Council of Ministers

SECURITY IN TRANSPORT

Container Transport Security Across Modes:
Conclusions and Recommendations

This document will be examined under item 3 "Main discussion blocks: Security in Transport" of the draft Agenda for the Ljubljana Council of Ministers.

Ministers are invited to agree the Conclusions and Recommendations and take note of the information given.
CONTAINER TRANSPORT SECURITY ACROSS MODES

CONCLUSIONS AND RECOMMENDATIONS

1. Context

A new wave of heightened security measures has emerged to address the security weaknesses in the transport system that were revealed in the September 2001 terrorist attacks and further highlighted by the Spring 2004 rail and public transport bombings in Moscow and Madrid. These measures, many of which are described in the Note on Security and Terrorism in the Transport Sector: Key Issues and Actions [CEMT/CM(2004)21] are designed to ensure maximum protection from terrorist activity across transport modes and are built on an existing security framework established over many years. These efforts, however, have mostly been concentrated within individual modes. It is increasingly accepted that additional weaknesses may exist in the linkage points between modes along the transport chain.

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

The study\(^1\), the findings of which are summarised in this Note, highlights vulnerabilities in the container transport chain by examining security issues related to maritime shipping containers as they transit the transport chain. Maritime containers are the focal point as opposed to other types of containers because they are the most numerous container type in international trade, are truly inter-modal, and ubiquitous. In addition, the study specifically focuses on the potential threat for containers to be used by terrorists as a delivery vehicle for chemical, biological, radiological or nuclear (CBRN) weapons, as this scenario largely underpins national and international policy agendas at this time.

Containerised transport is a hybrid system involving different modes of carriage. While Transport authorities typically have authority over the modes, Customs and Trade authorities have responsibility for the containers. The role of Transport Ministries is important: Ministers are among those first called to the front line to respond to any crisis involving the transport system. Secondly, transport authorities can establish rules to govern container handling and play a role as “gatekeeper” to the freight transport market via their regulatory oversight and licensing of transport companies, operators, and vehicles. Thirdly, transport authorities have a role to play in improving the transparency and communication of information regarding those actors handling and transporting containerised consignments.

2. The Container Transport Chain

Container transport is characterised by complex interactions among a great multitude of actors, operating systems and regulatory frameworks. It is this complexity, along with the lack of a single controlling entity over the entire container transport chain, which has led many specialists to conclude that the system is vulnerable to terrorism. Many of the security concerns are related to the presence of many small- and medium-sized enterprises operating within the system.

Containers move along a network of nodes and links through multiple modes of transport and supporting infrastructure. The container transport chain is not uniformly secure, and the level of protection can vary greatly from node to node and among modes. The risk of a security breach at any one point can compromise the security of the entire chain. A number of security issues relating to the physical flow of containers should be borne in mind. For example:

- The specific stuffing location is paramount from a security perspective because it represents the last point in the container transport chain where the physical contents of the container can be visually identified.
- Containers are most vulnerable to being tampered with when they are at rest and least vulnerable when they are in motion.

The importance of generating, receiving and processing information is paramount since the examination of information flows can reveal discrepancies that might indicate terrorist and/or criminal involvement.

All actors in the container transport chain should work towards the medium- to long-term goal of a system where the party responsible for generating security-relevant data provides that information to Customs when it is first generated – i.e. from the moment the container is stuffed. This goal will require among other aspects some form of consignment identification protocol -- such as the World Customs Organisation Unique Consignment Reference (UCR) -- and some form of guidelines on the advanced provision of data to Customs.

3. Threat Assessment

Will terrorists target containers as a means of delivering a CBRN weapon? There is no easy answer to this, particularly because many government agencies in charge of overseeing the different parts of the container transport chain have not yet undertaken a thorough and comprehensive risk assessment of this scenario. Measures for counter-terrorist security need to be proportionate to the threat, which will vary from place to place and from time to time.

The insertion of an illegal consignment within a container can take place in one of two manners. The first is by targeting a legitimate container, intercepting it during its voyage, opening it and hiding the illegal consignment inside, then re-sealing the container and reinserting it into the legitimate trade flow (“hijacked” container scenario). The second way involves setting up a legitimate trading
company and building a good reputation via normal trading patterns before, suddenly, switching to trade of illegal consignments (“Trojan horse” scenario).

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

4. Container Security Measures

Generally, measures to enhance container security will address the following aspects:

- **scanning** or otherwise physically confirming the contents of the container,
- ensuring the **physical integrity** of the container,
- ensuring the security of the **container environment** as it moves and is handled in the container transport chain,
- **tracking and tracing** the container as it transits the supply chain, and
- provision and use of **information** related to the consignment.

Not all of these measures are equally suited to counter both the “hijacked” and “Trojan horse” threats. Technical measures focusing on the integrity of the container and its environment are not of much use in the “Trojan horse” scenarios. Scanning remains one of the most effective measures to ascertain both of the types of threat. Intelligence- and information-based measures must necessarily be deployed to thwart the “Trojan horse” shipper.

5. Transport Authorities, Container Security and Terrorism

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

The spectre of containers being used to deliver CBRN weapons has motivated international action to bolster the security of the container transport chain. However, very real questions remain as to terrorists’ readiness, motivation and/or capability to use a container as a delivery platform for a CBRN weapon. These questions should be addressed more thoroughly through national/international assessments of specific risks posed by terrorists to the
Trade security and trade facilitation: a potential win-win situation

Security measures must be adapted to the threat.

Transport authorities have important policy levers at their disposal.

Guiding principles to secure the container transport chain...

container transport chain. Differentiating the threat is important to Transport authorities because ill-adapted security measures can slow down or block the flow of goods nationally and internationally.

Heightened security measures should not be seen in all cases as obstructions to legitimate trade, however. Potential win-win situations could be seen between trade security and trade facilitation, where the costs of higher security can be recovered, at least partially, through greater efficiencies in the supply chain.

Appropriate measures -- container scanning, ensuring the integrity of the container itself, controlling access to the container, tracking containers, and assessing container risk via the analysis of trade-related data -- have to be chosen to counteract the “hijacked container” and “Trojan horse” threats: what works for one scenario will not necessarily work for the other.

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

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

When undertaking the above actions, transport authorities should bear in mind a number of guiding principles. These include the following:

Container Integrity

- Shippers and/or those stuffing the container must play a primary role in securing the container transport chain, because they are the main actors in “real” contact with the contents of the container.
- Shippers and/or those stuffing a container should follow established security procedures, initiate an auditable custody trail and ensure that the container is sealed with, at a minimum, a high-security mechanical seal.

For further description of these principles, please see the full Report on Container Transport Security Across Modes [CEMT/CM(2004)22].
As electronic-seal technologies are not currently ready for commercial deployment for international use throughout the global container handling network, Transport and/or Customs authorities should not mandate the use of e-seals.  

**Access to Containers**

- Vulnerabilities in the container environment are highest when the container is at rest in rail yards, at road stops and in parking and shipping/loading terminal facilities. Securing these areas to the extent possible is therefore essential. In addition, dwelling time at terminals should be reduced by rationalising and optimising the container handling process.
- Inter-modal facilities should be physically secured to minimise the risks of unauthorised access. Restricted areas should be approached only through access control by positive identification of employees and visitors and should be under constant surveillance.
- Transport operators should screen employees according to security criteria. They should also check worker identification with other operators in accordance with national laws and develop protocols regarding access to containers by high security-risk workers.

**Container Tracking**

- The focus of container tracking should not be “real-time” but rather “right-time” tracking. Transport authorities should ensure that appropriate government agencies have access to this data as needed.
- In those cases where “real-time” tracking is the right solution, these systems should not be deployed without the back-up of a more “traditional” chokepoint control tracking system.

**Co-operation with Customs: Container Scanning and Trade Documentation**

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

---

3 A clear distinction must be made between security-relevant e-seal data (e.g. seal status and container number) and supply-chain management-relevant data (packing list, shipper, consignee identity, etc). While the former should eventually be made mandatory, the latter should not.
6. Specific Recommendations to Inland Transport and Maritime Authorities

Ministers have agreed to a number of recommendations to improve security in transport that would also have specific benefits for enhancing container transport security. Detailed hereafter, these recommendations should be implemented and existing initiatives improved.

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

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

Ministers also agreed in the 2001 Ministerial Conclusions on Combating Crime in Transport to set up specific contact points within Ministries to handle all crime and security questions. At this time, some Ministries appear to have done this – many others not. Designating contact points will continue to be important, given that security issues will no doubt persist as an issue of concern for ministries of Transport and government more generally in the foreseeable future.

In addition, the ECMT Resolution No. 97/2 on Crime in International Transport contains elements that can be adapted to counter terrorist threats in the container transport chain.\(^4\)

---

\(^4\) These include recommendations that Ministries of Transport:
- set up improved contacts with the police and customs authorities as well as trade organisations to ensure that information on crime, crime trends and criminals is exchanged wherever appropriate; (N.B. though not specified in this Resolution, it would seem important to add in the case of container transport security the exchange of information with intelligence and security services.);
- check that operators given licences and permits are bone fide operators without criminal records pertinent to vehicle/freight crime;
- maintain information on persistent offenders and withdraw licences or refuse to grant permits to them;
- provide information and advice to operators on theft avoidance, safe practices, recommended routes, protected parking areas and appropriate precautions;
- encourage the setting up of secure and safe parking areas and freight traffic centres for trucks and loads (containers, trailers, swap bodies). Standards of protection for such areas must be defined to commonly agreed levels or criteria.
The establishment of an inter-governmental task force to implement a common approach to container transport security would facilitate the necessary co-ordination between Transport authorities, Customs, and security and police agencies. This task force could be set up in the larger context of inter-governmental co-ordination on the range of security issues across the transport sector, as recommended in the Policy Note and Draft Declaration on Security and Terrorism in the Transport Sector [CEMT/CM(2004)5].

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

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