistic chain requires the development of a common culture and practice of security for each of its members. Different ways are possible for that: mandatory rules and norms or voluntary standards, or decisions taken by the stakeholders.

But some ideas are to be taken into account before considering the drawing-up of some texts or practices:

- ◆ the new Customs Code created the status of “Authorized Economic Operator” which enables its beneficiaries to work with the customs authorities in a quicker and more efficient way;
- ◆ the possible security decisions for international freight traffic have to be in coherence with these provisions in order to avoid a multiplication of various rules for the same transport;
- ◆ the impact of the security rules or norms shall not create a further distortion of competition between means of transport nor additional difficulties between companies of the rail sector;
- ◆ the existing administrative frameworks, CIM and SMGS have to be put in coherence and even if improvements have been shown, an active political will is needed to reach efficient common solutions.

The efficiency of the railway freight transport, of a supply chain including rail transport, depends on various criteria including duration and security of transport.

Saving time supposes being able to organize technically the transport in the best way. That means developing and improving the solutions to the difference of gauge, of electric supply, of signaling and safety devices....

It supposes also that the administrative or political constraints will not represent a waste of time. For example custom agreements between various countries or custom union can constitute a very efficient way to progress.



A freight train in Turkmenistan, July 2009. Turkmenistan is an important country along the trans-Caspian railway routes. (OSCE/Roel Janssens)



CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

As a result, we have to comply with various constraints from different entities with various roles and we have to combine these constraints and organize the answers in the way which enable to save the maximum of time.

The ways are possible:

- ◆ a top down reasoning giving the first part of the job to the administrative entities in order to define a more suited international legal framework which would be the common reference to the railways for organizing their technical work according to these rules
- ◆ a bottom up reasoning giving the first part to the railways for organizing their technical constraints and adding the administrative aspects in a second time.

As both are necessary it seems very interesting to start with real examples or demonstration. An idea could be, international freight corridor by international freight corridor, to look over the existing situations highlighting their positive and negative sides and, by sharing the experience and analysis, to ask the railways on the one hand, and the international administrative bodies on the other hand, to finalize the possible systems of answer and define the consequences on the reality of the transport: cost, time of control operations....

Within its current activity UIC is permanently acting toward these aspects in order to introduce more and more coherence between its members, even if they are in competition with each other, and UIC is ready to cooperate with the relevant international bodies. In this framework, the geographical and political priorities of the OCSE represent a particularly interesting partnership opportunity.



Fixed X-Ray scanner at a railway station , Copyright © UIC

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

Proposals for a Global Approach to Supply Chain Security

*Mark Miller, Regional Vice President for European Programmes, Cotecna Inspection, and
Moureen Schobert, Project Manager, European Organisation for Security (EOS)*

International and cross-border trade is an indispensable feature of today's world, and has become critical to the well-being of societies and economies. Indeed, the citizens' lives would be severely restricted without trade which depends upon transport to drive economic competitiveness and growth. Just in Europe, the overall trade and logistics sector accounts for € 1000 billion in annual turnover, employs 10 million people and represents over 10% of the EU's gross domestic market.

All trade relies upon the so-called supply chain – the continuous linking of activities in the systematic movement of goods from the point of origin to the final destination. As international trade has grown steadily, so has the supply chain: at least 4,7 million companies in Europe are currently involved in the supply chain and the resulting value of goods transported in containers amounted to 114 billion tkm in 2005. As an increase in international trade has entailed a growth in the supply chain length, complexity and volume, the vulnerability of the supply chain has also increased. Indeed, the whole supply chain is only as strong as its weakest link, with any deficiencies in a single link affecting the entire chain, whether this is a physical attack, theft of goods or supplier identity theft from terrorists, insiders threat or organized crime. The security of the Supply Chain is thus a transversal issue, linking border control, customs, transport, ICT issues, logistics and law for the safe and reliable transport of legitimate goods.

Several countries and organizations, aware of the need to guarantee the integrity of their frontiers and to ensure the functioning of the global economy in today's world, have developed or are developing programmes that include guidelines and best practice for ensuring the security of cargo, processes and personnel engaged in the supply chain. Unfortunately, current supply chain security initiatives are insufficient if we are to deal with the complex issues that the risk of terrorism, drug smuggling and organized crime pose. The implementation of differing national security measures results in a multiplication of security and safety controls, hampering the trade flow, creating market distortions, leading to unnecessary spending and adversely affecting the companies' competitiveness and employment. Operational, technical, administrative, regulatory and procedural issues all contribute to such a situation and have been extensively investigated by EOS. A brief overview is given in the following, before remedy actions possibly to be taken at the international level will be addressed.

GAPS IN SUPPLY CHAIN SECURITY

Lack of standardization of shared information and common and/or sufficiently harmonized security requirements. No standardization of information or of security requirements for supply chain security equipment, services and testing has yet occurred. This constitutes a barrier to trade, and risks that investing in national/regional security programmes will lead to inefficiencies and unnecessary costs. Indeed, as not all security requirements are harmonized, business competition between regions is distorted as the requirements affect businesses differently, while the multiplication of security and safety controls hampers the trade flow and results in unnecessary spending. Different advance notification regimes and AEO programmes persist without sufficient alignment for all those countries that have committed to introducing such requirements. The EU's Customs Security Programme (CSP) and its advance notification rules for exports, imports and transit goods introduced on July 1, 2009 are a step forward, as they are being adopted worldwide. Yet, harmonized procedures and definitions of the type of information that companies must provide within the framework of such regimes and programmes have still not been developed.

Lack of a coordinated approach that reduces the transaction costs involved in supply chain security. Hardly any trade is limited to the flow of goods within one country. This mandates an intervention at the international level, where all relevant States should look for ways of ensuring the seamless flow of trade across their borders. A coordinated approach between national administrations in terms of risk management, incident response, data sharing, training and risk prevention is needed, while a common architecture for integration of solutions and services in a 'one stop system' should reduce the costs of supply chain security procedures. The approach should be risk-based so that resources can be focused on the high-risk shipments while

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

facilitating easy passage for legitimate trade, where security requirements do not need to be too rigid.

Lack of information sharing between countries: One of the critical factors in securing the supply chain is providing enforcement and security agencies with the right information at the right time. At the moment it is difficult to obtain a complete information set for a single consignment’s journey from its origin through all stages of the supply chain journey to its destination, as no sufficient data collection and performance measures are in place. This is due not only to technical shortcomings such as the lack of interoperability and a certain degree of data harmonization and standardization, but also to governance issues that prevent effective transnational information sharing.

Lack of a coordinated approach across all modes of transport: Existing security measures do not apply to all transport modes, which entails that certain parts of the transport chain are insufficiently secured in comparison to others. In particular, road transport, composed of several thousand companies, is very vulnerable to criminal threats and is preferably used for drug smuggling, and thus requires specific attention. The lack of an intermodal approach also distorts competition between the various modes and creates unnecessary costs, jeopardizing overall economic growth.

Unsatisfying actual implementation and enforcement of supply chain security measures: There is a perceived conflict between achieving both objectives of facilitating the free flow of trade and of securing the supply chain. An incentive scheme in which secure supply chains benefit from streamlined procedures would therefore be needed, as it would allow suppliers to gain a return on the substantial investment required for introducing improved security. In order to develop well-targeted incentives, all stakeholders should be engaged in understanding their interests and the balance of benefits vs. security investment required to promote greater security.

Technical shortcomings: A global architecture with interoperable or compatible technologies and processes does not exist today, and sensors for cargo screening in air transportation, for certain chemical and biological threats, high throughput scanning systems or coherent risk assessment and management across different countries have not been developed yet. Such developments could however substantially improve supply chain security while facilitating the legitimate trade flow.



Copyright © EOS

EOS’ RECOMMENDATIONS FOR ENHANCED SUPPLY CHAIN SECURITY

EOS recognizes that ensuring supply chain security requires addressing a number of complex challenges. On the one hand, the supply chain involves a variety of different parties, all of whom handle a large volume of goods and information, and whose accurate and timely performance is critical to the proper functioning of the supply chain. On the other hand, the supply chain comprises very different modes of transport, maritime transport (sea and inland waterways), air, rail and road transport, each exhibiting different characteristics and security needs. In addition, any approach to supply chain security needs to find a balance between the imposition of security requirements and the necessity of guaranteeing a facilitated flow of goods.

Despite these complexities, EOS’ expert group on supply chain security has identified the following recommendations that could foster adequate policy responses by all major economic powers. Given the transnational nature of most trade, EOS recognizes that deficiencies in supply chain security have to be addressed at the international level, with the OSCE having to play a crucial part in coordinating efforts:

An international Platform on Supply Chain Security for Public–Private Dialogue and Cooperation: In order to improve the international governance of security policies and programmes, a Platform for Supply Chain Security in cooperation with the private sector should be created, either initiated by the EU, or under the auspices of the OSCE. Such platform should aim at:

- ◆ Bringing together all relevant social, economic and technical stakeholders of OSCE countries, be they public or private (Public Authorities, Customs, importers, exporters, warehouse operators, transporters, terminal operators, etc.), to propose a specific and comprehensive policy targeted at all modes of transport in the

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

supply chain to serve as guideline for adoption by national governments: i.e. maritime transport (sea and inland waterways), air transport, land (rail and road transport), fostering the development and implementation of economically viable solutions without imposing too great of a burden upon companies which would risk hampering international trade;

- ◆ Raising awareness of the importance of adopting a total supply chain approach to cargo security, thus encouraging companies to assume responsibility in securing their own processes within the supply chains;
- ◆ Ensuring that supply chain security measures are enforced, and specifying measures to remedy cases of insufficient enforcement, proposed for adoption by all OSCE countries;
- ◆ Defining benefits for those operators that secure their part of the supply chain, thus supporting a return on the investment in security. This should involve incentives for trade actors to become Authorized Economic Operators (AEO) or their equivalent.

Common requirements for equipment, testing, interoperability and services: Secure trade flow should be improved by developing common requirements for equipment, testing, interoperability and services. Achieving this would depend on:

- ◆ Increased international co-operation with mutual recognition efforts in relation to advance notification and certification programmes. Using the WCO’s SAFE framework as a reference, the programmes and rules introduced worldwide, e.g. in the EU, US, Japan and China, should request the same data in compatible formats, to allow for an efficient transmission between relevant authorities and all other parties involved in the supply chain. The harmonization should not just be for the content but also for other forms, such as electronic forms and data transmission;
- ◆ The establishment of a ‘best in class’ Risk Assessment method for supply chain security that ensures that priority threats and vulnerabilities are identified and addressed. Its development could be started by the EU in consultation with other trading partners and the industry, subsequently promoting such a Risk Assessment model as a model for international adoption within the OSCE region.

The development of economies of scale and critical levels of funding: Existing supply chain programmes and funding opportunities could be consolidated by:

- ◆ Urging all OSCE countries to enhance Research, Development and Innovation activities with regard to Supply Chain Security, while improving the co-ordination between their respective research agendas. This would also improve the efficiency of existing funding programmes and costs could be significantly reduced;
- ◆ Allowing the definition and implementation of a common architecture for the integration of solutions and services in a ‘one stop system’, based on the ‘Best in Class’ Risk Assessment methodology and innovative/interoperable solutions and services, while remaining compatible, where possible, with legacy systems. The architecture should foresee the use of security measures embedded into the infrastructure (‘security by design’) and be included in the business plan of the operators (not being considered as a constraint, but as a facilitator for the efficient and competitive movement of goods).

Funding priorities should be defined in co-ordination with all stakeholders i.e. the OSCE, its Participating Countries and the private sector, in order to avoid overlaps and duplications, while taking into account both the human element of the supply chain and evolving threats. The above-mentioned Platform would be the most appropriate forum for operating such co-ordination and should also engage in the development of consolidated and harmonized approaches and Risk Assessment methods.

Finally, EOS believes in the value of having OSCE-wide co-operation. Yet, it acknowledges the difficulty in bringing all relevant stakeholders together on such a sensitive field as is security. Therefore, the EU, and possibly the US, should take the lead, with the support of the OSCE to get all relevant stakeholders together in a regular public-private dialogue. The EU and the US should continue their dialogue following the Joint Statement of Purpose in September 2008 on Co-ordination of Efforts to Enhance Air Cargo Security, but should broaden the dialogue by inviting the OSCE and other OSCE countries.

NOTE: EOS is the leading European organization for private security sector providers of technology solutions and services. Composed of major European security stakeholders, it represents more than 20% of the global security market. Over the past years it has worked on identifying needs and elaborating recommendations for all major security domains (border control, supply chain security, civil and citizens’ protection, cyber security, ICT networks resilience, critical infrastructure protection). www.eos-eu.com

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

Supply Chain Security Management Update ISO 28000 Series

*CAPT Charles H. Piersall, Chairman, Technical Committee on Ships and Marine Technology (TC8)
International Standardization Organization (ISO)*



Coast Guards patrolling the harbour area of the port of Batumi, Georgia, May 2010 (OSCE/Mehdi Knani)

INTRODUCTION

This article will provide some background, examples of implementation and the current status of the ISO 28000 family of standards.

There are many new “buzzwords” being introduced into the topic of “security and security management and the safety and security of the supply chain” and some are coming from sources with no practical experience or understanding of what is needed by participating decision makers in the supply chain. First, let’s clarify the “supply chain”. It is not a simple, single linking of elements in a chain. It is a complex network of many links and nodes which is tailored to meet the needs of the particular organization, industry and government regulatory requirements. Along with many of these “buzzwords” are often attempts to create additional

layering of management systems standards, redefining the security regime and imposing additional certification requirements. This approach not only adds confusion, but additional unwarranted costs to the industry.

ISO 28000 serves as the “umbrella” management system standard which reduces financial burden while enhancing overall security performance by successfully planning for and successfully recovering from any disruptive event. It establishes a management system framework that can be used to cover all aspects of security- assessing risk, emergency preparedness, business continuity, sustainability, recovery, resilience and/or disaster management - relating to terrorism, piracy, cargo theft, fraud, and many other security disruptions. Organizations may tailor an approach compatible with their existing operating systems. Those who have adopted a process approach to management systems may be able to use their existing system as a foundation for a security management system as prescribed in ISO 28000.

ISO 28000 is the only published and certifiable International Standard that takes a holistic, **risk-based approach to managing risks associated with any disruptive incident in the supply chain -before, during and after the event. It suggests how to improve resilience and preparedness performance in a cost effective way based on a plan-do-check-act (PDCA) management system modeled after the proven framework and risk-based approach outlined in ISO 14001. PDCA can be described as follows.**

- ◆ Plan: establish the objectives and processes necessary to deliver results in accordance with the risk assessment
- ◆ Do: implement the processes.
- ◆ Check: monitor and measure processes against security policy, objectives, targets, legal and other requirements, and report results.
- ◆ Act: take actions to continually improve performance of the security management system.

ISO 28000 (Section 4.3.1) states, in part, **“risk assessment shall consider the likelihood of an event and all of its consequences which shall include: physical failure threats and risks, such as functional failure, incidental damage, malicious damage or terrorist or criminal action; operational threats and risks, including the control of the security, human factors and other activities which affect the organizations performance, condition or safety; natural environmental events (storm, floods, etc.), which may render security measures and equipment ineffective; factors outside of the organization’s control, such as failures in externally supplied equipment and services; and stakeholder threats and risks such as failure to meet regulatory requirements or damage to reputation or brand;....”**

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

ISO 28000 security plan strategy is to better prepare for disruptions and proactively manage risks through cost effective measures.

ISO 28000 (Section 4.4.7) on **Emergency preparedness, response and security recovery** states “The organization shall establish, implement and maintain appropriate plans and procedures to identify the potential for, and responses to, security incidents and emergency situations, and for preventing and mitigating the likely consequences that can be associated with them.

BACKGROUND

The following are quotes from ISO Press Release on publication of ISO 28000:

“ISO: Geneva - **Reducing Piracy, Fraud, and Terrorism** - The ISO 28000 series of standards on supply-chain security-management systems will help to reduce risks to people and cargo. The standards address potential security issues at all stages of the supply process, thus **targeting threats such as piracy, fraud, and terrorism.**

ISO Secretary-General stated: **“Threats in the international market-place know no borders,” The ISO 28000 series provides a global solution to this global problem. With an internationally recognized security-management system, stakeholders in the supply chain can ensure the safety of cargo and people, while facilitating international trade, thus contributing to the welfare of society as a whole.”**

The ISO 28000 series of international standards can be applied by organizations of all sizes involved in manufacturing, service, storage, or transportation by air, rail, road, and sea at any stage of the production or supply process.

The ISO 28000 series will facilitate trade and the transport of goods across borders. It will increase the ability of organizations in the supply chain to effectively implement mechanisms that address security vulnerabilities at strategic and operational levels, as well as to establish preventive action plans. Organizations can then continually assess their security measures to protect their business interests, and ensure compliance with international regulatory requirements. By encouraging the implementation of these standards by the various actors in the supply chains, countries will be able to maximize the use of government’s resources, while maintaining a level of optimal security.

The ISO 28000 series assists in implementing governmental and international customs-agency security initiatives, including the World Customs Organization’s Framework of Standards to Secure and Facilitate Global Trade, the EU Authorized Economic Operators Programme, the U.S. Customs Trade Partnership against Terrorism, and the International Maritime Organization’s (IMO) International Ship and Port Facility Security Code.” *End of quote*

The ISO 28000 series specifies the requirements for a security management system to ensure security in the supply chain network... **The standards address potential security issues at all stages of the supply process from point of manufacture, including sources of financing, to the final consumer thus targeting threats such as terrorism, fraud and piracy.** It involves many entities such as producers of the goods, logistics management firms, consolidators, truckers, railroads, air carriers, marine terminal operators, ocean carriers, passenger ships, ferries and inland transport, cargo/mode/customs agents, financial and information services, and buyers of the goods being shipped for all links in the supply chain.



*Container ship docked at the port of Poti, Georgia, May 2010
(OSCE/Mehdi Knani)*

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No.9/04

The security problem is one that is shared by government and industry, and meaningful solutions must reflect that global partnership. It is a problem shared by companies, large and small, involved in the secure transport of goods and movement of people.

IMPLEMENTATION

The ISO 28000 series is being implemented and certified in a variety of industries worldwide. Some examples of widely diverse industries are:

- ◆ **DP World** was first to certify a marine terminal and will complete ISO 28000 certifications throughout its network of 48 terminals in 31 countries worldwide by 2012. DP World is the only global marine terminal operator to have achieved simultaneous ISO 28000 certification and C-TPAT membership. Its European terminals were certified as Approved Economic Operator (AEO) by the European Union.
- ◆ **Port of Houston Authority**, one of the world's largest ports, was the first port authority in the world to attain ISO 28000 certification.
- ◆ **YCH Group**, Singapore, is the first supply chain management (SCM) company to be ISO 28000 certified. YCH Group is the leading integrated end-to-end supply chain management and logistics partner to some of the world's largest companies including Canon, Dell, Moët-Hennessy, ExxonMobil, B. Braun, LVMH, Royal Friesland Campina and Motorola.
- ◆ **TNT Express' Asia regional head office in Singapore** is the first express integrator to achieve certification to ISO 28000.
- ◆ **YCH India** is also certified TAPA 'A-class' and ISO 28000-compliant for its security systems. YCH India provides customized Supply Chain solutions for Electronics, Consumer Goods, Chemicals/Healthcare and Automotive industries in India. Its clientele includes DELL, ACER, TPV, General Mills, HCL and others.
- ◆ **DB Schenker**, the world's second-largest forwarder, obtained ISO 28000 certification for its regional head office for the Asia-Pacific sector in Singapore last year, along with its local office and operations at Singapore Changi airport. Klaus Eberlin, chief operating officer for the Asia-Pacific, views the ISO standard as a "kind of umbrella standard that encompasses elements like the TAPA programs. ISO 28000 extends beyond physical aspects of security to elements like information flow and financial data".

Other ISO 28000-certified companies include: **Asian Terminals** (first marine terminal in Philippines), **CTS Logistics-China** (kitting assembly of turnkey management of consumer electronic, IT and telecommunication products), **Banner Plasticard** - Philippines (design and printing of cards, personalization, embossing, encoding, thermal printing, wrapping crating and palletizing). There are also airport, railroad, pharmaceutical, health care, and high tech industries certifying to ISO 28000, and many other global industries.

Professional training for security and non practitioners using ISO 28000 is being conducted for (1) supply chain business operators and (2) Customs Officers.



(OSCE/Mehdi Knani)

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

ISO 28000 SERIES STATUS

- ◆ **ISO 28000:** Supply chain security management systems – **Published:** the overall “umbrella”, certifiable, management systems standard.
- ◆ **ISO 28001:** Best practices for implementing supply chain security, assessments and plans – **Published:** designed to assist industry meet requirements for Authorized Economic Operator (AEO).
- ◆ **ISO 28002, Resilience in the Supply Chain – Requirements with guidance for use – PAS in publication:** This standard is to provide additional focus on resilience. It supports the strong demand as firms are looking for assurance that their suppliers and the extended supply chain have planned for steps to prevent and mitigate the threats and hazards to which they are exposed. As part of the ISO 28000 management system, the ISO 28002 standard emphasizes the need for an on-going, interactive process to prevent, respond to and assure continuation of an organization’s core operations after a major disruptive event.
- ◆ **ISO 28003, Auditing & Certification – Published:** guidance for accreditation & certification bodies.
- ◆ **ISO 28004, Guide for implementing ISO 28000 – Published:** assist users in implementation.
- ◆ **ISO 28004, Addenda:** Additional guidance for adopting & certifying ISO 28000:
 - Amd1** – for use in medium & small seaport operations – **Draft for voting**
 - Amd2** – adopting ISO 28000 for small-medium sized businesses (SME) This specific guidance supplement will help medium and small businesses develop processes that comply with the general guidance contained in existing ISO 28004.
 - Amd3** – for security requirements for Authorized Economic Operator – to provide specific guidance to organizations seeking to incorporate requirements contained in ISO 28001 for Authorized Economic Operators into their implementation of ISO 28000. The security best practices contained in ISO 28001 were carefully developed in liaison with WCO – **PAS approved to publish.**
- ◆ **ISO 28005, Computer applications – Electronic port clearance (EPC) is the latest addition to the series. It provides for computer-to-computer data transmission. The details of this standard development have been briefed to IMO and WCO. To expedite the development, ISO 28005 has been broken into two parts:**
 - ISO 28005-1: Single window implementation – **Approved Work Item.** Republic of Korea (KATS) as new Project Leader
 - ISO 28005-2: Core data elements – **PAS Published; DIS approved 2010-05-14.** Norway (MARINTEK e-Maritime) as Project Leader

- ◆ **ISO 28006, Security management of RO-RO passenger ferries – Under development:** best practices for application of security measures
- ◆ **ISO 20858, Uniform implementation of ISPS Code – Published**

NOTE

CAPT. Charles H. Piersall has been Chairman of ISO/TC8 since 1995. His committee is a recipient of the Lawrence D. Eicher Leadership Award. A retired United States Navy Captain, he has over 54 years of distinguished maritime service – first as a senior naval officer and then as a senior industry executive. In addition to the highest military awards, he is also recipient of numerous high level awards based on his contributions to international standardization.



*Malta's transshipment port, Freeport, December 2009
(OSCE/Mehdi Knani)*

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

IRU Driving for Secure and Facilitated Road Transport

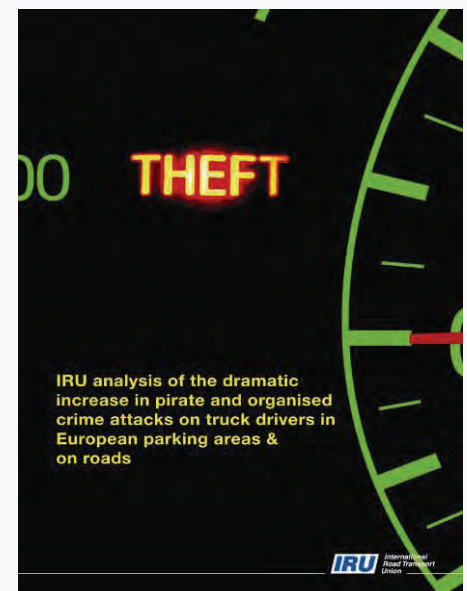
*Umberto de Pretto, Deputy Secretary General
International Road Transport Union (IRU)*

In today's globalised economy, where it takes 29 companies from 18 countries to have a simple cup of coffee, the demand for the sustainable mobility of goods is constantly increasing. The road transport industry is the backbone of strong economies and dynamic societies. Due to its unique, door-to-door goods transport services, road transport is the most flexible and reliable production and distribution tool to irrigate the global economy, interconnecting all businesses to all major world markets while driving economic growth and ensuring social progress through a better distribution of wealth, regardless of the geographical location. No country or region is landlocked to road transport.

However, terrorist atrocities around the world have drawn increasing attention to the fragility of systems involved in the international movement of goods, making security issues a top priority for all actors involved in international trade. Legitimate trade has also been used by criminals as a cover for other illicit activities, including illegal migration, drug trafficking, money laundering, Customs and transit fraud, movement of counterfeit goods and other offences threatening the well-being of national societies and the international community.

While sustaining the world's economic growth requires secure trade and road transport, it must be considered that facilitation cannot be ignored, even when security considerations are high on the agenda.

The International Road Transport Union (IRU) has thus always advocated striking a sound balance between facilitating formalities and procedures at borders and other “meeting points” between state administrations and private business, and providing a high level of security for the entire supply chain. The TIR System offers both facilitation and security.



THE TIR SYSTEM – A SECURE FACILITATION INSTRUMENT FOR INTERNATIONAL TRADE AND TRANSPORT

The TIR System, based on the TIR Convention, was created by the United Nations immediately after the Second World War to expedite the recovery of European industries and economies through facilitated trade and transport.

The basic principles of the TIR Convention consist in allowing goods, placed under TIR procedures by authorized transport operators, to be moved from a departure point to a final destination point under customs seals (secure truck or container) and an internationally agreed transit customs document, the TIR Carnet.

Goods moved under TIR procedures benefit from a suspension regarding the payment of taxes and duties throughout the countries transited, until the final destination has been reached and where the import declaration takes place. The TIR Carnet is a standard internationally agreed customs declaration which, represents for customs authorities the financial guarantee to cover the suspended taxes and duties in the event the goods are removed from customs control before they reach their final destination.

Since 1975, when the TIR Convention was amended to cover multimodal transport operations, the TIR System applies to any shipment as long as at least one leg of the transport is carried out by road. Therefore, multimodal transport including maritime, inland waterways and rail operations can benefit from the TIR System.

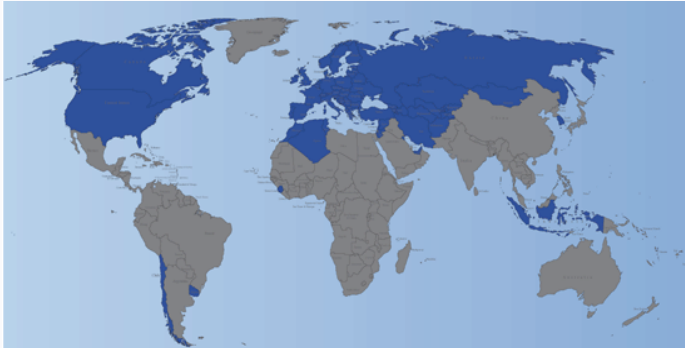
Over the past 60 years, the geographical scope of the TIR Convention has constantly expanded, from the 6 initial founding countries to the current 57 Contracting Parties where the TIR System is implemented. More than 40'000 authorized transport operators meeting the minimum conditions and requirements set out in the TIR Convention are using TIR procedures to carry out some 3 million transport operations every year.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04



Contracting Parties to the TIR Convention. Source: IRU

The use of modern information technologies has allowed the IRU and its Members to computerize the management of the TIR System through its international control system, SafeTIR, thereby ensuring a permanent and real time monitoring of TIR transport, from the issuance of TIR Carnets to authorized operators up until the termination of the related transport operations at final destination. In partnership with the 57 national Customs administrations, the IRU has implemented an appropriate IT communication network allowing a permanent update of TIR Carnet data.

TIR SYSTEM – BEST INSTRUMENT TO EFFECTIVELY IMPLEMENT THE WCO’s SAFE FRAMEWORK OF STANDARDS

To address and enhance the security of the international supply chain of goods, the World Customs Organization (WCO) published in 2005 the WCO SAFE Framework of Standards which was upgraded in 2007 to incorporate the technical guidance for the implementation of Authorized Economic Operators (AEO) requirements to obtain the AEO status. The SAFE is not an international regulatory instrument but a compilation of security standards that need to be applied on a country by country basis. As such, the WCO SAFE does not contain any binding provisions nor does it provide for any legal basis for mutual recognition.

The absence of a mutual recognition mechanism within the WCO SAFE gives no other alternative to States than to negotiate on a bilateral basis mutual recognition agreements to ensure that security requirements and the AEO status are granted on a bilaterally recognized manner.

The issue of recognition of the level of the security requirements cannot be efficiently resolved through a multitude of bilateral agreements but needs an internationally agreed mechanism that would provide the necessary level of harmonization to guarantee mutual recognition.

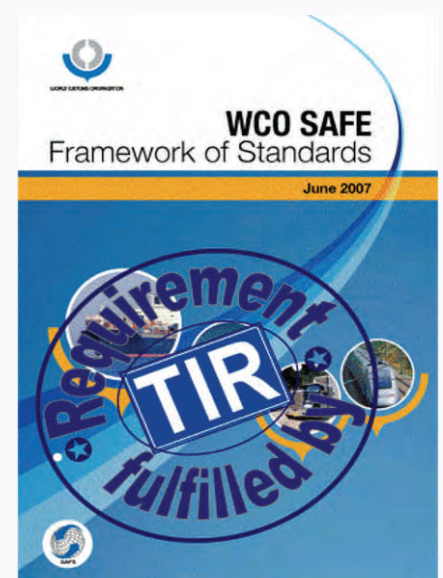
All IRU analyses, including the results of the Road Freight Transport Security Seminar held in Geneva on 17 September 2007, concluded very clearly that the TIR Convention is the best tool to fully implement, for the transport it covers, all the security requirement standards set by the WCO SAFE Framework, including those for the implementation of the AEO status.

A study commissioned by the US Chamber of Commerce and published in May 2008 also came to the same conclusion that the TIR Convention, due to the fact that it is the only convention providing mutual recognition of all customs controls between its 57 Contracting Parties, is the best multilateral legal instrument to implement all the security requirements of the WCO SAFE Framework, including those concerning the AEO status.

The use of the TIR Convention to implement the WCO SAFE Framework of Standards would allow for the transport carried out under the TIR procedure by authorized TIR Carnet holders to benefit from the global mutual recognition provided by the TIR Convention without relying on a multitude of bilateral agreements that could vary from one to the other which would lead to either a non harmonized implementation of the WCO SAFE or possible discrimination due to the variety of national security requirements.

To achieve the balance between facilitation of international trade and transport and security, it is increasingly recognized that the TIR Convention would only need a few technical adjustments in some of its annexes to fully reflect the WCO SAFE requirements.

Such an upgrade of the TIR Convention would not only confirm that it is a truly global instrument but would guarantee for the transport it covers a harmonized implementation in 57 countries of the security requirements set out by the WCO SAFE Framework of Standards.



“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

TRANSPARK ADDRESSING ORGANIZED CRIME’S ATTACKS ON ROADS

While security issues have been high on the political agenda due to terrorist activities, serious attacks on drivers and theft have not received sufficient political attention. These challenges – and their responses – pose serious daily problems for all actors involved, be they drivers, transport companies, authorities, trade associations, unions, insurers, truck stop operators, etc.

The number of vehicle thefts and freight robbery incidents appear to be increasing in many countries. The need to protect drivers, their vehicles and the freight carried is now becoming an issue of increasing concern, whose total direct cost is estimated at more than € 7 billion in Europe (not including indirect expenses or the value of lost business opportunities).

However, the information needed to better understand the nature and scale of the problem and its consequences on transport drivers, companies and the sector as a whole was lacking and only anecdotal evidence of attacks on drivers was available. To address these concerns and lack of accurate information, the International Transport Forum (ITF) and the IRU conducted a joint survey on attacks on international HGV drivers in Europe in order to better ascertain the nature and scale of these attacks.

The survey, which included some 1,300 face to face interviews and 700 replies to an Internet questionnaire from drivers and transport companies in more than 35 European, Balkan and Central-Asian countries over the period 2000-2005, showed that:

- ◆ 1 in 6 of all drivers interviewed (17%) have suffered an attack during the 5-year period investigated, 30% of them reporting more than one attack.
- ◆ 60 % of the attacks targeted the vehicle and its load, whilst the remaining 40% related to the theft of the driver’s personal belongings, with 21% of them being physically assaulted.
- ◆ 42% of the attacks took place in truck parking areas, 66% of which occurred between 10:00 pm and 6:00 am.

On the basis of these survey results, which highlighted the urgent need for immediate action by Governments and all other stakeholders, the IRU and the ITF have developed and launched [TRANSPark](#), a web-based platform which significantly facilitates the search for safe, secure and convenient parking areas in over 40 countries spanning from Portugal to Kazakhstan, while providing a full range of other useful services to all actors involved in goods transport by road, such as route planner, fuel prices, border waiting times, flash information on traffic restrictions, road works and blockades, legal advice and support, etc. Accessible free of charge on the IRU and ITF websites, TRANSPark is also available in PDA format for easy use from the truck cabin.

TRANSPark users can search for truck parking areas by country, around a location within a 100--km radius, or along their planned routes. All facilities available at the selected parking area are listed (security features, truck repair, vehicle wash, hotel, restaurant, etc.), and can be used as parking search criteria.

However, despite the industry’s repeated demands to national authorities to establish and maintain safe and secure truck stops and parking areas, little has been done so far by governments to tackle this dramatic situation. It is therefore high time that national authorities face their responsibilities and take all the necessary measures, including the construction of additional secure parking areas necessary to ensure the security of drivers, loads and trucks, in order to meet their constitutional obligation of ensuring the security of people and goods on their territory.

Moreover, rigid social regulations, such as the introduction of the digital tachograph, oblige drivers to stop in insecure areas in order to comply with the driving and rest times legislation.

Competent authorities should thus acknowledge the urgency of this dramatic and unacceptable human suffering and economic losses, and communicate to the IRU the location of secure parking areas on their territories for integration in the TRANSPark database.

WORKING TOGETHER FOR A BETTER FUTURE

To achieve our common objectives of facilitating and securing trade and transport, the IRU remains prepared to work in genuine public-private partnership with the OSCE and its member countries to ensure that road transport can continue to drive progress, prosperity and ultimately peace throughout the OSCE region.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

The CLECAT Supply Chain Security Compliance Handbook

EU freight forwarder’s perspective of the global Supply Chain Security

*Marco Sorgetti, Director-General, and Niels Beuck, Policy Adviser
European Association for Forwarding, Transport, Logistic and Customs Services (CLECAT)*

IF IT’S LEGAL, FLY IT

The new 300/2008 Regulation and its implementing provisions (185/2010) will soon be in force all over the European Union. These rules replace the famous 2320/2002, which was hurriedly put in place after 9/11 terrorist attacks in order to enhance aviation security. This ends an extensive period of consultations, where all parties concerned have tried to find acceptable solutions for their obligations and concerns: security for the citizen on the one hand and unobstructed trade flow on the other. The result of this work is supposed to be a comprehensive, harmonized ruling that makes EU airfreight supply chain (SC) secure as well as business-friendly.

Despite institutions’ laudable efforts to the contrary, airfreight security measures constitute a burden for the airfreight industry: only “regulated” agents and “known” consignors can take to the skies without prior cargo scanning. To become authorized some complex conditions have to be met. In addition part of the legislation forms a Commission’s Decision for Members States only; as such it is not public and one cannot avoid feeling uneasy with the idea that there is something “secret” and unknown about what one is supposed to do.

The old regulation was not exempt from criticism and the purported harmonization and transparency of the new regime is yet to be proven. The commitment of Logistics Service Providers (LSP’s) to achieve a decent balance between protection and facilitation has been unflinching in these complex years. We believe authorities ought to recognize it and take stock from all the efforts deployed, by maintaining a vital line of communication with all stakeholders, first and foremost those who are more directly affected. Let me open a small parenthesis: LSP’s and freight forwarders handle some 90% of the world flown cargo, this helps understand that anything affecting aviation security affects them directly.

CARING FOR SECURE TRADE LANES

Freight forwarders have traditionally helped international trade to flourish. When our business patterns evolved, the global economy made LSP’s an integral part of production lines, indeed one could say that there is no modern value chain without logistics. By ensuring that raw materials, semi-finished and consumer goods move from point of origin to destination at the right place, at the right time and in good shape, LSP’s ensure that trading actually happens. This helps us understand why security, after Sep 11th, has penetrated logistics in such a prominent way. Our lifestyle, our competitiveness and the actual functioning of our society depend on quality logistics, i.e. not only is logistics a potential threat, if transport means are misused, but it is also a value in itself that ought to be protected. This is all very clear when discussing security, it is not so obvious in other areas of policy, where, in our opinion, our voice is insufficiently heard, e.g. ensuring logistics can count on decent and sufficient infrastructures.

Freight forwarders, at their very best, use all modes of transport which guarantees flexibility, sustainability and efficiency. Nonetheless the use of all modes of transport complicates matters greatly from a security point of view, because not only is it necessary to be familiar with the applicable national security regime, but forwarders must also be aware of different regimes in different transport modes, in different countries and often in different continents.

It is therefore no surprise that security has become a real driving force behind the policy debate in the transport sector. Together with environment and emissions, security is the hot topic. SC security has hence become a central concern in our daily business. CLECAT has always acknowledged the importance and necessity of well functioning security programmes, with the view that the protection of citizens should remain their main objective, however mindful of the value of logistics as such. Theft prevention, smaller insurance premiums, Customs facilitation and, more than anything else, security-related values enhance the public image of the companies; all these are worthy rewards, but we maintain that the tail should not wag the dog: security measures should be primarily driven by the quest for citizens’ protection.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

"OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally", OSCE Ministerial Council Decision No.9/04

BECOMING FAMILIAR WITH THE THREAT

Customs, and interactions with other governmental agencies, has recently emerged as one of the most important items in the agenda of the forwarder, as Customs became the main vehicle to enforce security related regulations. On the way to security we have grown familiar with concepts such as "risk assessment", which is all but easy to grasp. This familiarity came at the cost of burdensome requests to our sector, which is essentially a cross-border business. Authorities ask for more information, sometimes without sufficient trade-off: additional burden eventually leads to higher costs for service providers and customers, but simplification is still just a word written on the blackboard. Whilst we talk about faster Customs clearance, fewer inspections, smaller sets of data, less frequent scanning and generally better cooperation with Customs, Single Window, etc one has the impression that all this is like Achilles's turtle. No matter how fast Achilles is, the turtle is always quicker...

THERE'S A LIGHT...

In order to mitigate our members' burdens, CLECAT undertook the task to compile a hopefully complete guide to the different security regimes applicable worldwide. The aim of our paper has been to provide companies with a practical guide, to show them which security initiatives they have to be aware of, which of them are mandatory, if they want to legally conduct their business, and where they can get further information on how to comply with security rules. There is also an ample section on non-mandatory, wide-spread rules.

Security is an area where losing orientation is easy, and easier still to set off on time consuming (and often very costly) endeavours that come to no avail in the end. By the time the first edition was finished we questioned whether this should be an in-house or a public exercise. After some debate, we concluded that it was in everyone's interest to enhance the level of awareness in security and we decided to publish our guide on our website for free consultation ([link](#)). All parties are welcome to consult it and more than welcome



Clive Broadley, President of CLECAT, presenting CLECAT's Supply Chain Security Compliance Handbook, at the 9th Freight Forwarders' Conference, 3 December 2009 in Brussels

to contribute with their remarks and suggestions. The guidebook was published on the occasion of the 9th Freight Forwarders' Conference at the end of 2009. It has been structured by highlighting first and foremost EU mandatory requirements, considering CLECAT is committed to EU affairs, it then shows EU voluntary initiatives and programmes and lastly the main international mandatory and voluntary security initiatives. When available, appropriate web-links are provided for those who wish to delve deeper. When reading the booklet, one cannot fail to see that governments have adopted regulations aiming at improving cargo and SC security with two different (and sometimes opposing) principles: scanning of all cargo at relevant points (e.g. US 100% scanning) or a system-based approach aimed at reducing the number of sensitive cases (e.g. C-TPAT and AEO programmes, focussing on advance cargo information). Both aim at enhancing the visibility and the security of the SC, but both of them increase its costs as well. Costs and benefits must find a balance in a properly managed SC, but listening to the divergent views of different stakeholders can often leave one puzzled. The US plan to enforce 100% scanning of inbound maritime containers is an extreme example: expensive measures to achieve an allegedly false sense of security. However, according to latest information received, the DHS is trying to convince the US legislative organs that 100% security through scanning cannot be achieved, because it would create major disruptions in global trade and exorbitant costs for US consumers, leaving their trading partners even worse-off.

A QUESTION OF BALANCE

This however shows the thin line between what I would call authoritative and cooperative approaches. Both have been used and have their place under certain conditions. However the best result can be achieved

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

with a combination of these, e.g. the basic requirements needed to achieve an adequate level of security for citizens, with an added trusted trader programme. More stringent security measures are then possible for those who anticipate benefits for private partners (faster Customs clearance, lower fees, less information transmission, etc.); private companies can become partners of the authorities, if they choose to do so.

Risk management is so far the only acceptable way to address the security challenges that states, industry and citizens face, each dealing with its part of risk and measures to mitigate. This concept advantageously starts by providing incentives for the high investments that are necessary to comply with these regulations. If they have the right size, companies want to become “secure operators” because they expect to streamline their logistics chains through security measures; they do not mind investing, if they can use the enhanced visibility of their operations to promote their image vis-à-vis their customers.

LIVING IN A MUTUALLY RECOGNIZED WORLD

There is another aspect of our work that we hope shall not be completely forgotten, even though it is a by-product of our efforts. Achieving the best possible security level or, better, achieving the best compromise between security and facilitation is not easy and it is more difficult if it is pursued in an un-coordinated way. From an industry point of view harmonized rules are essential, if possible, with a global scope. The European Union has fortunately seen this necessity and has undertaken great efforts to bring harmonized rules (at least at EU MS’s level) into trade security, foremost with the AEO rules and the new air transport security regime (Regulation 300/2008). The air security regime, in particular, has not only a security aspect, but it also enshrines a harmonizing and optimizing component. Besides leading to a harmonized system of rules in all EU Member States, there is hope that this will create an international security partnership, implemented by a certain number of bilateral mutual recognition agreements, thus contributing to streamlining international trade protocols.

In this light, the European regime is only the first step, the next, the mutual recognition of security rules between the EU AEO programme and the US C-TPAT, is under discussion; albeit on shaky ground, as this was expected to come to fruition at the end of last year, but it seems to be progressing slowly. The EU Council adopted a position in favour of mutual recognition with Japan, other programmes are on the move, e.g. China, Australia and New Zealand. The work done in the past years by the WCO has created the conditions for this progress.

Reciprocity, which is still missing, is the key element to provide tangible incentives: the mere fact of not being subject to security vetting twice is a priceless advantage in trade.

SECURITY IS A PUBLIC GOOD

On another tone, cargo SC’s have been somehow safeguarded from terrorism so far, thus enabling authorities to conclude that the logistics industry could be treated as a partner in the fight against terrorism, instead of a threat. However the requirements that are imposed on our industry must be effective and proportionate and should not appear as an attempt to unload a primary state responsibility on to the private sector.

The issue became conspicuous when the financing of aviation security was discussed institutionally. It is our firm belief that the states’ duties towards their citizens comprise of offering all possible protection against terrorism. In view of the secondary benefit of protecting industrial assets, it is conceivable that some costs are shared by the industry, but in no way the entire, or even the larger part of the burden of making our society more secure. CLECAT has therefore strongly supported the European Parliament in its stance in regards to a Commission proposal in this area that at least the costs of more stringent measures should be borne by the Member States.

As explained above we have produced an inventory of security measures companies must or may face in their business. This includes a whole different chapter of investigation looking at the taxonomy of crimes and manmade disruptions in the supply chain. Analyzing different threats, addressing them through appropriate measures, introducing these concept in business culture and investments strategies are challenges that have not been faced by others before. There are indications from business that this is an interesting, but frighteningly complex task, requiring skills and knowledge that could not be found in CLECAT alone. A group of relevant stakeholders gathered under the auspices of an FP7 project called LOGSEC. This was recently kicked-off and more information will be available on our website, or - very gladly - at the next opportunity to meet.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No. 9/04

Supply Chain Security: A Shipowners' Perspective

*Timothy Watson, Policy Officer
International Chamber of Shipping (ICS)*

Primarily as a result of the events of September 11 2001, in recent years there has been a far greater emphasis on security amongst international bodies concerned with security issues across all segments of the supply chain. This shift in focus led to a flurry of activity and the emergence of a number of new initiatives and security requirements in order to try to mitigate the threat of a weapon of mass destruction being delivered through the international supply chain. Maritime security in particular has been comprehensively covered by international instruments such as the International Maritime Organization (IMO) International Ship and Port Facility Security (ISPS) Code and the World Customs Organization (WCO) SAFE Framework of standards.

The ISPS Code, which entered into force in July 2004, provides a comprehensive set of measures to enhance the security of ships and port facilities. It prescribes responsibilities to governments, shipping companies and port operators to detect and prevent security threats in the maritime sector and provides a framework for such monitoring and risk assessment. Ship operators have already successfully implemented the stringent requirements of the Code which, as part of the Safety of Life at Sea (SOLAS) Convention, is mandatory for the 148 contracting parties.



Port of Batumi, Georgia, May 2010 (OSCE/Mehdi Knani)

In addition to the work of the International Maritime Organization, the unique competencies of the World Customs Organization were also recognized early on, and a series of measures with regard to intermodal supply chain security were developed by the WCO – not least of which the SAFE Framework of standards to secure and facilitate trade. ICS was closely involved with the development of the SAFE Framework, and remains closely involved in its maintenance through the SAFE Working Group, which oversees amendments to the Framework, and the WCO Private Sector Consultative Group, which is becoming the principal industry sounding board for a variety of other WCO initiatives.

Despite the often considerable investment required, the vast majority of ship operators have already successfully implemented these new requirements. However, responding to demands from politicians to maintain the integrity of cargo as it moves through the wider supply chain has proved an even greater challenge.

Notwithstanding these international measures at the international level, the shipping industry continues to engage with Customs authorities worldwide, as they develop ever more complicated supply chain security regulations. This mosaic of complex initiatives, codes and regulations have presented both problems and opportunities for the maritime industry.

Over the past five years, the liner shipping industry in particular has successfully adapted to the requirements for details of cargo to be reported to Customs authorities, in the nation of delivery, prior to lading aboard the vessel at the port of export. The requirements, initially introduced by the United States, for the filing of advance cargo information allowing for the screening of cargo through risk management techniques, are now also being implemented along similar lines in other countries, such as Europe and China. The shipping industry has largely been willing to comply with these requirements, which often apply to bulk and break bulk freight as well as containerized cargo, despite the significant costs involved in meeting the technology requirements. The shipping industry's goal has been to ensure that, so far as possible, all of these rules are in accordance with principles adopted by the WCO as part of its SAFE framework, and follow the generally accepted trend towards a multilayered approach to supply chain security.

CTN Electronic Journal

Enhancing Container and Supply Chain Security

July 2010

“OSCE participating States will act without delay to enhance container security, based on best practices and on norms and standards agreed internationally”, OSCE Ministerial Council Decision No.9/04

However, the task of maintaining global uniformity has been frustrated as politicians keep moving the goal posts in ways that are not always compatible with WCO principles. In particular, ICS is maintaining its opposition to the implementation of the U.S. law on 100% container scanning of US bound cargo at foreign ports. This unilateral measure works at cross purposes with the risk based approach hitherto adopted by the WCO, and could undermine other existing supply chain security programmes. It would also likely result in hugely increased costs to trade and the wider economy, is not considered practical, and would be for no proven security benefit. Recent indications that implementation of the law will be delayed until at least 2014 have been welcomed by many stakeholders, and it is hoped that following further feasibility studies by US Customs and others, this draconian law may soon be reconsidered.

ICS has also been involved in helping WCO to amend its standards in line with the additional U.S. Importer Security Filing (ISF) requirements, commonly called ‘10+2’. These rules were fully implemented in January 2010, and are now being enforced. This rule has been accepted in principle by carriers (as a preferable alternative to 100% scanning) but concerns over the cost of implementation remain. Dialogue is continuing between the WCO, the DHS and industry on amendments to the SAFE Framework in order to take account of the new rule.

In addition to this, work is also continuing at the WCO to further develop Authorized Economic Operator (AEO) programmes, which are designed to afford trade facilitation benefits to those companies that prove compliance with certain security requirements. In order to increase the uptake of these schemes, however, there remains a need to give greater benefits to certified AEOs, and to deliver mutual recognition of AEO certifications between countries.



Port of Istanbul, Turkey, December 2006 (OSCE)

Further to ongoing work at the WCO and with individual countries, the shipping industry has also been engaged at a number of fora to develop vessel level security measures. In particular much work has been done to develop the Long-Range Identification and Tracking (LRIT) system and the Automatic Identification System (AIS), both developed by the IMO. When taken together these measures can be considered an integral layer in the supply chain security tracking and tracing process.

Another area of supply chain security which is of grave concern to the shipping industry is the piracy situation off the Coast of Somalia and in the Indian Ocean. Indeed, the shipping industry has felt deepening frustration at the seeming impotence of the international community to address this crisis, which since the beginning of 2008 has seen 1800 seafarers taken hostage, with their ships hijacked for ransom. This is despite the comprehensive measures that ship operators have taken to defend their crews, including compliance with the “Best Management Practices” developed by ICS and other industry associations, in cooperation with military navies, and the implementation of Ship Security Plans as required by the ISPS code.

The need to continue to enhance the security of the global supply chain remains a critical issue for shipping, an international industry at the centre of world trade. There remains, however, a clear need for the benefits of any proposed new measure to be weighed against its potential impact on the smooth flow of global trade. Ultimately a multilayered risk management process that allows for legitimate trade to flow smoothly is the best way forward, and it is essential that all parties in the supply chain cooperate and share information, in order to ensure that we strike the right balance between security requirements and trade facilitation. The shipping industry, which has worked tirelessly in the development of the SAFE Framework, implementation of the ISPS Code and engagement with foreign customs authorities, has proven that it can play its part.

NOTE

The International Chamber of Shipping (ICS) is the principal international trade association for merchant ship operators, representing the global shipping industry at the International Maritime Organization and other inter-governmental fora that impact on the industry. ICS membership comprises national shipowners’ associations from 31 nations representing all sectors and trades and about 75% of the world merchant fleet.