Facilitating Trade in a Secure Environment: The Case of Containerised Cargoes

Philippe Crist – OECD Division of Transport
UNECE, Geneva, November 13-14, 2003
OECD work on Terrorism and Trade

Trade Directorate has undertaken considerable work on the description and quantification of trade facilitation measures -- including a preliminary assessment of the Trade impacts of the World Trade Center attacks.

Maritime Transport Committee is carrying out a two-year programme of work looking at terrorism risk factors in shipping, assessment of costs associated with security-related SOLAS amendments and the ISPS Code, and analysis of security concerns related to ship ownership and registration requirements.

The European Conference of Ministers of Transport and the Maritime Transport Committee are completing a project investigating the policy issues related to container verification and tracking.
Supply chain w/ a focus on maritime, containers not bulk

1. Terrorism risk in shipping
2. Securing the supply chain:
   • system description
   • current trends
3. Adapting the response to the threat
   • technology
   • information
   • standards
4. Compelling issues we should not forget...
Are the risks real?

Terrorism: USS Cole, Limburg, Sri Lanka, etc.
<table>
<thead>
<tr>
<th>Are the risks real?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorism: USS Cole, Limburg, Sri Lanka, etc.</td>
</tr>
<tr>
<td>Cargo Theft: estimated at 30-50 billion/year worldwide</td>
</tr>
<tr>
<td>Drug and contraband smuggling</td>
</tr>
<tr>
<td>Shipping container qualities: ubiquity, flexibility and velocity</td>
</tr>
</tbody>
</table>
The Port of Rotterdam: Urban/industrial mix
<table>
<thead>
<tr>
<th>Are the risks real?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Terrorism: USS Cole, Limburg, Sri Lanka, etc.</td>
</tr>
<tr>
<td>Cargo Theft: estimated at 30-50 billion/year worldwide</td>
</tr>
<tr>
<td>Drug and contraband smuggling</td>
</tr>
<tr>
<td>Shipping container qualities: ubiquity, flexibility and velocity</td>
</tr>
<tr>
<td>Cargo accidents (bulk and container)</td>
</tr>
</tbody>
</table>
Are the risks real?

Terrorism: USS Cole, Limburg, Sri Lanka, etc.

Cargo Theft: estimated at 30-50 billion/year worldwide

Drug and contraband smuggling

Shipping container qualities: ubiquity, flexibility and velocity

Cargo accidents (bulk and container)

Criminal/terrorist financing: LTTE
Possible economic repercussions of terrorist attack utilising maritime transport

US West Coast Port Shutdown: estimates range from USD 467 million to 19.4 billion.

Conference Board/Booz Allen Hamilton port security wargame: USD 58 billion (90 days)
**Container-based Logistics Chain:** International Trade from A to B

Buyer places order, validates payment...

... and shipper ships good
Container-based Logistics Chain: Detail

- Originating shipper
- Freight-forwarder/Consolidation centre
- Intermodal terminals
- Rail yard
- Road transport operators
- In-transit stop(s)
- Port
- Ocean carrier
- Gate area
- Temporary storage
- Quayside
- Customs
Container-based Logistics Chain

- Origin
- Local/regional logistics hub
- National/international hub
- Customs/government interface
- Maritime carrier
- Road/rail carrier
- Destination
- Shipper
- Port
- Ocean voyage
- Interchange/transhipment
- Buyers/consignees
214 000 000 TEU’s handled by ports worldwide (173 million minus empties)

Number of actors involved?

Data required? @ 30 shipping/trade documents per container: Approx. 5.2 billion!

System works extremely well: fast, flexible and affordable trade.

But… is the present system compatible w/ new security concerns
World Container Transport System: 2 views

(Current) Trade-driven System

Fast, flexible, ubiquitous

Key variables:
- Speed/Timely delivery
- Secure Payment
- Trust

Performance Measure (examples):
- Did the container make it on time?
- Was payment delivered on time?

Security-driven system

Secure, verified and transparent

Key variables:
- Known shippers/transport actors
- Strong and verified container integrity
- Secured container environment
- Trust but verify

Performance Measure (examples):
- Who packed the container?
- Who accessed the container?
- Where is the container from?
- Where is the container?
Pre-World Trade Center Attacks, Customs operate at national points of entry.
Pre-World Trade Center Attacks, Customs operate at national points of entry. Some shippers/operators have anti-theft measures in place.
Container-based Logistics Chain: Customs and Trade Security

Post-World Trade Center attacks, US Container Security Initiative and 24-hour rule push “borders” to last port of loading... and beyond.
IMO SOLAS and ISPS (effective July 2004) seek to secure the maritime leg and port interface.
US C-TPAT proposes to push the security “perimeter” upstream to encompass the entire trading environment.
Container Security: Two fundamentally different threats

“Hi-jacked” Container

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

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

**Risk of discovery:**
Relatively high given risk of discovery and numerous visual inspections along the transport chain.

Container from “Trojan Horse” Shipper

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

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

**Risk of Discovery:**
In the case of a trader with an established “legitimate” trading record, very low.
Container Threats: 5 Responses

1. Scanning & Inspection
2. Ensuring Container Integrity
3. Securing Container Environment
4. Container Tracking
5. Container/Trade documentation & data
Reconciling Threats and Responses: Hijacked vs. Trojan Horse Containers

- Scanning & Inspection
- Physical Integrity
- Container Environment
- Tracking
- Trade docs & data

“Hi-jacked” Container

“Trojan Horse” Shipper
Reconciling Threats and Responses: Hijacked vs. Trojan Horse Containers

Scanning & Inspection | Physical Integrity | Container Environment | Tracking | Trade docs & data

“Hi-jacked” Container | Technology-oriented responses

“Trojan Horse” Shipper | Intelligence-oriented responses
Dishonest employees of common carriers have discovered the weakest link in cargo container security: the bolt connecting the handle to the locking bar. In less than two minutes, simply using a common household electric drill, the handle can be disconnected from the locking bar.

The result: **the door will open without the seal ever having been touched.**

It's a simple matter to insert a replacement bolt, add a few dabs of touch-up paint, and no one will be the wiser. Even the trained eye of a marine surveyor will be hard-pressed to notice the evidence of tampering!

*(www.sealock.com)*
Reconciling Threats and Responses: Technology

• Seals only provide evidence of tampering, they do not secure the container, and often do not even secure the door to the container.

• Existing standards for high security seals (PAS 17712) should be met, at a minimum -- further work possible with mechanical seals.

• A good seal in a bad process is worthless -- sealing methodologies and practices must be standardised across the supply chain.

• Electronic seals: Most shippers are not e-ready -- electronic means should enhance mechanical seal and not replace it -- in the short to medium run.

• Data should pertain to security concerns, write capability superfluous and possibly dangerous.

• Must not be wedded to proprietary readers/technology and should be useable across the globe (single radio frequency).

• Dangers of vendor-led process, need consensus and/or decision by regulatory authorities on needs before technology is adapted.
Detecting container security risks requires access to a lot of information… from divergent sources.

Information used for targeting inspections… not in lieu of inspections.
Container Inspection: Customs “authorisation” and targeting
Container Inspection: Customs “authorisation” and targeting

Large volume of container trade is repetitive: Same shippers, same shipments, same consignees, large number of containers. These streams are relatively easy to “secure” (CT-PAT, in-house systems, high-quality data control) and can be slated for less rigorous customs scrutiny.
"Un-authorised" containers are subjected to greater data scrutiny and subjected to a targeting matrix.

"Problem" containers are scanned and/or inspected.
physical flow: “where is the container?”

- container yard operator
- truck/road
- factory
- truck/road
- consolidation centre
- truck/road
- intermodal facility
- wagon/rail network
- rail yard
- wagon/rail network
- intermodal facility
- truck/road
- port gate
- port storage
- quayside
- vessel

flow of custody: “who knows where the container is?”

- container yard operator
- shipper
- local truck firm
- cons. ctr. operator
- long-dist. truck firm
- rail operator
- local truck firm
- port terminal operator
- carrier

- freight forwarder/3PL

flow of container information: “who knows what is in the container?”

- buyer
- buyer’s agent
- buyer’s bank
- shipper
- shipper’s bank
- freight forwarder
- (land transport operators)?
- (port terminal operator)?
- customs
- customs broker
- carrier

data transmission forms and methods: “how and what info. is passed on?”

- Invoice
- Packing list
- Visa
- Original bill of lading
- Purchase order
- Block train composition
- Letter of credit
- House bill of lading
- Master bill of lading
- Ship manifest
- Import entries
- Paper/flat files
- Fax
- In-house EDI
- 3PL EDI
- Internet
- EDIFACT
- Port EDI
- Customs EDI
- Carrier EDI
Ideally, the physical flow, events and actors along the container logistics chain would be tightly coupled to information and documentation flow.

but....

• Poor integration/coordination amongst different actors, processes and data systems.
• Manual processes for coordinating manifest and shipping data.
• Inability to quickly isolate and act on security and logistics exceptions.
• Unnecessary process and data lead times caused by incompatible structures.
• Data re. container is faster/slower than actual container movement.
World Customs Organisation initiatives: Advance Cargo Information and Unique Consignment Reference number.

Harmonised trade documents, information transmission protocols (both paper and electronic) and trade processes -- need to ensure adequate “hooks” between public and proprietary systems -- role for UNECE, UNCTAD, ICC, and industry.

Industry-Government partnerships -- Information Analysis and Action Centres for operational management of security incidents.
**Standards: What role, what reality?**

Pre-2001 trade based on (blind?) trust, post 2001 trade to be based on verifiable trust.

Standards are the “language” of verifiable trust.

However, it is not likely that security/customs “standards” will be accepted until the question of vetting is solved….

In the short run, it is more likely that standards can serve as guidelines for bilateral agreements.
Closing: Compelling issues and open questions....

Is container security scaleable? How much security, for whom and when?

Costs: a. Not all costs are costs. B. Not all exports face the same logistics costs. Developing countries and low-value exports will be hit disproportionately.

Paying for security: What is easy (for regulators) is not necessarily fair nor efficient. How to structure cost recovery?

E-everything (Customs, Trade, Industry) vulnerabilities… role for strong and evolving cyber-security.

The world is not on-line, mandating unrealistic technology will create a trade divide -- in the short- to medium-term.