'Combating border protectionism?: ICTs and security assurance in open economies'

Dr Christopher Pokarier

Waseda University, Tokyo

pokarier@waseda.jp

Notes of a presentation given to the PECC-ANU workshop on
'Global Supply Chain Security and ICTs', Aichi Expo, 23 June 2005.

The issue

Question: Can the application of information and communications technologies (ICTs) provide enhanced security assurance without compromising (or ideally, enhancing) the goals of open and integrated economies?

Specifically, can ICT applications allow for more selective interventions by the state in cross-border movements?

And, by implication, might border protection strategies featuring ICT applications help to attenuate the risk of 'border protectionism'; namely disproportionate, misguided, or private-interest motivated interventions in cross-border movements.

Targetted Border Protection

Targetted interventions in cross-border movements for security purposes:

- Provide direct incentives for secure conduct by addressing problems closer to source (eg. by enhancing surveillance of, or restrictions on, a source rather than all from an entire country-of-origin)
- Minimize disruption to valuable cross-border flows
- Bring greater certainty to the international business environment – reducing transaction costs & increasing incentives for welfare-enhancing cross border economic activities

<u>The contemporary border protection quandary</u>

Borders define nations as territorial and institutional entities and are governed by states.

Cross-border movements are overwhelmingly by private actors and occur through private institutions and contracts.

Societies have increasingly recognized the welfare-enhancing role of cross-border movements of goods, services, people, finance and information.

In this context, state actors charged with border protection increasingly co-opt and pattern those private actors who facilitate cross-border movements.

Such private actors are often caught between client demands and expectations (often grounded in industry or community standards – eg. re: privacy) and enforcement officials

<u>Terminology</u>
'Combating border protectionism?: ICTs and security assurance in open economies'

border protectionism?

Recent concern with <u>border protection</u>. Many concerns are legitimate but there is also the risk that of old phenomena in new guise:
- protectionism & broader economic nationalism – motivated by private economic interests or illiberal perceptions of the public interest
- statism & bureaucratism

Security assurance –

<u>Security:</u> protection against threats to the bodily integrity and welfare (material and emotional) of people in a defined space from acts of violence, diverse biohazards, and severe environmental degradation

<u>Assurance:</u> "The basis for trusting that a system implements security policies as intended" (CDE)

Assurance entails a perceptual component (which implies too the risk of false assurance)

Open economies – openness to significant cross-border flows of goods, services, people, finance and information

There is no a priori assumption that the state is the sole or even principal source of security assurance

<u>Imperatives</u>

- Growing recognition of the importance of efficient international supply chains to the competitiveness of firms, economies, and economic welfare
- Recent events – 9/11 & other terrorism, SARS, Avian flu, BSE, tsunami, rising biodiversity concerns, human environment concerns
- Need to guard and further advance the gains from economic integration of nations
- APEC/PECC level – direct experience of all recent negative events but also a growing policy community with established dialogues and agendas on key related issues

<u>Interface of APEC/PECC agendas</u>

Trade liberalization

Trade facilitation through best practice logistics, paperless trading etc

Counter-terrorism

Capacity-building in pubic economic governance & corporate governance

E-governance

Crisis readiness and response – post SARS, tsunami etc

Recent commentary & research

- Secure trade serving SCM and trade facilitation objectives – eg. APEC & PECC work (ongoing need to guard the distinction between corporate efficiency issues & state-derived artificial barriers to trade)
- Principles for secure trade – OECD, UNCTAD
- Maritime and port security issues
- Diverse US-based projects on homeland security & US international competitiveness (CIBERs - Centers for International Business Education and Research
- RFID devices & other ICT applications: promise and technical problems
- Privacy & individual protection issues with RFID devices, US screening & profiling

A few (slightly obtuse) conceptual matters

Conceptualizing states in markets
Determinants of state intervention in market transactions:
- Interests
- Institutions
- Ideas

Academic recognition that 'ideas' about national and societal interests can mask private interests and legitimate suboptimal institutions has been expanded to application of cognitive science to understanding dynamic economic systems (Douglass North, 2005).

Growth, cognition and uncertainty

North (2005): Sustainable economic growth has involved ever greater control of humans' environment; with a consequent reduction in uncertainty

Dynamic economic systems allow for effective cognitive adjustments to changed realities; and in turn adjustments in business and broader societal systems

9/11, SARS, Avian Flu etc – have changed perceptions of the international business environment held by both market and non-actors in significant ways <u>– the world truly has changed</u>

<u>Turning uncertainty into risk</u>

Uncertainty vs Risk – unknown versus known probabilities

Known probabilities allow:
- pricing through insurance and other markets for financial risk and hence effective re-assignment of risk
- private & public actors to make cost-benefit analyses of what risks should..
- be re-assigned or borne directly
- avoided altogether through desisting from certain courses of action
- or attenuated through investments in risk reducing practices, technologies, systems and infrastructures.

Open question: To what extent ICT applications to supply chain security help to turn uncertainty into (manageable) risk?

<u>The ubiquitous security system vision</u>

Modern ICTs present promising visions of seamless
- Integration
- Interoperability
- Coordination

Between state agencies, private organizations and citizens – within and across borders – that provide high levels of security assurance…
- Discretely
- Justly
- at low cost…..

While this alluring vision of ubiquitous ICT-based security assurance provides impetus

to the creative and entrepreneurial pursuit of new applications it also presents dangers

Existing and emergent systems

- Existing systems – such as maritime shipping – have, over a long period, evolved in response to commercial pressures for certain types of assurance
- Legacy systems are deeply embedded in existing industry, human resource and social systems and can rarely be subjected to 'scrap and build' solutions
- The `social embeddedness' of business systems is a significant factor in their resilience and responsiveness or otherwise
- ICTs provide data pipes & mines – human systems turn data into useful knowledge –
- which is usually decentralized, deeply localized, not fully knowable by state actors and sometimes downplayed by aspiring IT systems vendors

Security in diversity?

Dangers arise from excessive concern with:
- centralization, coordination and standardization
- hierarchies of leadership in response to critical incidents

Reasons:
- Wisdom of crowds – the many will be collectively wiser than the few
- Decentralization for systems resilience
- Voluntary communities of good practice have proven to be efficient disseminators of best practices & sources of creative collaboration
- Tournaments also effectively foster innovative good practice and speed its dissemination

The collective voluntary responses of research institutes to SARS produced extraordinarily effective scientific responses to the disease, speeding management of the threat.

Some specific issues

Securing an 'open and mobile society' (OECD, 2003) – key cross-border movements:
- Goods
- Services
- People
- Finance
- Information

Goods

- ICT applications have been making significant contributions to enhanced supply chain management
- Hopes for ICTs in simultaneously enhancing supply chain efficiency and security assurance have centered on cross-border flows of goods
- This also reflects the growing recognition that maritime shipping and air cargo services may provide vectors for cross-border terrorism
- Also heightened cognition of potential biohazard risks to communities and threats to environments through cross-border trade in goods

US Maritime trade security initiatives

The now-familiar:
- ISPS
- CSI
- C-TPAT
- Smart and Secure Trade (SST) Lanes Initiative

The May 2005 US Congressional review of maritime trade security program signaled ongoing concerns about the limited scope and efficacy of these programs; suggesting a more stringent (and better financed) border protection regime.

Who participates; who pay?

- Fear of costly delays upon arrival have encouraged shippers and carriers to comply with C-TPAT – fears encouraged by Dept of Homeland Security
- CSI and C-TPAT explicitly justified by US officials in terms of externalizing costs of US security
- Though costly need to place US officials abroad has led to the US identifying criteria for new participants in CSI and CT-PAT
- Significant distributional issues – amongst ports, shippers and carriers – may impact on shipping patterns, with implications for trade and investment flows
- Carriers may face financial vulnerability disproportionate to their actual control in the maritime shipping supply chain

Tracking

- Tracking of maritime shipping has a strong security imperative – hence ISPS – with security and safety benefits for carriers
- Constant cargo tracking through GPS and other applications – now popular and evocative imagery –
- but commercial demand in container market is often overstated
- existing systems generally provide sufficient cargo tracing – container and contents loss, for instance, is apparently not a major issue for shipping firms (as risk is managed through insurance

Traceability and sensors

End-to-end traceability and monitoring is in stronger commercial demand, reflecting:
- consumer concerns about food products in response to heightened risk perceptions, owing to BSE, avian flu, chemical residue concerns etc
- may attenuate risk of commercial disputes over spoilage
- may support efficient inventory management
- assurance factor can be a point of product/supplier/place-of-origin differentiation
- some potential to attenuate the extreme vulnerability of all producers from a country-of-origin to a disproportionate regulatory response to a detected hazard which closes the market

RFID (radio frequency ID) applications

- Diverse technologies, applications
- Expanded Universal Product Code (UPC), electronic product code (EPC) systems
- Passive, active, semi-passive (all of varying data volumes capacity, security) – diverse types for diverse applications but some standards needed if broader security assurance is a major objective
- Standards issues – ISO and EPC-Global etc are setting standard, plus major commercial users like Walmart
- Technology can allow multiple standard readers
- RFIDS are not a trade security 'silver bullet' – the judgment of a recent State Department workshop

RFID – new vulnerabilities

- RFID killers – a large magnetic pulse (or in the microwave oven!)
- RFID manipulators – eg. RFDump software or RFID Washer
- Hacking – any compact data storage device – phishing
- Non-encryption RFID allows (too) ready identification of contents
- central databases can be more secure – but with reliability of access issues
- encrypted semi-passive or active, dual storage and central database oriented, RFID applications have promise for high value-added shipments

RFID technology and consumer concerns

- Embedded RFID devices not deactivated after sale (sometimes to benefit of consumer – warranty, service, recovery after loss or theft) but allows items to be identified
- Major privacy issue in the USA – championed by American Civil Liberties Union and other NGOs and activist groups
- California has just banned RFID applications in all state documents

<u>What to do with the data? (If you can read it)</u>

- Strong corporate interest in, and provision of, integrated B2B ICT-based SCM solutions
- Border protection requires effective B2G, G2G and cross-border G2G interfaces
- Business-government data sharing protocols must be made specific to protect firms, clients and state actors
- Better and more timely trade data may serve public economic management and business analysis
- Government promotion of paperless trading may bring significant benefits to exporters and enhanced cooperation with other ICT-based secure trade initiatives

<u>e-Documentation</u>

Paperless trading is still far from ubiquitous, despite the vision of the APEC Paperless Trading Roadmap. (eg. only about 1/3rd of B/Ls submitted to carriers in Japan are in e-form: meaning manual data entry to meet US 24-hour manifest rule)

Australia and collaboration with trading partners provides a promising example:

- EXDOC – early B2G initiative for agricultural commodities, linking AQIS & Customs to provide EPN (Exporter Permit Number) and ECN (Export Clearance Number)

- SANCRT – dedicated EDI-based G2G system, since 1998, providing paperless export certificates (certifying all import and other regulatory requirements of the target market have been met – eg. A-J beef trade)

- E-cert – Internet-based G2G replacing SANCRT – scaled-up from NZ model, with expanding bilateral trials and implementation with a number of APEC and Non-APEC members – much still to be done to achieve widespread take-up by exporters, importers and their governments.

<u>Cross-border movements: Services</u>

- Attention so far largely to cross-border transport services that provide a potential vector for both terrorism and biohazards
- 9/11 provoked an understandable US focus on airline security, while impacting severely on the financial capacity of the industry to bear the costs of new security assurance measures
- Maritime shipping industry, by contrast, has been in a period of cyclical high profitability so has found compliance with ISPS etc easier
- Airlines – advance manifest requirements for US – recent flight diversions cancellations through mis-identification and denial of entry into US airspace
- Cross-border service provision very often involves movement of people…

Cross-border movements: People

Cross-border movements of people:
- support and promote international supply chains
- share knowledge-based resources
- are critical to the international supply and consumption of services
- and are important to enhanced cooperative public governance between jurisdictions

ICTs and immigration controls

- Smart biometric passports – International Civil Aviation Organization (ICIO) has called for their full implementation by 2015 (US 'policy laundering'?)
- ICIO guidelines are minimal, leaving discretion to issuing country as to how much extra data capacity and content may be stored
- ill-conceived US proposal to embed unencrypted transponders in US passports has been withdrawn
- Delayed US requirement beyond October 2005 for other countries to introduce compatible passports
- Concerns expressed about detectable presence of passport – making bearers more vulnerable to crime abroad
- Ongoing debate about the extent to which writable functionality on smart chips

should be taken advantage of (eg. e-visa straight to chip, arrival and departure records)

Japanese case

- fingerprinting and facial biometrics upon arrival requirement will be introduced
- promise of streamlining for residents of Japan through a new smart card version of the alien registration card, containing fingerprint and facial biometrics
- efficiencies for legal foreign residents if databases are effectively interfaced
- eg. re-issue & even re-entry difficulties diminished if passport & visa or registration card are lost
- Effective e-governance initiatives could also make visa renewals, alien registration etc far more efficient
- e-documentation – confirmation of employment document submitted on-line?
- Will test determination of Japan and other governments on whether it is simple enhanced border protectionism is a shared commitment to 'rule-based internationalization' (ルールを守る国際化)

Security & e-migration controls

- more effective enforcement of immigration regime
- but security against terrorism and other crimes will remain entirely dependent on information exchange with other national and international agencies – significant problems with the US Secure Flight program, for instance.
- more extensive common travel document? – criminal record certificate etc?
- biohazard risk management? – WHO health card data stored on passport?
- Anti-crime measures – the Mexican Attorney General and 160 anti-crime officials were recently subdermally e-tagged to discourage their kidnapping

Finance

- Long experience of state agencies co-opting private enterprises to help regulate cross-border flows

- Recent anti-money laundering initiatives take this further
- Does this experience provide a positive or negative experience for state-private sector partnerships for monitoring and policing cross-border financial flows?
- Financial services providers are distinctively and extensively regulated and monitored – as are passenger air services but less so is maritime shipping

Information

- Recent initiatives across cyber-crime
- Long-established interception practices for national intelligence purposes (eg. Echelon – intelligence partnership between Anglo-American countries)
- Modern ICTs massively increase the volume of cross-border communications while also increasing the capacity for automated interception
- Post 9/11 – significant new state investments in interception

Corporate realities

Virtue is its own reward?
Depends! On…
- role in the supply chain
- the type of application and,
- the type of risk it might attenuate

One must be wary of blithely asserting that ICT applications for trade security 'make good business sense anyway'.

Commercial barriers to adopting security-enhancing ICT applications

- coordination problems - those who bear the implementation & compliance costs might not capture the financial benefits of greater assurance
- eg. owing to insurance practices – be in FOB or insurance policy treatment of port delay costs
- complexity of logistics, maritime shipping industries – little vertical integration

- reflects key features of demand for, and supply of, maritime shipping services
- Carriers are most exposed to border enforcement regimes – but have little direct control over the clients they provide services to (if manifest is in order and container is sealed then it goes onboard)
- adoption of e-applications will vary based on the structure of export industries – eg. many SMEs shipping through fragmented small-scale shippers

Issues for firms in adopting security-enhancing ICTs

- Fear of 'border protectionism' may make costly applications 'rationale'

- Many larger firms favor mandatory not voluntary changes
- Shipping industries have strongly cyclical profitability
- Established exporters have trusted legacy systems
- Some large firms have had bad past experiences with customized IT applications – delays, commercial hold-up by systems providers leading to budget over-runs

Private providers of ICT-based trade security solutions

Corporate actors will play important roles in:
- Hardware provision
- Systems applications
- Capacity-building – through consulting, training etc

Yet… the security assurance industry may encourage 'border protectionism'

- Public sector enterprises have had mixed experiences with ICT solutions providers
- The design, implementation and costing of security-oriented systems may be more difficult to submit to expert and public scrutiny
- Risk of insufficiently accountable 'securocrats' making policy with insufficient understanding of the critical private systems on which they impact

Moving borders to secure them?

In a practical enforcement sense and sometimes legal sense, national borders may shift in the pursuit of border protection ends
- CSI and C-TPAT is a forward defense approach placing enforcement officers in foreign ports
- Australia's recent changes to the migration act excised parts of Australian territory for the purposes of claiming refugee status – retreating borders
- Embedding enforcement in the operational practices of private border-spanning organizations (such as financial institutions) entails a form of 'virtual borders'
- Cross-border agency cooperation may, it is frequently alleged, free enforcement agents from some of the legal and policy constraints upon conducting operations directly

Ubiquitous ICT-based security solutions?

- Total systems solutions may create new systemic vulnerabilities
- ICT systems are only as good as the information within them
- Risks to firms and individuals from profiling and data matching errors, or no data being equated to higher risk, must be taken seriously
- Systems legitimacy will be essential to its effectiveness & sustainability
- Significant danger of <u>misplaced assurance</u> – with all actors in cross-border supply chains being less vigilant against threats owing to better ICT-based systems

Security architectures: Technological, institutional and human
- Mobile factors of production moving across multiple production locations makes for significant systems complexity
- Better information in itself can provide significant security assurance (in a cognitive sense), reducing uncertainty & promoting economic confidence
- Legitimate community concerns about terrorism, biohazards and severe environmental degradation must be taken seriously
- While a new 'border protectionism' – old-fashioned economic nationalism with the added spices of homeland security, fear of the plague and no-risk environmentalism