

REPORT ON CONTAINER TRANSPORT SECURITY ACROSS MODES

EXECUTIVE SUMMARY

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

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

Transport Authorities Must Address Weak Links of the Container Transport Chain

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

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

More Specific Threat Assessments Involving Transport Authorities Needed

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

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

Security Measures must be Adapted to the Threat

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

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

Policy Levers at the Disposal of Transport Authorities

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

In addressing the security threat to the container transport system, Transport authorities should a) establish and/or build on rules governing container handling by operators under their authority and define procedures regarding container integrity, access and tracking, b) introduce security criteria in the licensing process of vehicles, operators, personnel and facilities and monitor whether licensees continue to meet these

security requirements and c) communicate to Customs information regarding operators under their jurisdiction that might be useful in the container screening process.

Guiding Principles to Secure the Container Transport Chain

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

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

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

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

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

Specific Recommendations to Inland Transport and Maritime Authorities

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

CONCLUSIONS: TRANSPORT AUTHORITIES, CONTAINER SECURITY AND TERRORISM

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

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

Containerised transport¹ is both an essential and massively complex system that can be likened to the global economy's circulatory system. The system is supported by a web of specialized terminals and handling facilities, transport operators, freight integrators and other actors as well as multiple strands of information flows. These have all co-evolved with the single-minded purpose of delivering steel boxes to the right destination at the right time. The ubiquity of these containers was, and is still, seen as the system's principle strength and sign of success. However, after the September 11th attacks on the United States, many countries realized that they had relatively little control over possible mis-use of the system by terrorists.

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

Transport Authorities Must Address Weak Links of the Container Transport Chain

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

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

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

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

Addressing the security of the container transport chain requires a comprehensive 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.*

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

More Specific Threat Assessments Involving Transport Authorities Needed

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

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

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

Security Measures must be Adapted to the Threat

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

Generally, the measures used to mitigate the threat of these scenarios fall into five groups: container scanning, ensuring the integrity of the container itself, controlling access to the container, tracking containers, and assessing container risk via the analysis of trade-related data. *Not all of these measures are equally suited to counteract both the “hijacked container” and*

“Trojan horse” threats as described above: what works for one scenario will not necessarily work for the other.

Policy Levers at the Disposal of Transport Authorities

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

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

Guiding Principles to Secure the Container Transport Chain:

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

Container Integrity

- Container Security is a shared responsibility among all actors; any breach in security in one link compromises the security of the entire chain. However, because they are the main actors with any “real” contact with the contents of the container, *Shippers and/or those stuffing the container must play a primary role in securing the container transport chain.*
- Shippers and/or those stuffing a container should follow established *security procedures*, initiate an *auditable custody trail* and ensure that the container is *sealed* with, at a minimum, a *high-security mechanical seal conforming to ISO PAS 17712.*
- Electronic-seal technologies *are not* currently ready for commercial deployment for international use throughout the global container handling network – primarily because of the multiplicity of competing and incompatible operating standards and

limited operational experience. These conflicts will no doubt be overcome yet, until that happens, Transport and/or Customs authorities should not *mandate* the use of e-seals.

- A clear distinction must be made between *security-relevant* e-seal data (e.g. seal status and container number) and *supply-chain management-relevant* data (packing list, shipper, consignee identity, etc). If e-seal usage is mandated, only use of the former should be made mandatory.

Access to Containers

- *Vulnerabilities in the container environment are highest in rail yards, road stops and parking and shipping/loading terminal facilities. Dwelling time at terminals should be reduced* by rationalising and optimising the process of container handling for both economic and security reasons.
- *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 – that is, ensuring that those who need to find out where a container is can do so *when* they need to know. In this context, most existing operator-specific tracking systems are sufficient for this purpose. Transport authorities should *ensure that appropriate government agencies have access to this data as needed.*
- In those cases where “*real-time*” tracking is the right solution, these systems should not be deployed without the back-up of a more “*traditional*” chokepoint control tracking system.

Co-operation with Customs: Container Scanning and Trade Documentation

- Screening and scanning of containers, while complimentary, are not the same. *100% container screening is possible, should an administration choose to do so -- 100% scanning, on the other hand, is not practical with current technologies.*
- Transport authorities should assist Customs in their container screening exercises by ensuring that “*proprietary*” information (e.g. regarding transport operators, licensees, etc.) is made available to Customs for their container risk assessment in accordance with national rules on data confidentiality.

- Transport authorities should also *support the concept of advanced information submission to Customs and use of the Unique Consignment Reference number* among transport operators.

Specific Recommendations to Inland Transport and Maritime Authorities

Agreed recommendations should be implemented and existing initiatives improved.

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

- Promote a co-ordinated 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. Given the wide and diverse range of issues related to transport crime, security and terrorism, a contact point able to centralise and co-ordinate the inquiries to the appropriate individuals of competence within the Ministry would be extremely useful.

In addition, the ECMT Resolution No. 97/2 on Crime in International Transport contains elements that can be adapted to counter terrorist threats in the container transport chain².

² These include recommendations that Ministries of Transport:

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

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

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

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

³ These include ports not participating in international trade, vessels of less than 500 GT and vessels not trading internationally.