

---

# UNECE 15.1.2009

## Inland transport security

Mr. Juha Hintsa

Cross-border Research Association;  
EPFL & HEC UNIL, Lausanne



# Cross-border Research Association (CBRA)

- CBRA was formally established in 2005 with HEC University of Lausanne in the field of Supply chain security in the year 2002.
- CBRA acts as an independent organization for a better understanding of the challenges in international supply chain management.
- CBRA works both with academic and government agencies (customs, etc.) to achieve the objectives and constraints of each, promoting one over the other.
  - World Customs Organization; Textiles; Clothing; Machinery; Logistics sector; TRADE INTEGRATION - etc.
- Our team has following nationalities (in alphabetical order) since past few years: Bangladesh, Belgium, Canada, China, Colombia, Finland, Germany, India, Italy, Jordan, Luxembourg, Netherlands, Romania, Senegal, Switzerland, Turkey, UK, USA

CBRA is bringing the operations management approach to cross-border, security and customs business!

- Business process (re)design
- Technology management
- Performance measurement
- Cost management



We look always for new, highly motivated researchers to join us!!

# Foreword (yes, we know this)

---

- International trade: high product variety & increasing volumes
- International supply chains: long chains & complex structures
- International supply chain crime: smart & growing
- Supply chain security initiatives: lots going on



# Agenda

---

- Part A:
  - Supply chain security (SCS) definitions
  - Complexities regarding SCS research
  - The position of SCS end-user - state of confusion!?
  - Roles and demand for SCS academics – is there?
- Part B:
  - CEN Feasibility study on SCS toolbox / standard



# Supply chain security management (SCSM) definitions

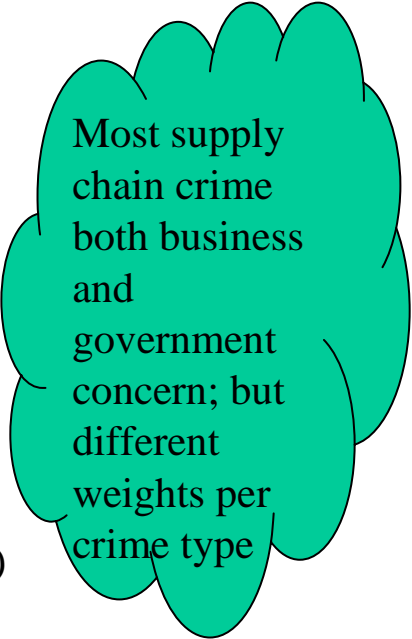
---

- "SCSM can be defined as the application of policies, procedures, and technology to protect supply chain assets from theft, damage, or terrorism, and to prevent the introduction of unauthorised contraband, people, or weapons of mass destruction into the supply chain“ – Closs et al. 2004.
- “SCSM covers all processes, technologies and resources exploited in a systematic way to fight against end-to-end supply chain crime; the primary goal of each single SCSM measure is either to prevent a crime, to detect a crime, or to recover from a crime incident in fastest possible time; single SCSM measures fall typically in one of the following five categories: cargo, facility, human resources, information technology, and management systems; the typical supply chain crime includes theft, smuggling, counterfeit, sabotage for financial gain, terrorism for destruction, and any type of fraud and corruption (the detailed crime definitions subject to national and international regulations).” - Hintsä et al. 2009.

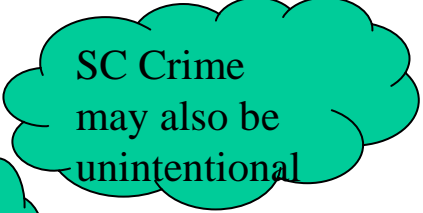


# Various types of supply chain crime

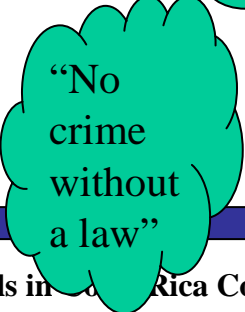
- Theft (single pieces)
- Theft (full shipments / units)
- Smuggling (for duty fraud)
- Smuggling (for illegal goods)
- Other illicit trade
- Intellectual property violations
- Other industrial espionage
- Sabotage (planned)
- Causing ad-hoc damage (irrational)
- Civil unrest (looting etc.)
- Source side crimes (bad ingredients / raw materials etc.)
- Illegal sales (selling to minors / without recipes etc.)
- Data system crime
- Blackmailing
- Violence (illegal threat, act of violence)
- Money laundry
- Terrorism (destruction on supply chain)
- Terrorism (destruction on destination)
- Corruption



Most supply chain crime both business and government concern; but different weights per crime type



SC Crime may also be unintentional



“No crime without a law”



---

# Complexities regarding SCS research (and policy making; and security management)



# SCS researcher wish list – page 1

---

*“Bring me the wisdom, to carry the research, and publish the results, on following topics (as no-one has been able to)”:*

- Proving which security measures are REALLY efficient (per product type; per crime type; per geography etc.)
- Modeling how to calculate the TRUE cost of security in end-to-end supply chains
- Measuring the REAL benefits which are gained by SCS enhancements (focus on tangible ones)
- Showing how Chief security officers should divide their budgets between various types of security measures (cargo – facility – HR – IT etc. ; prevent – detect – recover etc.)
- Creating accurate statistics on various crime incidents (theft, smuggling, IPR etc.)
- Analyzing whether SCS can ACTUALLY become a (technical) barrier for trade





# SCS researcher wish list – page 2

---

*“Give me the wisdom to achieve following”:*

- I will understand the REAL threats and vulnerabilities in supply chains; maybe even bit on the probabilities and consequences.
- I will get access to detailed corporate and government SCS data (so I can analyze – write – publish)
- I will recognize which SCS technologies actually REALLY work (maturity, robustness, open standards, false positives, etc.)
- I can see through the SCS hype; through superficial SCS initiatives; through the SCS push...
- I will NOT promote SCS buzzwords in 2009 (“collateral this-and-that”; “...facilitation”; “9/11...”)



---

So....

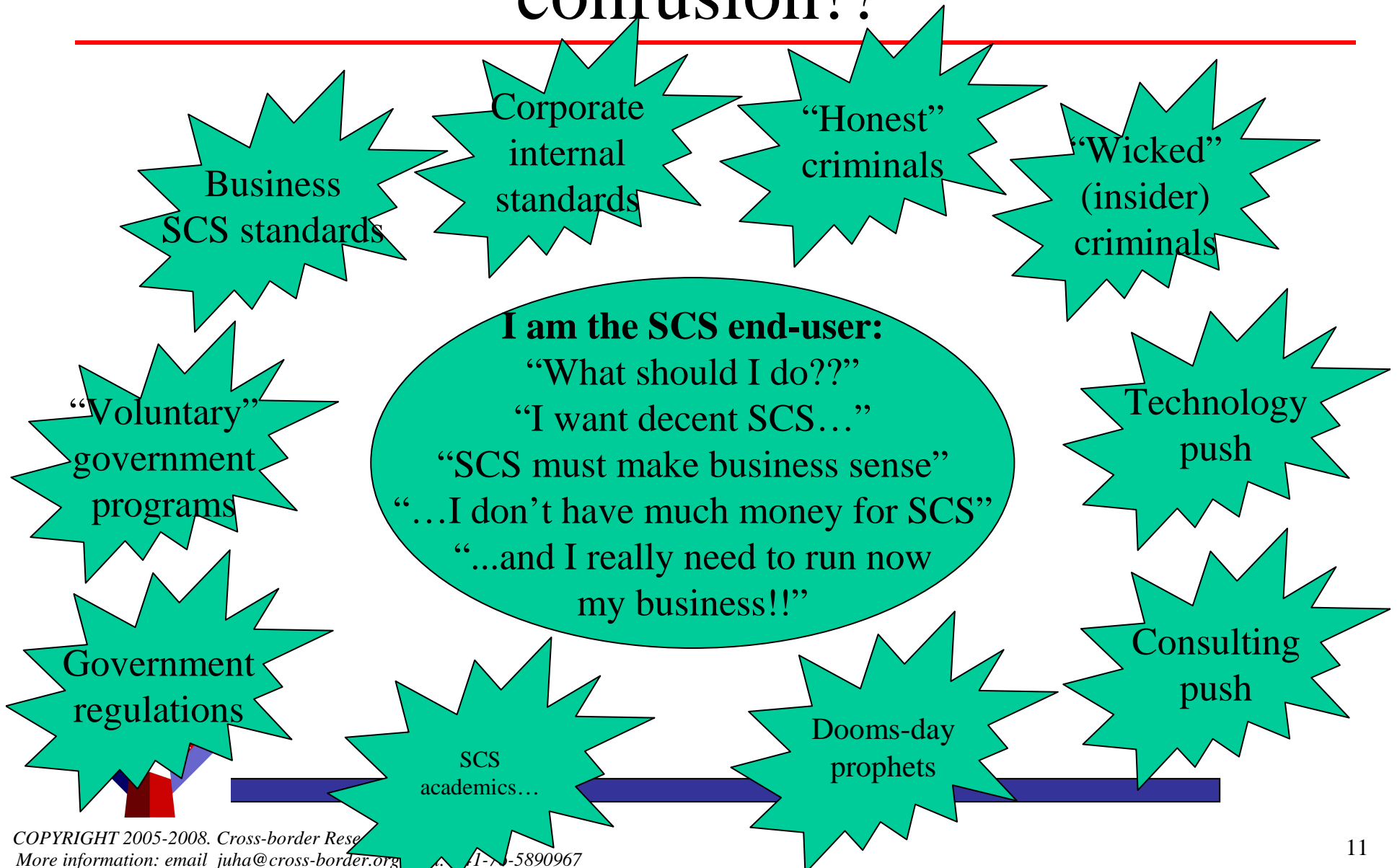
Supply chain security @  
Academic research:

Nightmare... or Daydream?



# Poor SCS end-user - state of confusion!?

---



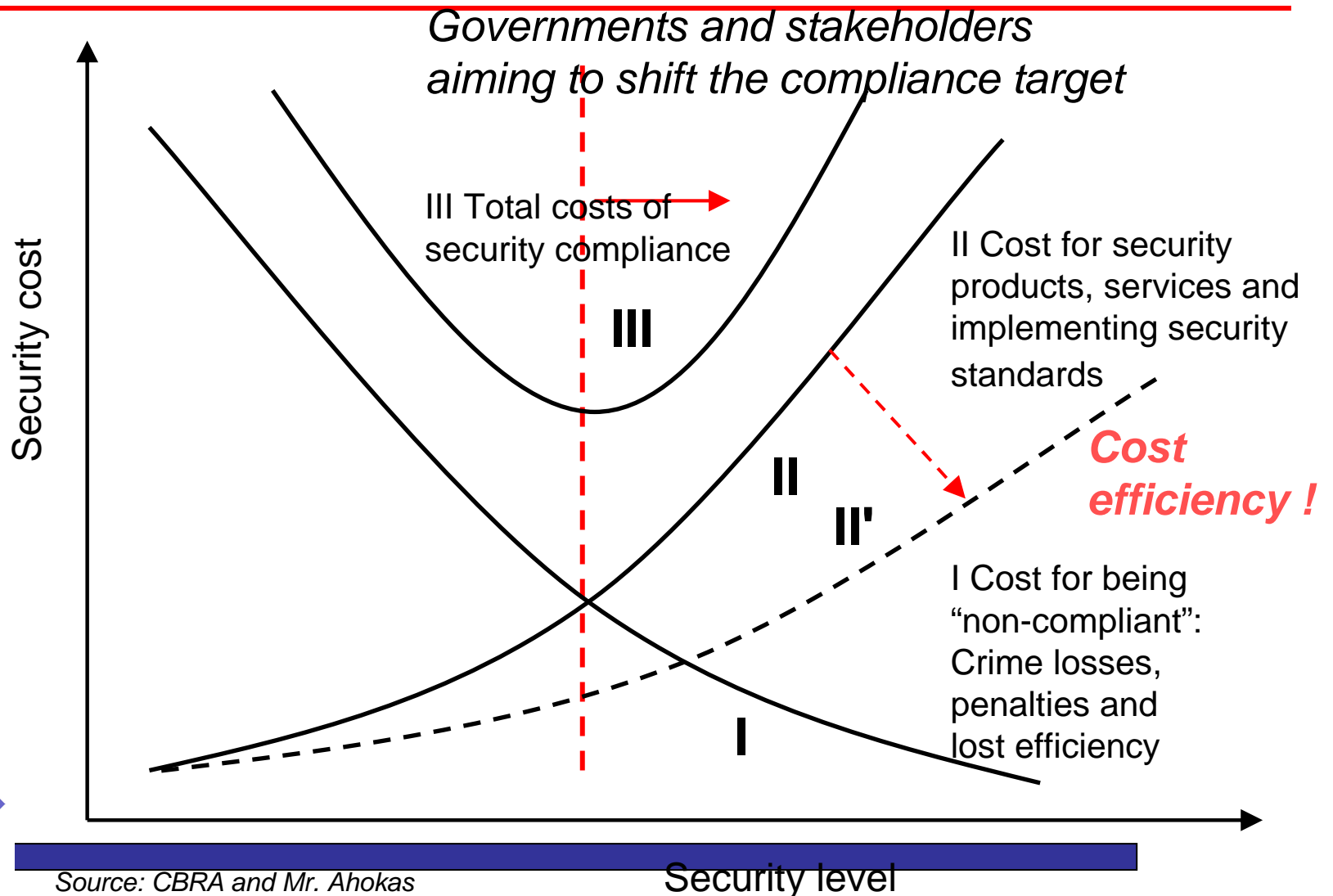
# Roles and demand for SCS academics – is there?

---

- Researching for SCS theories; constructs; definitions; paradigms; bottlenecks; weakest links...
- Applying principles from operations management; optimization; simulations; game theories; statistical analysis...
- Assessing SCS technology and/or procedure pilots...
- Publishing articles; case studies; book (chapters); good practices; benefits; costs...
- Contributing to standards development..
- ...what else??



# As we know, at the end of the day, SCS is an(other) optimization problem!!!



Source: CBRA and Mr. Ahokas

# Part B.

---

## CEN Feasibility study on SCS toolbox / standard

Around 5 million companies in Europe?  
Maybe 10% within the EU AEO pool?

Would businesses benefit from a  
“light SCS toolbox/ standard”,  
which has been created by the  
end-users themselves?



# CEN SCS - Overall objectives (expert group, 2005 onwards)

---

- To enhance security in the supply chain, i.e. secure interconnectivity between the various transport modes, operators and public authorities
- To define the most effective and cost-effective measures in relation to the three levels of risks (normal, heightened, exceptional)
- To develop a method for supply chain vulnerability assessment by operators in the supply chain
- To allow business the opportunity to develop tailor-made and cost beneficial security measures
- To streamline different terminologies on supply chain security statuses



# CEN SCS - Possible elements of research (spring 2009)

---

- Analysis and comparison of the existing labels and standards
- Identification of user needs and requirements regarding a possible toolkit and/or standards
- An analysis whether a specific rather than generic risk approach for SMEs will be necessary
- An analysis whether a CEN SCS standard can reflect the nature of security threats, which may be country / mode specific rather than EU wide.
- An analysis of the experience obtained in various Member States while implementing the AEO; including operators who are not covered by customs legislation





# Feasibility study kick-off meeting at CEN, Brussels, 6.2.2009

---

Please contact us on any ideas, comments,  
source files, etc. regarding the  
CEN SCS Feasibility study!!

Email: [juha@cross-border.org](mailto:juha@cross-border.org)  
Tel. +41-76-5890967

Thanks!

