

## 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. Juha Hintsa

Cross-border Research Association

Lausanne, Switzerland

PICARD2012 Conference, Morocco 25-27.9.2012

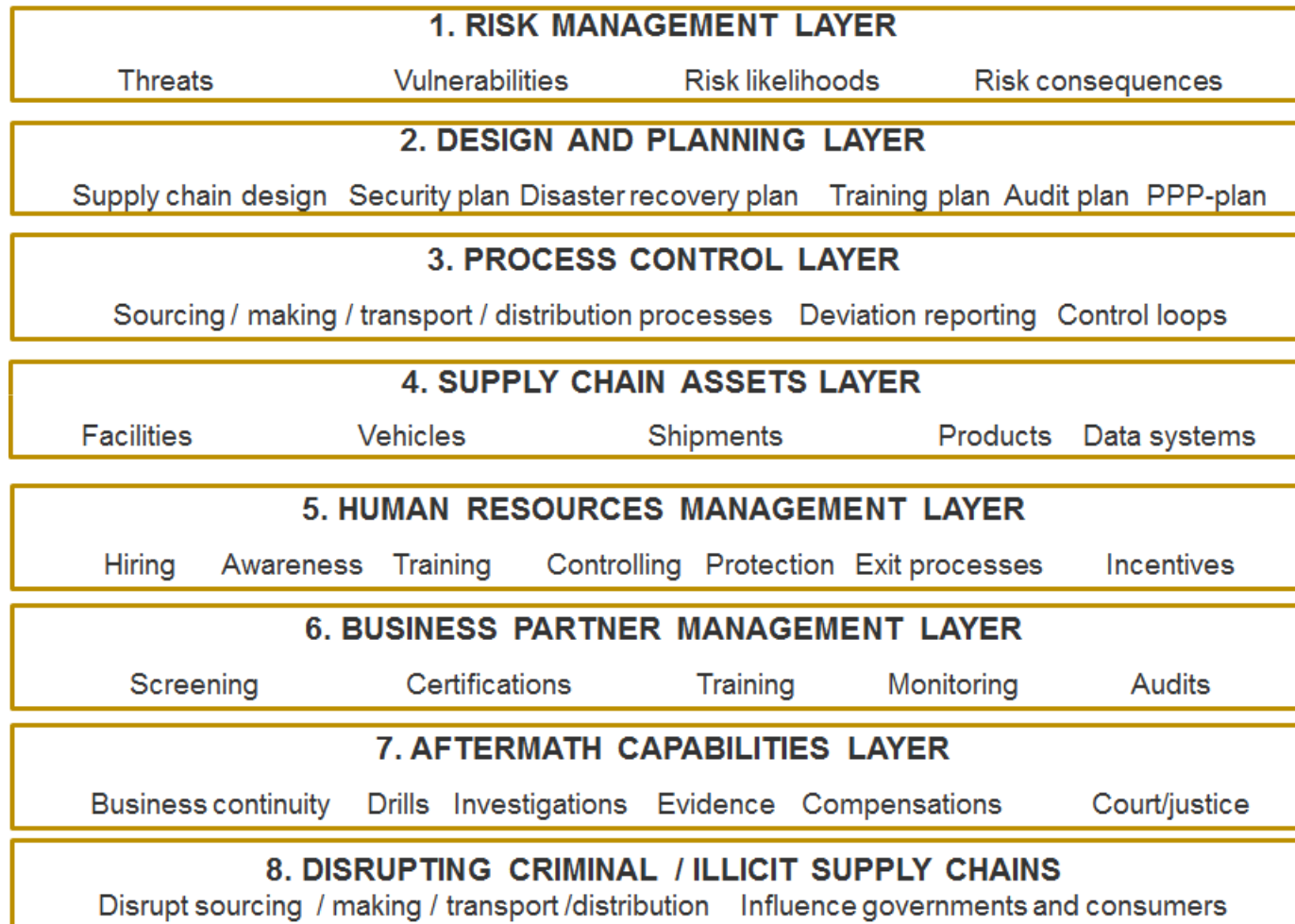
# Illicit side – one (rough) crime taxonomy – supply chain view

- 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)



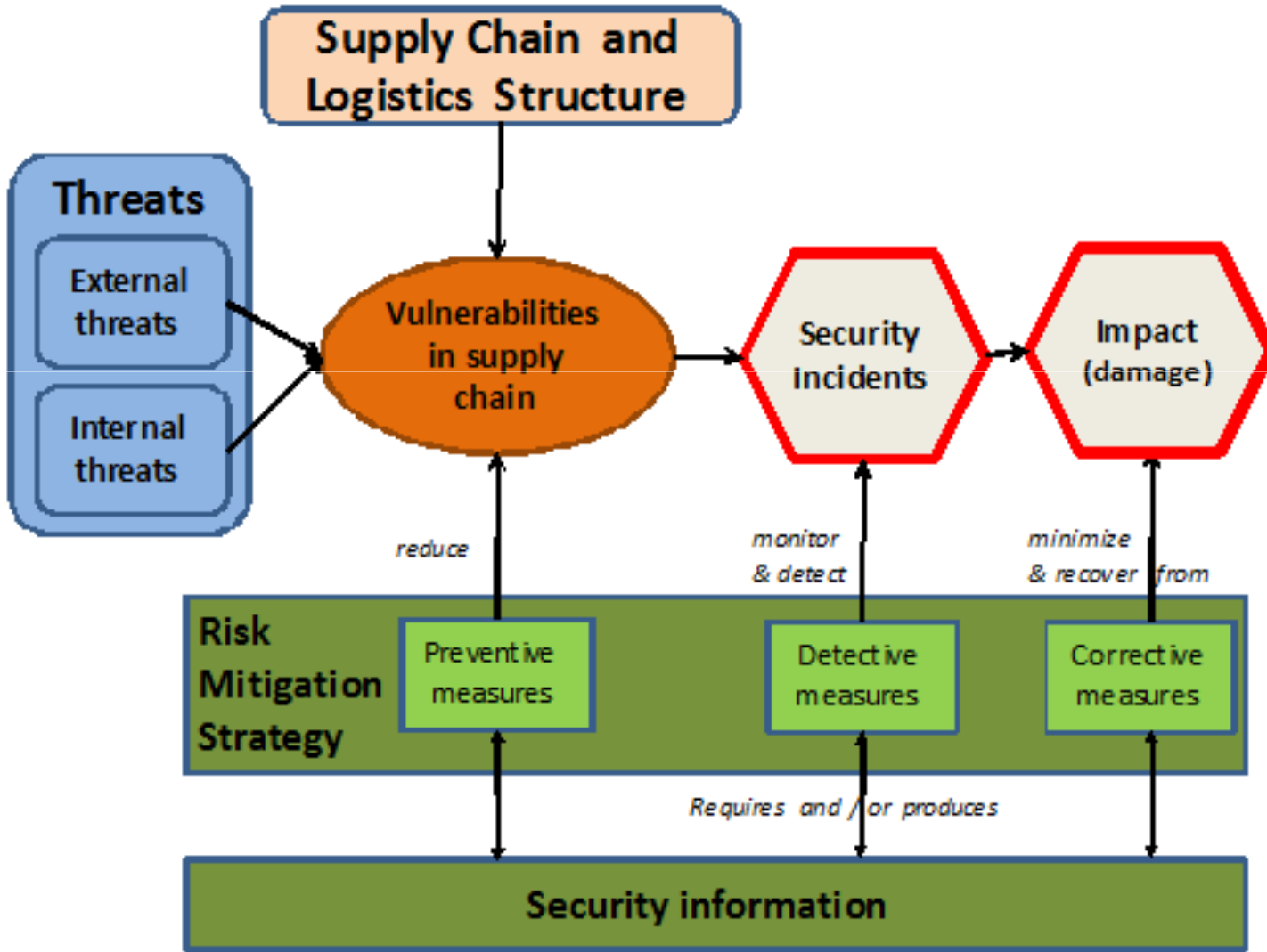
# Security side – “What is good security made of” - Examples of potential knowledge gaps today

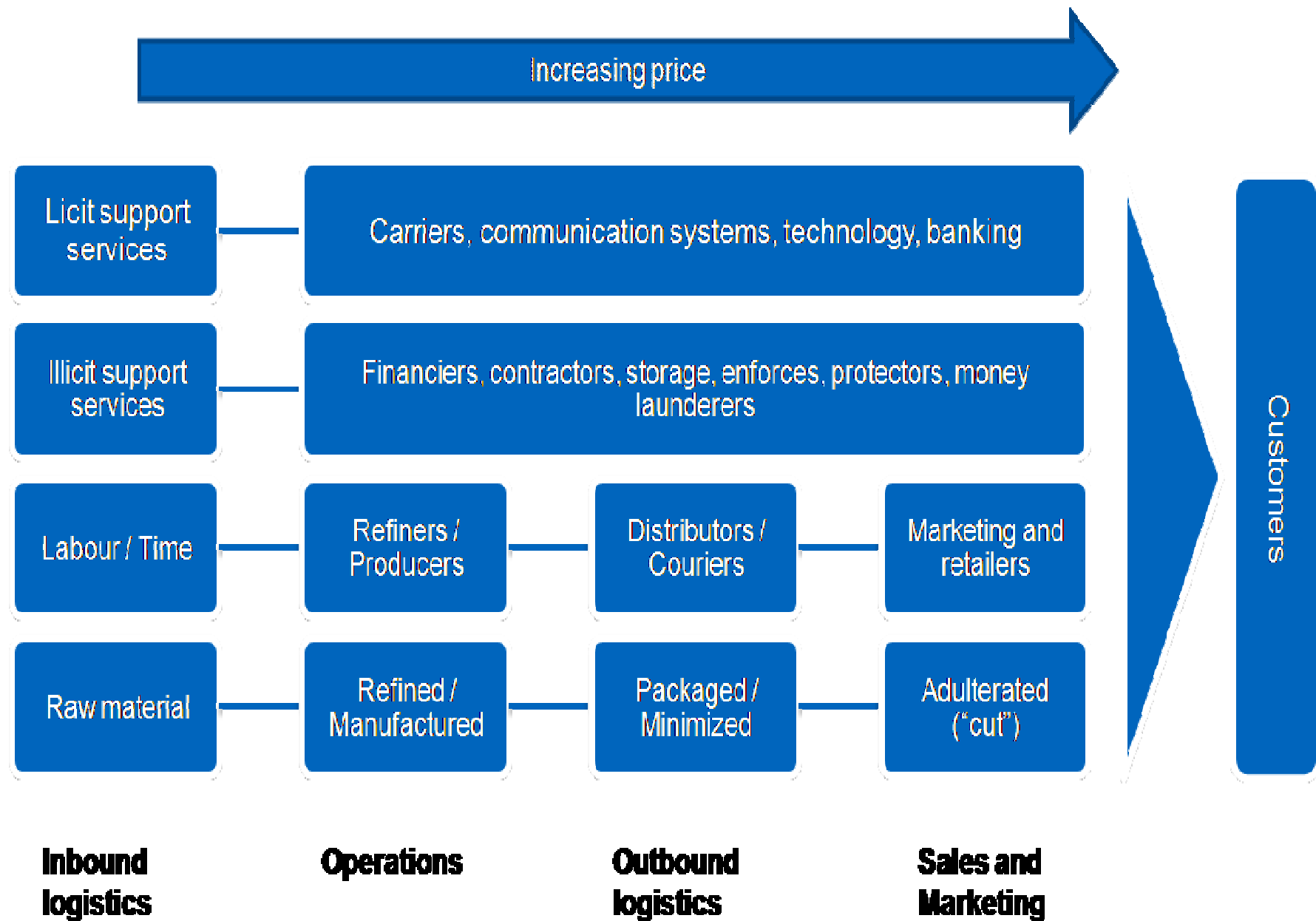


Keywitness observations and  
interpretations in the context of  
security, customs risk management &  
future threats <> customs-academia  
collaboration

- Opportunities & benefits
- Challenges & bottlenecks
- Requirements & recommendations
- Final words

# Supply chain security overview diagram (adapted from Juettner et al 2003)



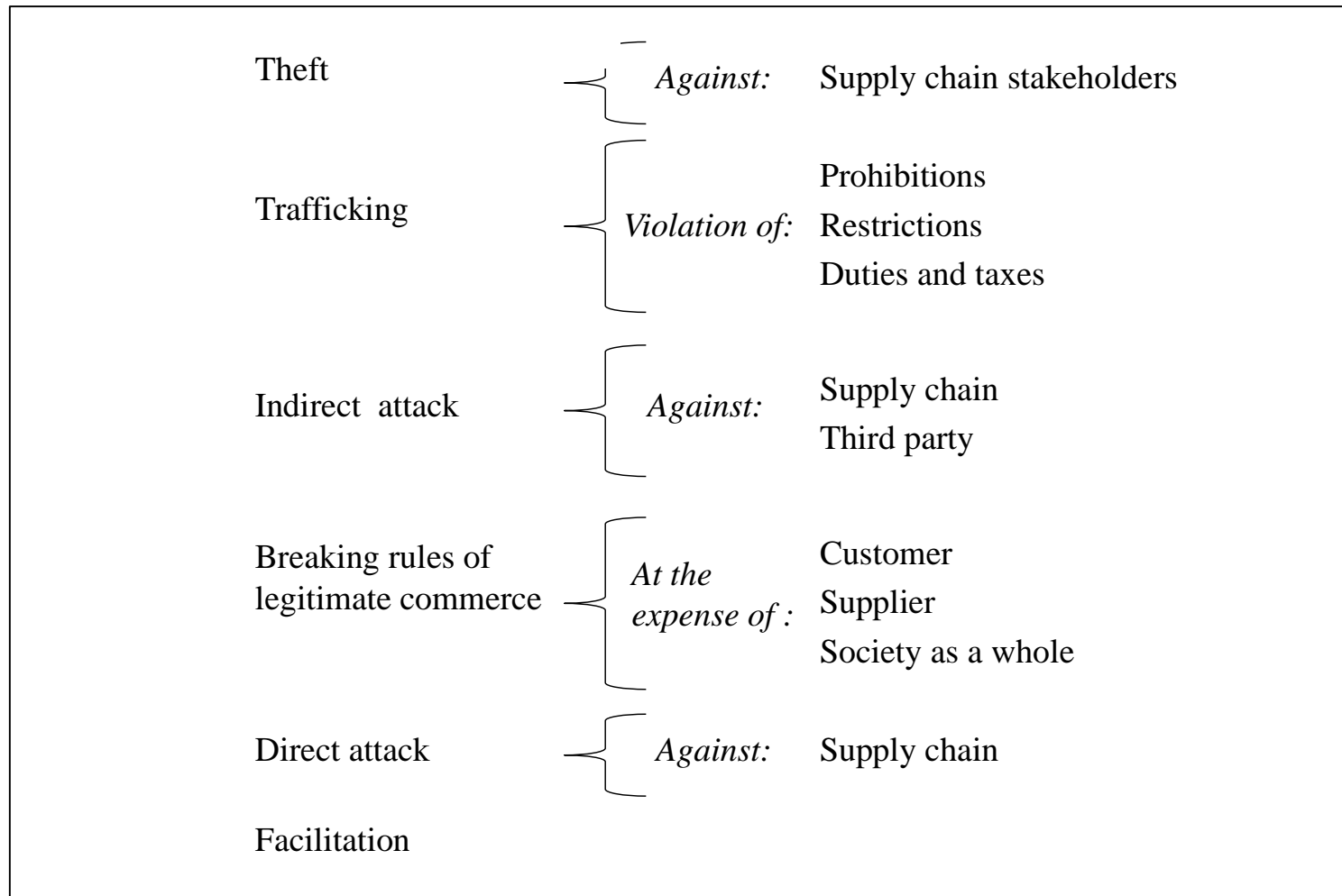


Source: Alan Wright (2006) Organized Crime, Willan Publishing s. 90

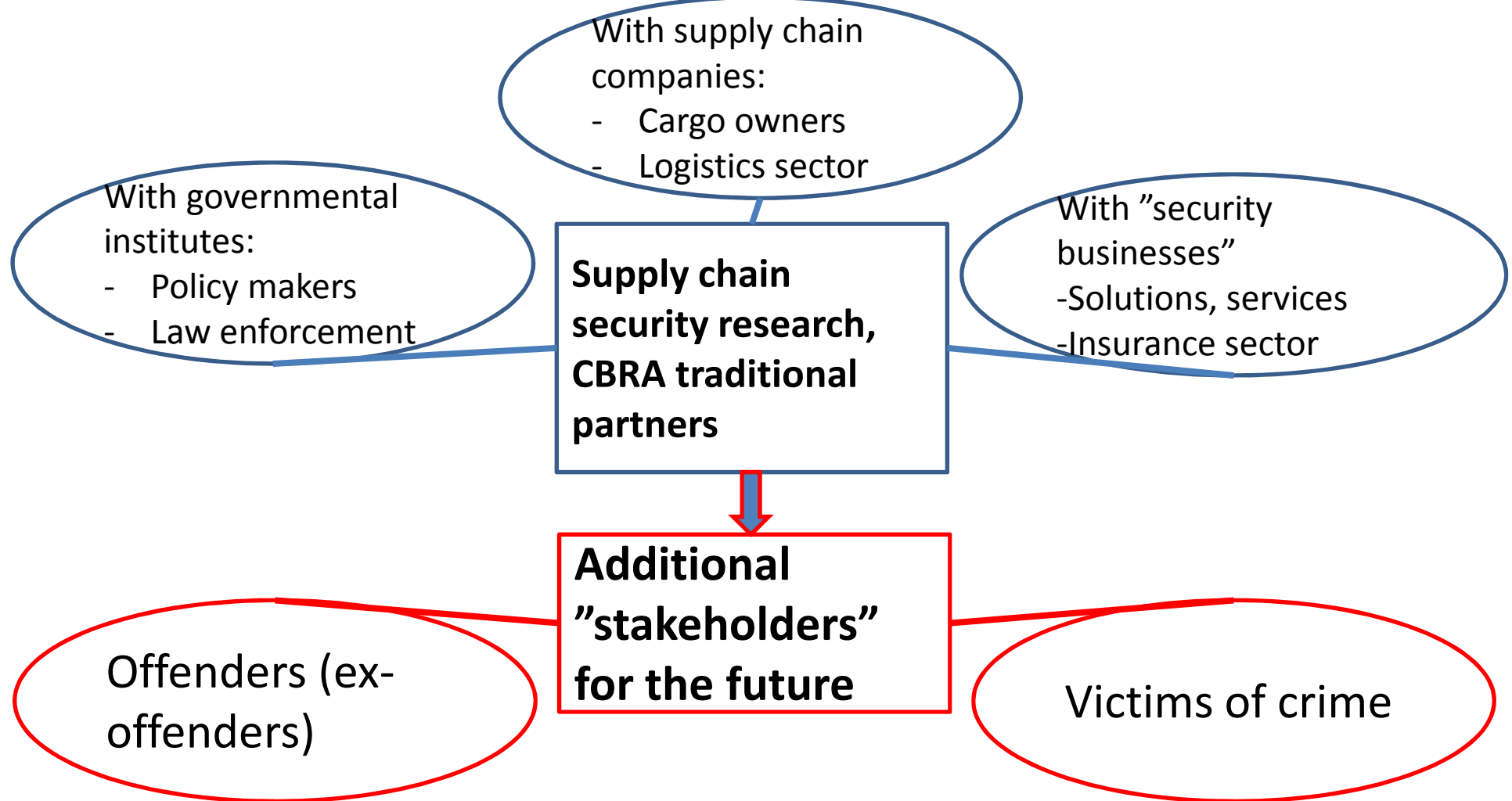


# Supply Chain Crime Taxonomy

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



# "All parties" in supply chain security – research perspective (CBRA 2012)



# Four categories of "customs clients" (WCO 2011)



<b>CLIENT CATEGORIES</b>	Voluntary compliance; People who want to comply	Assisted compliance; People who try to comply but don't always succeed	Directed compliance; People who will avoid complying if they can	Enforced compliance; People who deliberately do not comply
<b>CLIENT BEHAVIORS</b>	Voluntary compliance; Informed clients	Attempting to comply; Uninformed clients	Resistance to compliance; Will avoid if possible	Criminal intent; Illegal activity

# 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.
- **FP7-project SAFEPOST:** “Reuse and Development of Security Knowledge Assets for International Postal Supply Chains”. Grant agreement no: 285104. Date: 1.4.2012-31.3.2016 *SAFEPOST URL: <http://www.safepostproject.eu/>*
- **FP7-project CASSANDRA:** "Common assessment and analysis of risk in global supply chains ". Grant agreement no: 261795. Date: 1.6.2011-31.5.2014 *CASSANDRA URL: <http://www.cassandra-project.eu/>*
- **FP7-project FOCUS:** " Foresight Security Scenarios: Mapping Research to a Comprehensive Approach to Exogenous EU Roles ". Grant agreement no: 261633. Date: 1.4.2011-31.3.2013 *FOCUS URL: <http://www.focusproject.eu/>*
- **FP7-project LOGSEC:** “Development of a strategic roadmap towards a large scale demonstration project in European logistics and supply chain security”. Grant agreement no: 241676. Date: 1.4.2010-31.3.2011 *LOGSEC URL: <http://www.logsec.org/>*
- **FP7-project INTEGRITY:** “Intermodal Global door-to-door container supply chain visibility”. Grant agreement no: 218588. Date: 1.6.2008-30.10.2011 *INTEGRITY URL: <http://www.integrity-supplychain.eu/>*