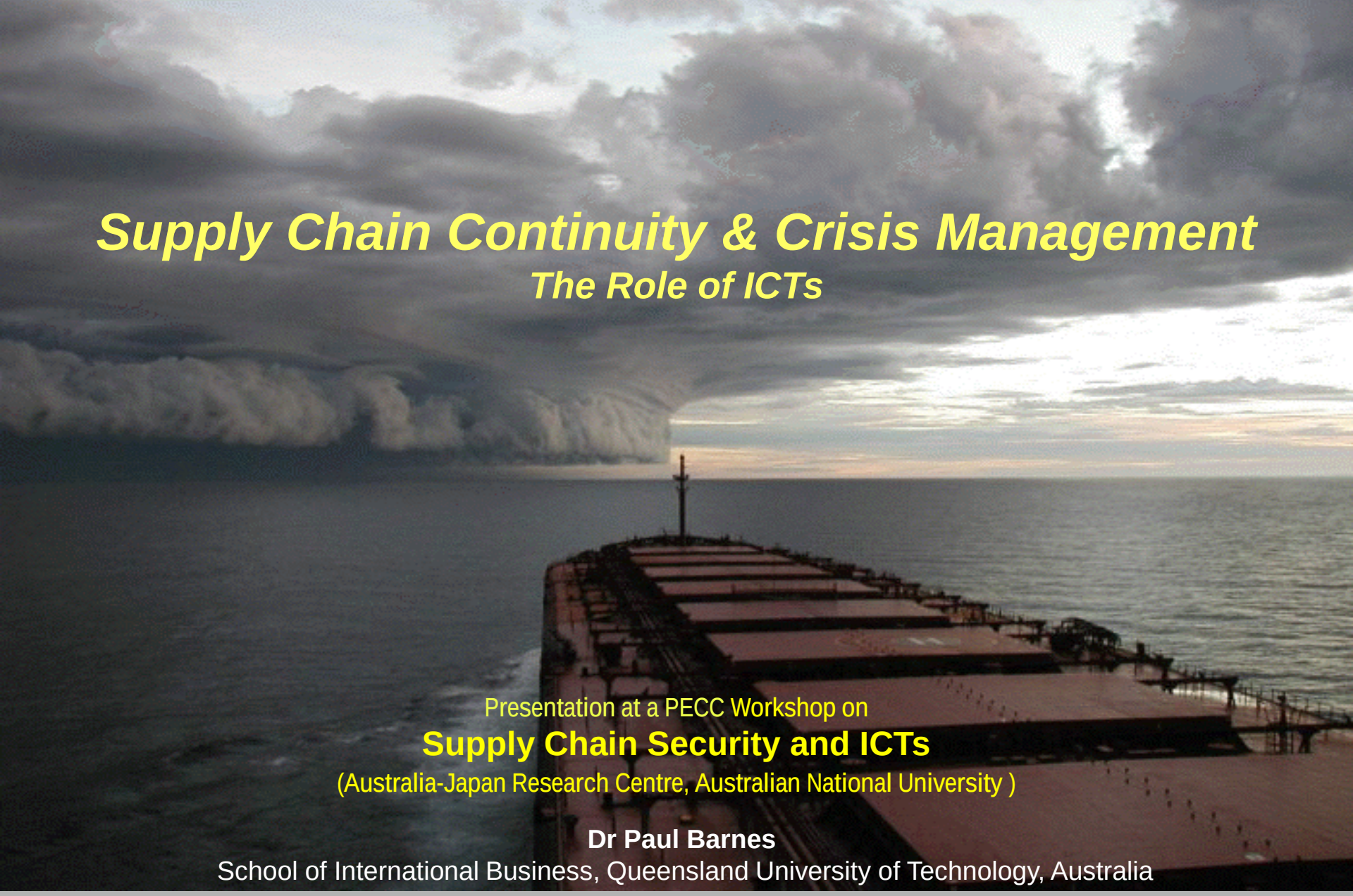


Supply Chain Continuity & Crisis Management

The Role of ICTs

Presentation at a PECC Workshop on

Supply Chain Security and ICTs

(Australia-Japan Research Centre, Australian National University)

Dr Paul Barnes

School of International Business, Queensland University of Technology, Australia

Overview of Presentation

- Aspects of Maritime Security - Old & New
- A Conceptual Framework Systemic & Organizational Vulnerability
- Options for Crisis Management & Vulnerability reduction
- Questions of Importance

- In October 2001, authorities in the southern Italian port of Gioia Tauro discovered an unusually well-equipped and neatly dressed stowaway locked inside a shipping container.
- Italian police named the stowaway as Rizik Amid Farid, 43, and said he was born in Egypt but carried a Canadian passport.

  He was found to be carrying:
  - two mobile phones,
  - a satellite phone,
  - a laptop computer,
  - several cameras, batteries,
  - airport security passes and,
  - an airline mechanic's certificate valid for four major American airports.

Maritime Security - *Issues of Complexity*

Cargo

- Using cargo to smuggle people and/or weapons.
- Using cargo to transport conventional, nuclear, chemical or biological weapons.

Vessels

- Using the vessel as a weapon
- Using the vessel to launch an attack.
- Sinking the vessel to disrupt infrastructure

External Impacts

- Loss of life and damage to property.
- Disruption to trade flows.
- Additional cost of transport due to additional security measures

People

- Attacking the ship to provoke human casualties.
- Using the cover of seafarer identities to insert terrorist operatives.

Money

- Using revenue from shipping to fund terrorist activities.
- Using ships to launder illicit funds for terrorist organisations.

Security in Maritime Trading Systems

What are the Challenges?

- Approx. 90% of world trade moves in shipping containers

  - Any reduction of throughput is likely to have a significant impact on regional and national economies.
- Global business enterprise, and trading systems in particular, are vulnerable to terrorist incidents

  - Perturbation of maritime supply chains will impact on movements of material across large sections of the network.
- The asymmetry of approach in modern terrorism can make use of systems of commerce

  - Maritime trade as a vector for terrorism.

Supply Chain Impacts – Reduced Continuity

- An industrial dispute (late 2002) impacting 29 US West Coast ports involved > 200 ships.
- A total of 300,000 containers remained unloaded and rail and other inter-modal shipments were delayed across large sections of the transport network.
- Resulting in filled warehouses, freezers and grain elevators on both sides of the Pacific Ocean, costly mid-ocean diversions of maritime traffic to other ports and businesses, laid-off workers and/or reduced production.
- Estimated loss from this disruption on Hong Kong, Malaysia and Singapore alone was estimated to be as high as 1.1 % of nominal GDP.

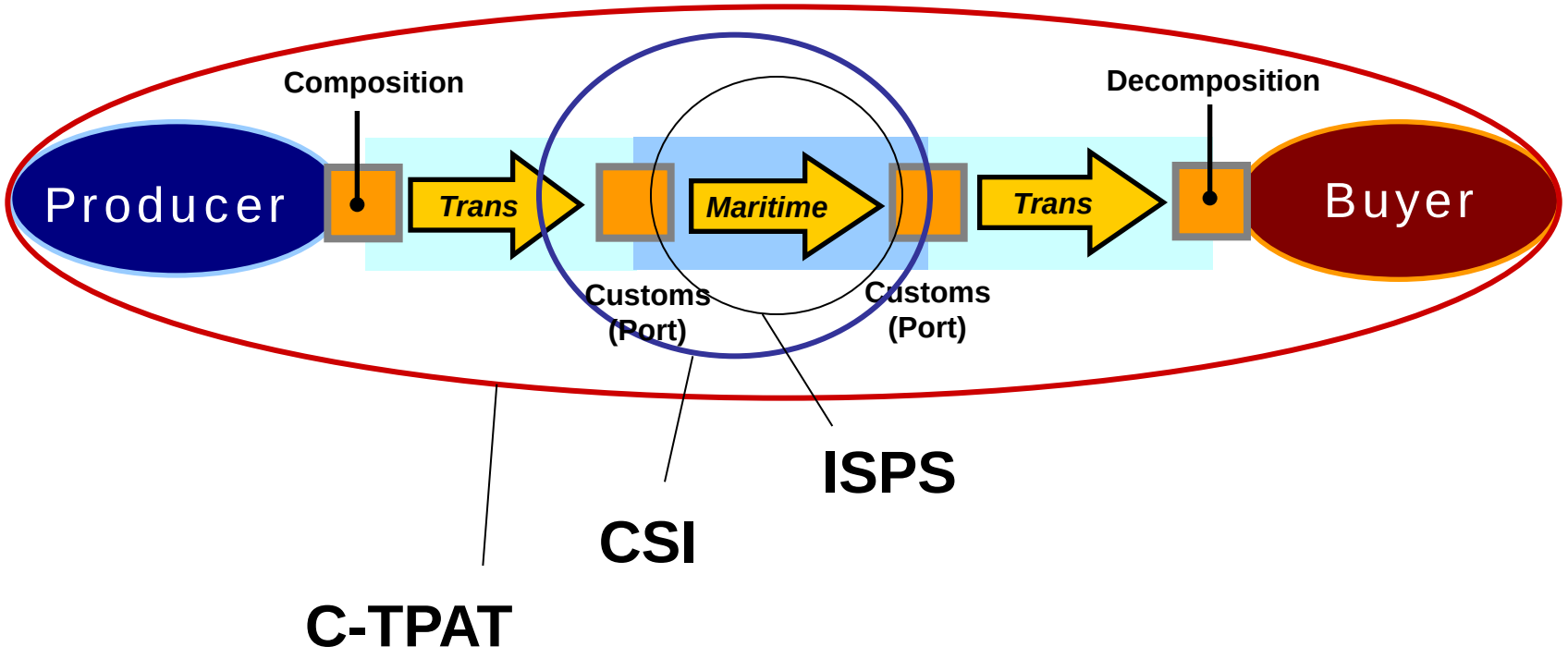
Why is Security and Crisis Management important?

- Crises have become *Normal*
- Often with a sudden emergence
- Causing major consequences

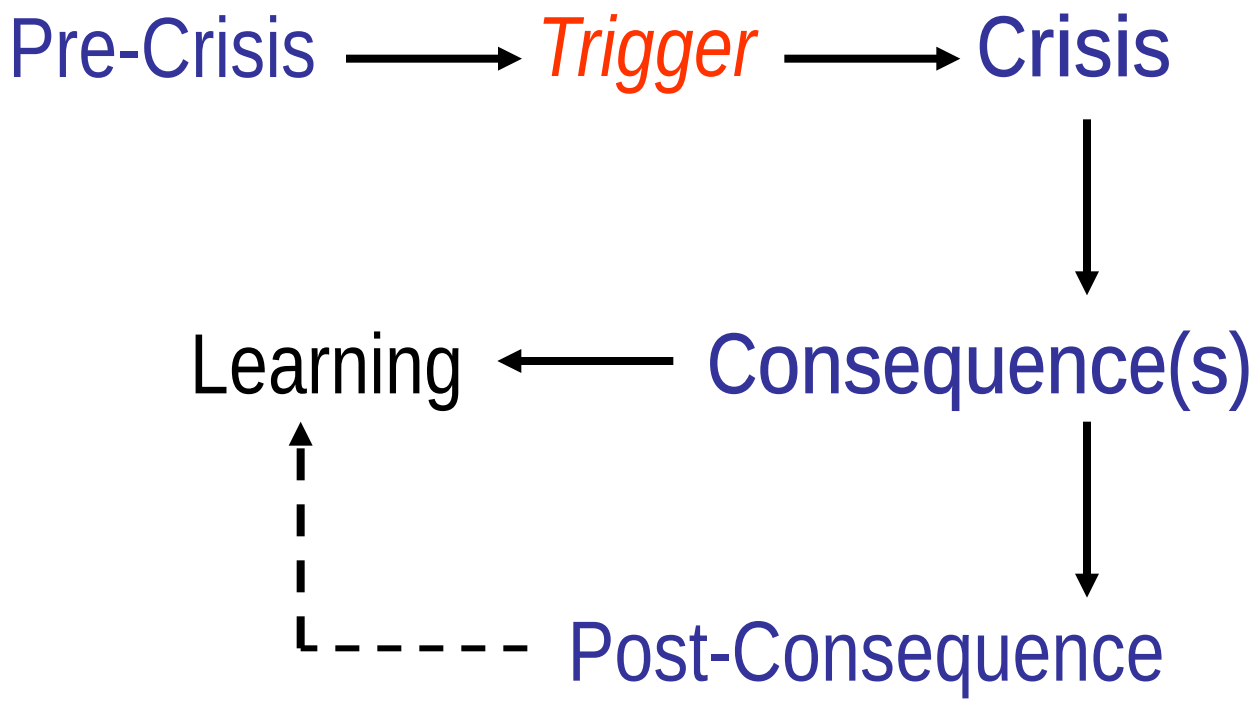
Why does it matter?

- Could the crises *or their triggers* have been attenuated?
- Could their consequences have been mitigated?
- Could they have been **anticipated** and resilience enhanced?

Security Initiatives being applied to a Supply Chain



Assumptions



Systemic *Critical Infrastructure Protection*

- Loss of interoperability & interconnectivity (data, networks)
- Interdependency of Infrastructure
- Power supply (Generation & transmission)
- Telecommunications (Soft & hard)
- Transport systems (Road, rail, air, water)

Network Complexity

- *System of Systems* (Supply Chains)

Vulnerability

*A susceptibility to change or loss as a result of existing **functional or** organisational practices and/or conditions.*

Type 1

The operational complexity within a port: encompassing the transport node infrastructure and onsite operators

Type 2

An attribute of the maritime movements themselves (with ports as nodes of the system) and global logistics management practices that underpin supply chains.

Application of the Concept

Increased complexity

Knowable uncertainty

Un-knowable

Vulnerability from:

Complex interactions between close packed system elements

Interactions at a higher level – *Systems of Systems*

Clusters of Critical Infrastructure

Complex

Vulnerable

Systemic & Organisational Vulnerability

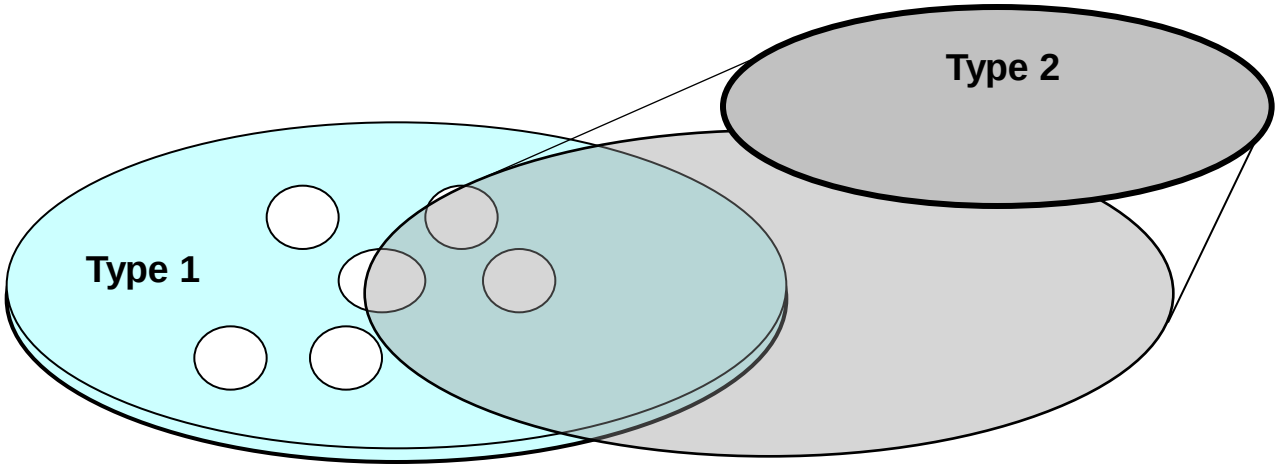
Decision making in Crises (Assumptions)

They will be impacted by the presence of:

- Uncertainty / Ignorance
- High Decision Stakes
- Extreme Systems Complexity

A conceptual Frame

Type 1 and *Type 2* Vulnerability



The December 2004 WCO endorsed *Draft Framework of Standards to Secure and facilitate Global Trade* emphasises four principles:

- Harmonized advanced electronic manifest information on cross-border shipments
- A risk-management approach to inspections
- The application of modern technology, *and*
- Customs privileges for businesses that meet minimal supply-chain security standards

Questions – Before uncontrolled expectations about ICTs emerge.1

- What is the priority?
  - Enhanced Continuity of Supply or Security?
  - Can both be delivered?
- Have within-port vulnerabilities been mapped?
  - (eg: interactive complexity of critical infrastructure)
- Is the nature and organisation of current security risk management functions and governance systems within a port compatible with known threats and has the *flexibility to respond to emergent threats or merely compliant with legislative requirements or mandated treaties?*
- Do ports have an adequate depth of trained risk and crisis management staff?

Questions – Before uncontrolled expectations about ICTs emerge.2

- If embedded ICTs did identify problems during a maritime leg or during an up-load or off-load what would Port Authorities or Shipping companies do?
  - Proliferation Security Initiative?
  - How would false positives / false negatives be treated?
- Once embedded ICTs were a mainstay in a supply chain how would system-wide security integrity be maintained – how would *resilience* be sustained?
- Assuming there are expectations/requirements to share commercial-in-confidence information what requirements might be sought by industry participants in respect to data protection?

Maritime Borders have become Security Borders

The Information Economy may have become a Security Economy

The interplay between the new Borders and this equally new form of Economy requires careful and deliberate attention

Thank You