Keywitness:
Towards "illicit <> security @ cross-border supply chains" - research framework to support assessment of research gaps and setting up of priorities, in the context of customs risk management & future threats

Dr. JuhaHintsaa
Cross-border Research Association
Lausanne, Switzerland

Illicit side – one (rough) crime taxonomy – supply chain view

1. Illicit activities where supply chain (performance) suffers directly from these acts
   – E.g. cargo theft, vehicle hijacking (incl. sea piracy), sabotage, destruction inside supply chain (terrorism)

2. Supply chain are exploited in order to carry out illicit activities (no automatic disruption in supply chain)
   – E.g. prohibited and restricted goods smuggling, duty and tax fraud, counterfeit goods, parallel trade, destruction at target destinations (terrorism)

3. Illicit acts which do not bring immediate (illegal) benefit, but rather facilitate points 1 or 2 above.
   – E.g. cyber crime, document forgery, false or stolen identities, violence (in parts), corruption (two types),
Illicit side - Examples of potential knowledge gaps today

- **Crime consequences** (per stakeholder / victim group; policy, enforcement, logistics, cargo owner, security business, insurance, citizen / consumer / tax payer)
- **Crime statistics** (much is inaccurate & much goes unreported)
- **Crime linkages & portfolios** (what facilitates what, e.g. cyber crime & smuggling)
- **Crime dynamics / displacement** (increasing security may lead to crime shifting to another place / time / mode)
- **Illicit supply – demand formation** (e.g. counterfeit goods, drugs, endangered species)
- **Illicit actors & motivations** (from petty criminals and insiders to organized crime and terrorist groups)
- **Illicit fulfillment / execution** (including transport mode & routing; concealment etc.)
- **Cost-benefit, including risks, for the illicit actors** (crime profitability; likelihood of getting caught; severity of penalties)
- **Share of "commercial supply chains"** (versus other means)
Security side (8-layer Supply Chain Security Management model)

<table>
<thead>
<tr>
<th>Layer</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. RISK MANAGEMENT LAYER</td>
<td>Threats</td>
</tr>
<tr>
<td>2. DESIGN AND PLANNING LAYER</td>
<td>Supply chain design</td>
</tr>
<tr>
<td>3. PROCESS CONTROL LAYER</td>
<td>Sourcing / making / transport / distribution processes</td>
</tr>
<tr>
<td>4. SUPPLY CHAIN ASSETS LAYER</td>
<td>Facilities</td>
</tr>
<tr>
<td>5. HUMAN RESOURCES MANAGEMENT LAYER</td>
<td>Hiring</td>
</tr>
<tr>
<td>6. BUSINESS PARTNER MANAGEMENT LAYER</td>
<td>Screening</td>
</tr>
<tr>
<td>7. AFTERMATH CAPABILITIES LAYER</td>
<td>Business continuity</td>
</tr>
<tr>
<td>8. DISRUPTING CRIMINAL / ILlicit SUPPLY CHAINS</td>
<td>Disrupt sourcing / making / transport/distribution</td>
</tr>
</tbody>
</table>
Security side – ”What is good security made of” - Examples of potential knowledge gaps today

- **PRE-CONDITIONS FACILITATING SUCCESS**
  - User awareness
  - User belief
  - User commitment
  - Practicability
  - Availability

- **QUALITY AND SUSTAINABILITY**
  - Low false-rates
  - Stability
  - Harsh conditions
  - Anti-tampering

- **EFFECTIVENESS**
  - Crime reduction
  - SCS compliance
  - Collateral benefits

- **INTERDEPENDENCY MANAGEMENT**
  - Easy to identify
  - Limited number
  - Low coordination cost

- **CONSEQUENTIAL COSTS**
  - Crime displacement
  - Escalating effects
  - Creative adoption
  - Enticement effects

- **TIME-BASED PERFORMANCE**
  - Security side: minimum time
  - Crime side: maximum time

- **ETHICAL AND ESTHETICAL IMPACTS**
  - Civil liberties
  - Conduct of staff
  - Stakeholders
  - Environment

- **Examples of potential knowledge gaps today**
Keywitness observations and interpretations in the context of security, customs risk management & future threats <> customs-academia collaboration

- Opportunities & benefits
- Challenges & bottlenecks
- Requirements & recommendations
- Final words
Supply chain security overview diagram (adapted from Juettner et al. 2003)
Increasing price

Licit support services
- Carriers, communication systems, technology, banking

Illicit support services
- Financiers, contractors, storage, enforces, protectors, money launderers

Labour / Time
- Refiners / Producers
- Distributors / Couriers
- Marketing and retailers

Raw material
- Refined / Manufactured
- Packaged / Minimized
- Adulterated ("cut")

Inbound logistics
Operations
Outbound logistics
Sales and Marketing

Supply Chain Crime Taxonomy

Supply chain crime covers illegal acts that exploit infrastructure and services of legitimate logistics and transport function, or facilitate such activities.

- **Theft**
  - Against: Supply chain stakeholders

- **Trafficking**
  - Violation of: Restrictions
  - Duties and taxes

- **Indirect attack**
  - Against: Supply chain
  - Third party

- **Breaking rules of legitimate commerce**
  - At the expense of: Customer
  - Supplier
  - Society as a whole

- **Direct attack**
  - Against: Supply chain

- **Facilitation**

Männistö and Hintsa (2012)
"All parties" in supply chain security – research perspective (CBRA 2012)

Supply chain security research, CBRA traditional partners

With governmental institutes:
- Policy makers
- Law enforcement

With supply chain companies:
- Cargo owners
- Logistics sector

With "security businesses”
- Solutions, services
- Insurance sector

Additional "stakeholders” for the future

Offenders (ex-offenders)

Victims of crime
Four categories of "customs clients" (WCO 2011)

<table>
<thead>
<tr>
<th>RISK LEVEL</th>
<th>Low</th>
<th>Voluntary compliance; People who want to comply</th>
<th>Assisted compliance; People who try to comply but don't always succeed</th>
<th>Directed compliance; People who will avoid complying if they can</th>
<th>Enforced compliance; People who deliberately do not comply</th>
</tr>
</thead>
<tbody>
<tr>
<td>CLIENT CATEGORIES</td>
<td>Voluntary compliance; People who want to comply</td>
<td>Assisted compliance; People who try to comply but don't always succeed</td>
<td>Directed compliance; People who will avoid complying if they can</td>
<td>Enforced compliance; People who deliberately do not comply</td>
<td></td>
</tr>
<tr>
<td>CLIENT BEHAVIORS</td>
<td>Voluntary compliance; Informed clients</td>
<td>Attempting to comply; Uninformed clients</td>
<td>Resistance to compliance; Will avoid if possible</td>
<td>Criminal intent; Illegal activity</td>
<td></td>
</tr>
</tbody>
</table>
Examples of past and current European research projects – Thanks to European Commission

- **FP7-project CWIT**: “Countering WEEE (Waste Electrical and Electronic Equipment) Illegal Trade”. New project to be launched early 2013, with two year duration.