Supply Chain Response to Global Terrorism: A Situation Scan

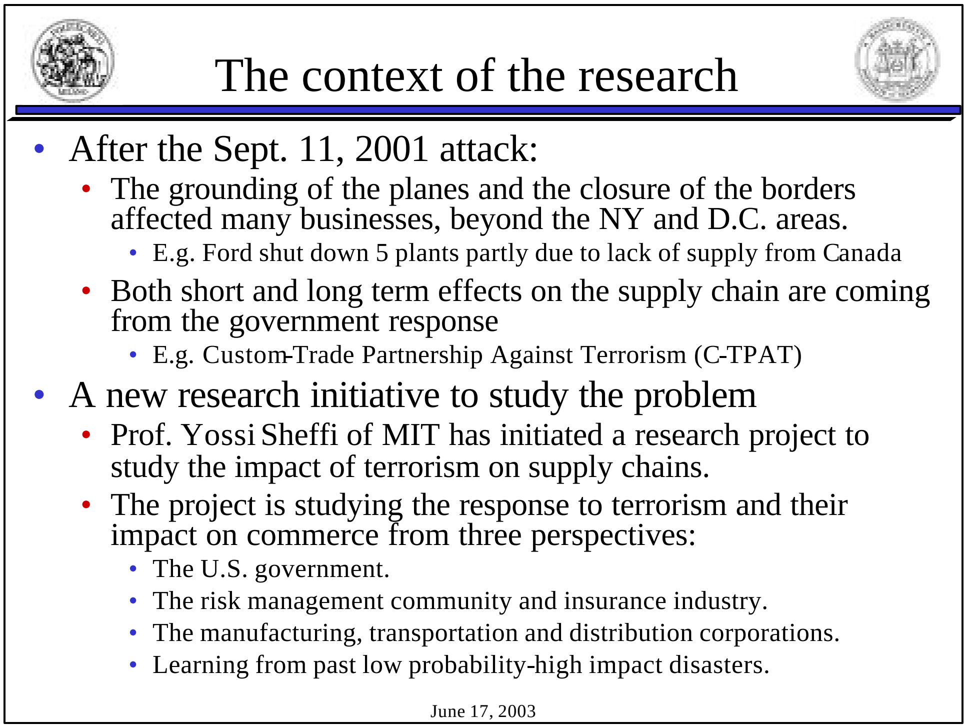
Yossi Sheffi, James B. Rice, Jr.*, Jonathan M. Fleck*, Federico Caniato°*

* Center for Transportation and Logistics, Massachusetts Institute of Technology
° Department of Management, Economics and Industrial Engineering, Politecnico di Milano

Cernobbio, June 17, 2003
EurOMA POMS Joint International Conference

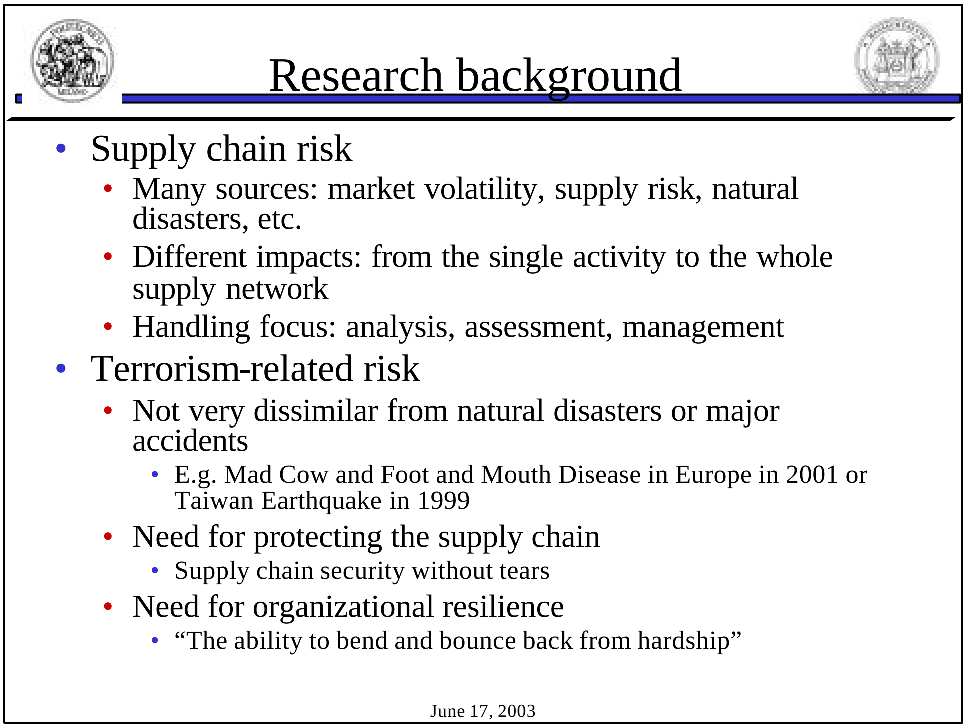
Outline

- The context of the research
- Research background
- Research goals
- Sample and methodology
- Results
- Conclusion



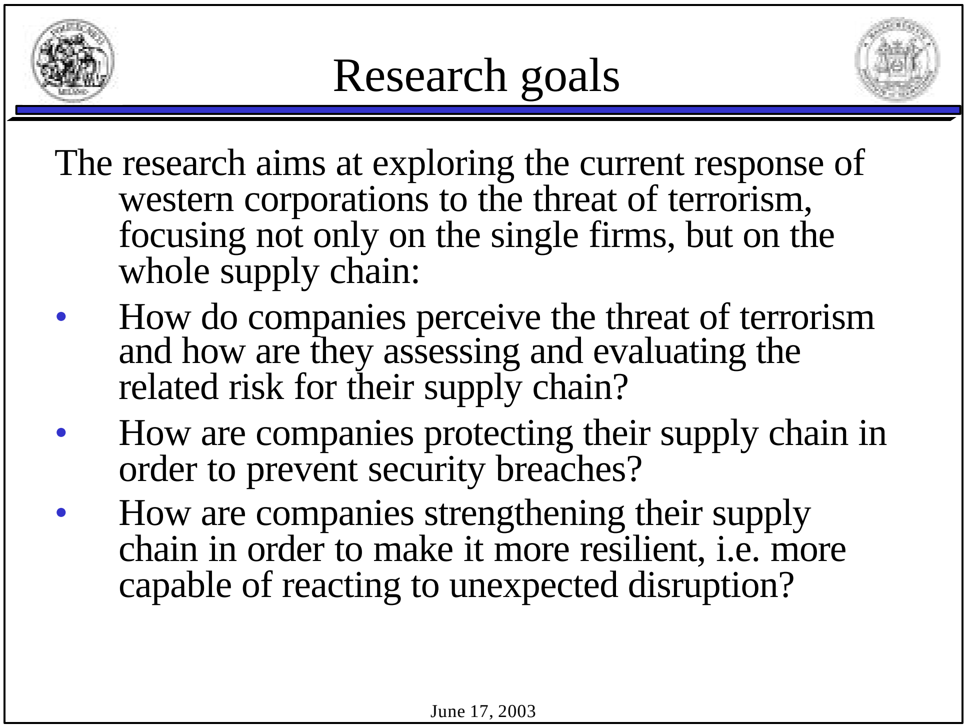
The context of the research

- After the Sept. 11, 2001 attack:
  - The grounding of the planes and the closure of the borders affected many businesses, beyond the NY and D.C. areas.
    - E.g. Ford shut down 5 plants partly due to lack of supply from Canada
  - Both short and long term effects on the supply chain are coming from the government response
    - E.g. Custom-Trade Partnership Against Terrorism (C-TPAT)
- A new research initiative to study the problem
  - Prof. Yossi Sheffi of MIT has initiated a research project to study the impact of terrorism on supply chains.
  - The project is studying the response to terrorism and their impact on commerce from three perspectives:
    - The U.S. government.
    - The risk management community and insurance industry.
    - The manufacturing, transportation and distribution corporations.
    - Learning from past low probability-high impact disasters.



Research background

- Supply chain risk
  - Many sources: market volatility, supply risk, natural disasters, etc.
  - Different impacts: from the single activity to the whole supply network
  - Handling focus: analysis, assessment, management
- Terrorism-related risk
  - Not very dissimilar from natural disasters or major accidents
    - E.g. Mad Cow and Foot and Mouth Disease in Europe in 2001 or Taiwan Earthquake in 1999
  - Need for protecting the supply chain
    - Supply chain security without tears
  - Need for organizational resilience
    - “The ability to bend and bounce back from hardship”

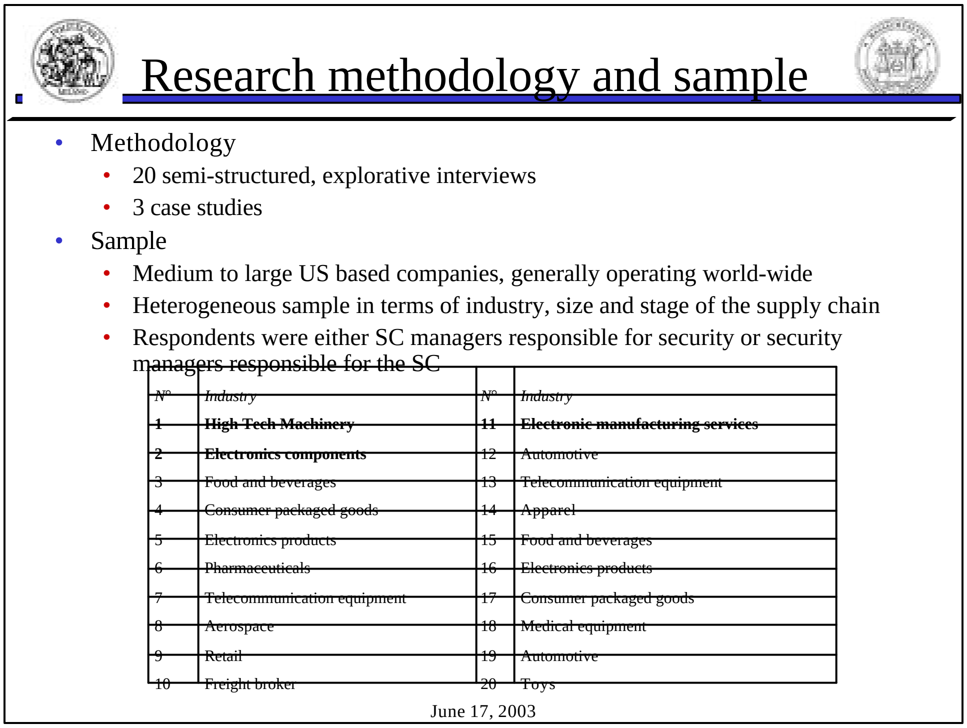


Research goals

The research aims at exploring the current response of western corporations to the threat of terrorism, focusing not only on the single firms, but on the whole supply chain:

- How do companies perceive the threat of terrorism and how are they assessing and evaluating the related risk for their supply chain?
- How are companies protecting their supply chain in order to prevent security breaches?
- How are companies strengthening their supply chain in order to make it more resilient, i.e. more capable of reacting to unexpected disruption?

June 17, 2003

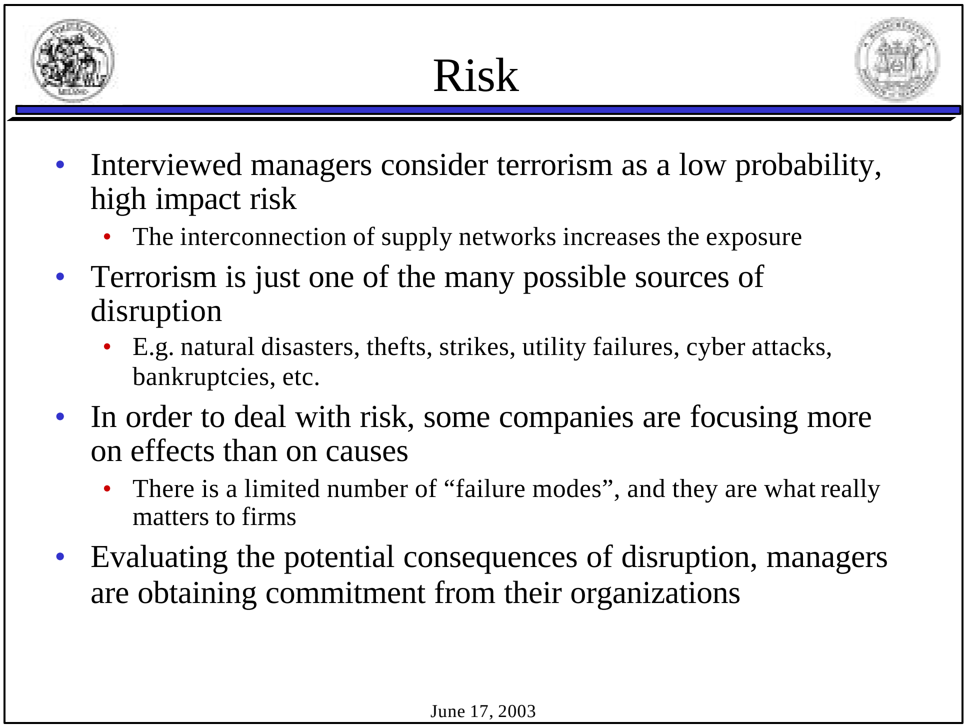


Research methodology and sample

- Methodology
  - 20 semi-structured, explorative interviews
  - 3 case studies
- Sample
  - Medium to large US based companies, generally operating world-wide
  - Heterogeneous sample in terms of industry, size and stage of the supply chain
  - Respondents were either SC managers responsible for security or security managers responsible for the SC

N°	*Industry*	*N°*	*Industry*
1	**High Tech Machinery**	**11**	**Electronic manufacturing services**
2	**Electronics components**	12	Automotive
3	Food and beverages	13	Telecommunication equipment
4	Consumer packaged goods	14	Apparel
5	Electronics products	15	Food and beverages
6	Pharmaceuticals	16	Electronics products
7	Telecommunication equipment	17	Consumer packaged goods
8	Aerospace	18	Medical equipment
9	Retail	19	Automotive
10	Freight broker	20	Toys

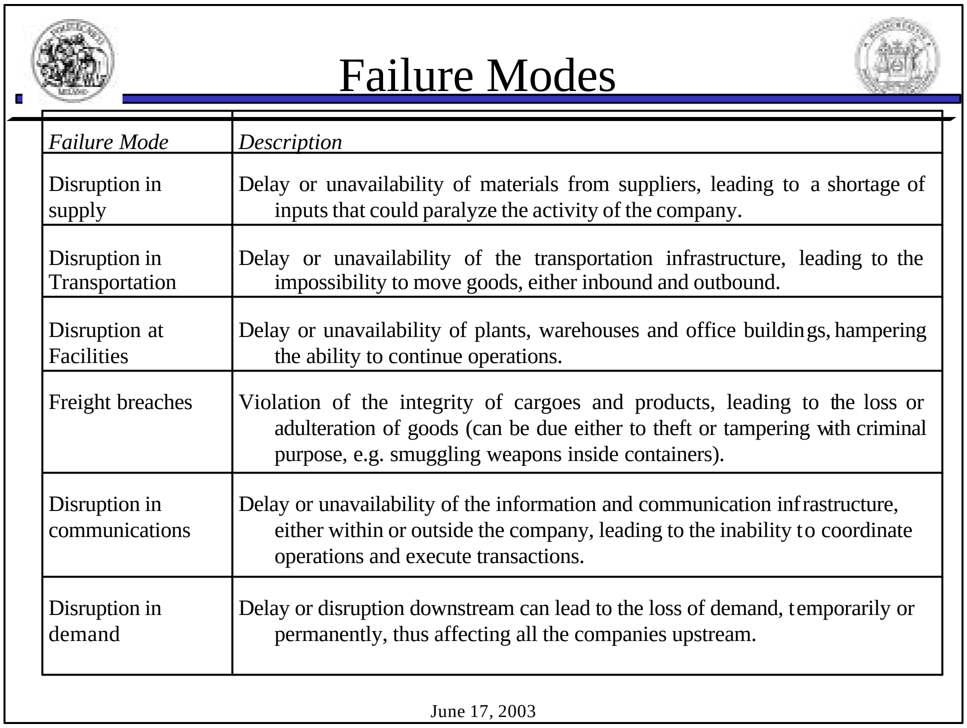
June 17, 2003



Risk

- Interviewed managers consider terrorism as a low probability, high impact risk
  - The interconnection of supply networks increases the exposure
- Terrorism is just one of the many possible sources of disruption
  - E.g. natural disasters, thefts, strikes, utility failures, cyber attacks, bankruptcies, etc.
- In order to deal with risk, some companies are focusing more on effects than on causes
  - There is a limited number of "failure modes", and they are what really matters to firms
- Evaluating the potential consequences of disruption, managers are obtaining commitment from their organizations

June 17, 2003



Failure Modes

Failure Mode	*Description*
Disruption in supply	Delay or unavailability of materials from suppliers, leading to a shortage of inputs that could paralyze the activity of the company.
Disruption in Transportation	Delay or unavailability of the transportation infrastructure, leading to the impossibility to move goods, either inbound and outbound.
Disruption at Facilities	Delay or unavailability of plants, warehouses and office buildings, hampering the ability to continue operations.
Freight breaches	Violation of the integrity of cargoes and products, leading to the loss or adulteration of goods (can be due either to theft or tampering with criminal purpose, e.g. smuggling weapons inside containers).
Disruption in communications	Delay or unavailability of the information and communication infrastructure, either within or outside the company, leading to the inability to coordinate operations and execute transactions.
Disruption in demand	Delay or disruption downstream can lead to the loss of demand, temporarily or permanently, thus affecting all the companies upstream.

June 17, 2003

Supply chain security

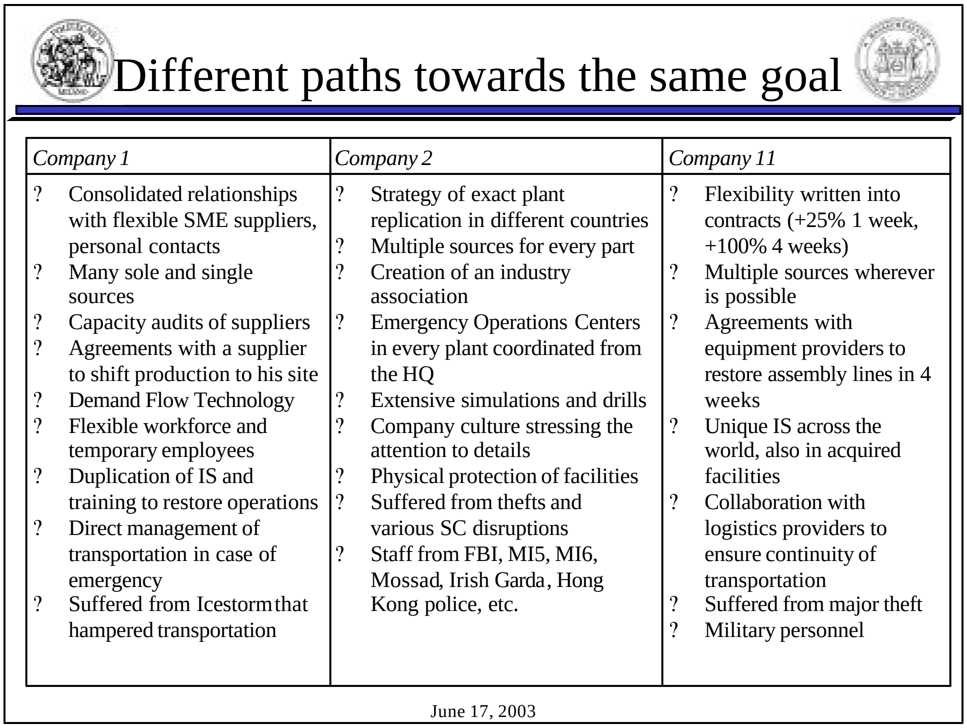
Area	*Basic Initiatives*	*Advanced Initiatives*
Physical security	? Access control, badges, etc. ? Gates, guards, camera systems, etc.	? Background checks ? Test of security by an external firm attempting to break in
Information security	? Hardware: firewalls, dedicated networks, etc. ? Software: intrusion detection, antiviruses , passwords, etc.	? Audits of partners ' IS security ? Education and training for IS security
Freight security	? Inspections ? US Government initiatives ? Cargo seals	? Procedures, audits and certification ? Industry initiatives ? GPS, RFID, e-seals, biometrics, smartcards, security sensors, etc.

June 17, 2003

Supply chain resilience

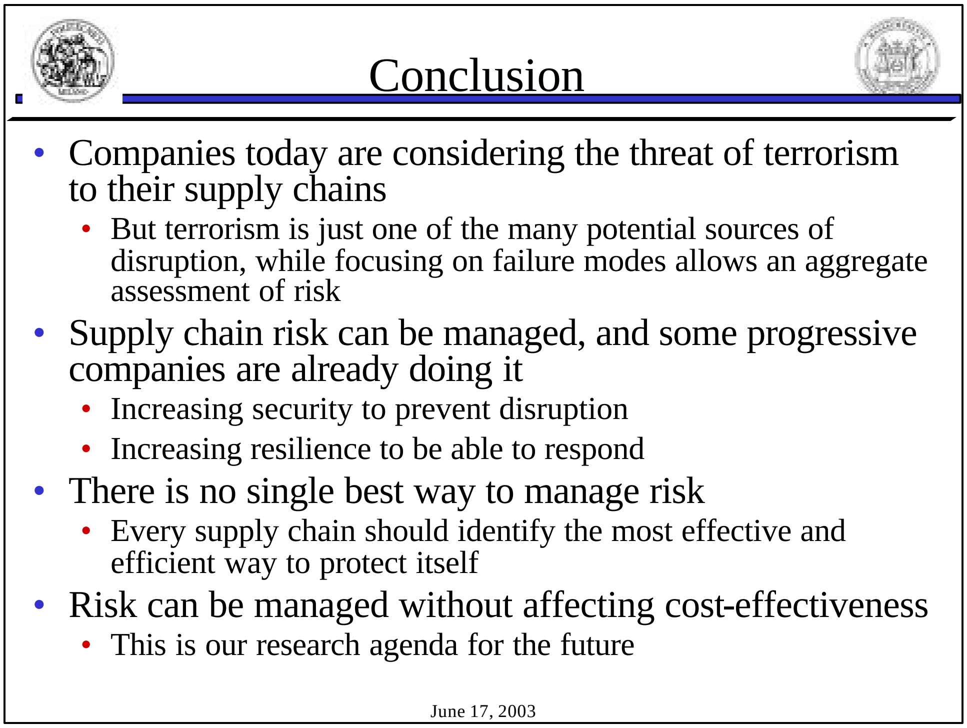
- A spontaneous attitude or something that can be developed and achieved?
  - Two areas of intervention emerged from the interviews
- Organizing for resilience
  - Contingency planning at SC level
  - Training and education: simulation, wargaming, etc.
- Supply network design
  - Complexity increases vulnerability…
  - …but networks are more resilient, because they are redundant
  - The alternative to redundancy is flexibility
  - In some industries there are mostly sole or single sources, but they are not always considered as a vulnerability

June 17, 2003



Different paths towards the same goal

Company 1	*Company 2*	*Company 11*
? Consolidated relationships with flexible SME suppliers, personal contacts ? Many sole and single sources ? Capacity audits of suppliers ? Agreements with a supplier to shift production to his site ? Demand Flow Technology ? Flexible workforce and temporary employees ? Duplication of IS and training to restore operations ? Direct management of transportation in case of emergency ? Suffered from Icestorm that hampered transportation	? Strategy of exact plant replication in different countries ? Multiple sources for every part ? Creation of an industry association ? Emergency Operations Centers in every plant coordinated from the HQ ? Extensive simulations and drills ? Company culture stressing the attention to details ? Physical protection of facilities ? Suffered from thefts and various SC disruptions ? Staff from FBI, MI5, MI6, Mossad, Irish Garda, Hong Kong police, etc.	? Flexibility written into contracts (+25% 1 week, +100% 4 weeks) ? Multiple sources wherever is possible ? Agreements with equipment providers to restore assembly lines in 4 weeks ? Unique IS across the world, also in acquired facilities ? Collaboration with logistics providers to ensure continuity of transportation ? Suffered from major theft ? Military personnel



Conclusion

- Companies today are considering the threat of terrorism to their supply chains
  - But terrorism is just one of the many potential sources of disruption, while focusing on failure modes allows an aggregate assessment of risk
- Supply chain risk can be managed, and some progressive companies are already doing it
  - Increasing security to prevent disruption
  - Increasing resilience to be able to respond
- There is no single best way to manage risk
  - Every supply chain should identify the most effective and efficient way to protect itself
- Risk can be managed without affecting cost-effectiveness
  - This is our research agenda for the future