IRISH EXPORTERS ASSOCIATION
TRADE FACILITATION 2003

Jack Short
Secretary General
ECMT

Improving Transport Security and Efficiency;
Contradiction or Opportunity?

Dublin, Ireland
21 March 2003

The views expressed in this paper are those of the author and do not represent the views of ECMT or those of its Member Countries
Introduction

This paper focuses on the impacts and actions in the transport sector since the terrorist attacks of September 11 2001. As background, it first assesses the economic and trade consequences of the attacks. The actions taken in the sector are then summarised. The recent initiatives are discussed and the challenges for the transport and trading system are set out.

Economic Impacts

The terrorist attacks on the U.S World Trade Centre and the Pentagon resulted directly in the destruction of physical assets estimated at $14 billion for private businesses, $1.5 billion for state and local Government and $0.7 billion for the Federal Government. Cleanup and rescue costs have been estimated at $11 billion. The attacks occurred at a time when business growth was slowing and they further dented waning confidence. Economic forecasts were quickly revised downwards by an additional 0.5 percentage points. Specific sectors like airlines were particularly hit. The insurance sector faced an unprecedented catastrophe, with losses estimated to be somewhere between $30 and $60 billion. The tourism sector saw a sharp drop in demand1.

In response to the crisis, the US Federal Reserve injected massive amounts of liquidity into the system. Interest rates tumbled to as low as 1.2% on 19 September. Monetary policy was eased aggressively with Central Banks around the world lowering interest rates substantially. The fiscal response was rapid too and an emergency-spending package of some $40 billion was approved. In the US, $5 billion in direct grants and $10 billion in loans were given to the airlines. Stricter limits applied in Europe, and Sabena and Swissair went bankrupt.

Overall, the short term adverse effect was less than feared initially. In the US, the agencies acted rapidly to restore confidence, inject liquidity and safeguard the financial system.

Although the efficient and rapid response mitigated the short-term impact, the medium term implications should not be underestimated. It is certain that some impacts will be long lasting. For example, insurance coverage for terrorism related activities is now more difficult to obtain and premiums have increased by up to 30% on some facilities. Security, especially for entering the United States has been and will continue to be tightened. Thirdly, public spending on security and military operations is likely to grow again.

1. OECD: Economic Papers
Trade Impacts

World trade grew 10% in 2000 and only 1 or 2% in 2001. So international trade has slowed but it is not possible to disentangle the effects of terrorism from the more general economic slowdown that had already begun.

The costs of trading have obviously increased because of the additional security requirements and additional risks associated with trade. But there is great uncertainty, both on the size of these extra costs and on their likely impacts on trade. Administrative costs of trade, including customs are estimated to cost 2-7% of the value of trade. Transport costs vary from about 1% of the value for goods like pharmaceuticals up to over 20% for fertilisers. Obviously, higher transport and trading costs will reduce exports and imports. Studies show that trade is highly sensitive to the costs of trading. Some econometric studies estimate that each 1% increase in trading costs can reduce trade itself by between 2 and 3 percent. This is surprisingly large and would be a maximum. But it does illustrate the potential risk 2.

Transport Impacts

Following the September 2001 attacks, there were major short-term disruptions in the transport sector, with US air space closed for four days and ports for two. Border crossings were closed along the border with Canada, where half a million vehicles cross daily, leading to particularly severe logjams. Some companies, for example in the automotive industry, dependent on just-in-time deliveries, saw a complete breakdown in their supply chains. New security measures were introduced initially for aviation but rapidly extended to other modes.

The terrorist attacks of September 2001 in New York and Washington modified probably forever the way security is approached in the transport sector. The use of transport vehicles as actual weapons of destruction targeting both passengers in the vehicles and individuals located in the target buildings exposed a whole new degree of vulnerability within the transport system. As a result of the magnitude of physical destruction and loss of life, transport authorities and service providers on all levels and in all sectors have had to adjust traditional security assessment procedures and tools to manage and effectively respond to this new level of risk.

Well before these terrorist strikes on the United States, transport infrastructure and equipment has been the target of terrorist action for a number of reasons, among them, it is:

2. OECD: Trade Directorate
Relatively accessible;
- Can attract significant public attention and media coverage;
- Is often linked with national symbols such as national airlines;
- Can affect large numbers of people in a single strike.

Transport sector experience since the events of late 2001 has revealed a number of areas of uncertainty with regard to ensuring security against terrorism attacks in transport. Transport authorities and operators have since September 11 found themselves seeking answers to a number of security-related questions, among them:

- Are existing security measures and procedures sufficient in the current post-September 11 context? Where are the remaining vulnerabilities in the system and how best can they be addressed? Is it just a question of better implementation/greater enforcement of existing procedures or are new measures needed?

- Are the current evaluation tools, including risk and vulnerability assessment methodologies, sufficient to provide the necessary information to decision-makers given the magnitude and potential impact of the terrorist threat, particularly with perceptions of heightened insecurity in certain areas since the attacks? What are the costs of using these tools, and who should cover these costs? What are acceptable levels of risk?

- Similarly, how much security is « enough »? That is to say, where is it necessary to draw the line in tightening security so as to avoid unnecessarily increasing transport costs without adding benefits, and thereby constraining transport activity which is essential to national economic health?

In seeking to come to grips with these and other questions, transport entities have been meeting on local, regional and national levels of government and within some sectors on a multilateral basis to take stock of security considerations relative to counter-terrorism, share best practice, and evaluate necessary technical, legal and legislative adjustments to ensure maximum protection based on evaluated risk against terrorist activity in transport. Transport authorities support the objectives to facilitate trade and frequently work with shipping and industry representatives to put the case for smoother flows of goods and information. They therefore have been in the forefront of those asking for measures that are proportional, based on proper assessment of risk and do not engender costs without benefits.

The following section summarises some of the responses from the transport sector, actors and authorities.
Transport Sector Responses

Aviation

National responses

In the hours immediately following the attacks, access to airports and aircraft around the world was tightened -- US airports were closed for three days to evaluate security measures and take immediate precautions to increase scrutiny of passengers and baggage. Enhanced security measures, including improved passenger screening and intensified baggage processing, were taken around the world following the attacks:

On the freight side, there was a similar intensification of security precautions, including the use of x-ray machines to screen cargo and verify contents of freight shipments. Further measures included required earlier deadlines for dropping off cargo shipments at airports, bans on shipments from unknown customers, and waiting periods before cargo is loaded onto planes.

International responses

International co-ordination on improved aviation security was rapidly strengthened. The International Civil Aviation Organization (ICAO) convened a high-level Ministerial Conference on Aviation Security in Montreal 19-20 February 2002. Ministers from 154 States and 24 international organisations agreed in Montreal a global strategy for strengthening aviation security world-wide, and issued a public Declaration endorsing the establishment of a comprehensive Aviation Security Plan of Action, subsequently approved by the Council of ICAO at the fourteenth meeting of its 166th Session, on 14 June 2002.

Key elements of the Plan of Action\(^3\) include:

- Identification, analysis and development of an effective global response to new and emerging threats, integrating timely measures to be taken in specific fields including airports, aircraft and air traffic control systems;
- Strengthening of the security-related provisions in the Annexes to the Convention on International Civil Aviation, using expedited procedures where warranted and subject to overall safety considerations, notably to provide for protection of the flight deck;
- Close co-ordination and coherence with audit programmes at the regional and sub-regional levels;
- Processing of the results by ICAO in a way which reconciles confidentiality and transparency;

---

Follow-up programme for assistance, with rectification of identified deficiencies.

The European Civil Aviation Conference (ECAC), comprised of 38 Member states, has had ongoing work on air security against terrorism for nearly three decades. Since the 11 September attacks, ECAC has held a series of task force meetings that have produced recommendations on improved aviation security measures.

The European Union, which prior to 11 September had not introduced any air security legislation, has based its aviation security legislation on the ECAC aviation security or AVSEC measures. The European Parliament and the Council have adopted a regulation in December 2002 establishing common rules in the field of civil aviation security.

Maritime

The maritime sector is the second transport domain in which a concentration of efforts to enhance the security framework has taken place since September 11.

International and national bodies have been active in examining existing laws and conventions within the IMO, OECD, WCO and other bodies.

International responses

In the wake of the attacks, the United Nations International Maritime Organisation (IMO), which has primary responsibility for multilateral agreements on international maritime rules and issues, undertook a reassessment of the state of international maritime security regulations. The IMO Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, held from 9 to 13 December 2002, adopted a number of amendments to the 1974 Safety of Life at Sea Convention (SOLAS), the most far-reaching of which enshrines the new International Ship and Port Facility Security Code (ISPS Code). The Code contains detailed security-related requirements for Governments, port authorities and shipping companies in a mandatory section (Part A), together with a series of guidelines about how to meet these requirements in a second, non-mandatory section (Part B). The Conference also adopted a series of resolutions designed to add weight to the amendments, encourage the application of the measures to ships and port facilities not covered by the Code and pave the way for future work on the subject. The mandatory measures are:

- Early implementation for the fitting of Automatic Identification Systems for all ships of 500 gross tonnage and above on international trips;
- The mandatory development of ship security plans for all ships engaged in international trips;
− The required designation of a ship security officer, responsible for crew training, implementation of the ship security plan and co-ordination with port security officers;
− For shipping companies, the requirement to designate a company security officer in charge of inter alia preparing ship security plans;
− Mandatory preparation of port security plans as well as the carrying out of port vulnerability assessments according to specified guidelines;
− The required designation of a port security officer, with mandatory security training for port workers.

At its meeting on 16-17 July 2002, and following extensive consultations with member governments and industry, the OECD Maritime Transport Committee agreed to initiate projects related to security in the transport chain:

• Ownership and Control of Ships
  This will examine how a "cloak of secrecy" can be created around the ownership of vessels, and will seek to identify "best practices" that would enhance transparency without negatively affecting the confidentiality of commercially sensitive, but non-security related, details.

• Risk Assessment and Economic Impact
  This work will provide an assessment of the risks faced in various links of the transport chain, the potential cost of measures to counter those risks, and who should bear those costs.

• Verification of Cargoes
  This will examine how to verify the identity of cargoes loaded for transport, and how to prevent containers being tampered with on-route. The goal is to ensure the integrity of cargo throughout its journey to the final destination.

The European Commission will table specific legislative proposals with regard to the security of ships and ports during the term of the Greek Presidency, following the decisions taken by the IMO Diplomatic Conference in December 2002.

The World Customs Organization (WCO) has issued a Resolution on supply chain security and trade facilitation at the Council Sessions in June 2002, which addressed a series of steps to protect the international trade supply chain from acts of terrorism or other criminal activities and established a Task Force of Customs experts in order to implement the measures it recommends.

National responses

After the events of September 2001, a number of countries took measures that include:

− increased screening, boarding, and inspection of ships;
heightened surveillance of port facilities and maritime infrastructure;
- establishment of exclusion zones around sensitive ships such as military vessels or cruise ships;
- increased number and scope of container screening programmes.

Since the events of September 2001, the US has tightened security measures involving ports and ships to a greater extent than other countries.

The US Government’s Container Security Initiative (CSI) is designed to enhance security of oceangoing sea containers by pre-screening cargo containers at ports of origin or transit rather than waiting for these goods to arrive in US ports for inspection.

The CSI consists of four core elements. These are: (1) establishing security criteria to identify high-risk containers; (2) pre-screening containers before they arrive at US ports; (3) using technology to pre-screen high-risk containers; and (4) developing and using smart and secure containers. Several significant pieces of legislation were passed including:
- Maritime Transport Antiterrorism Act 2002
- Port Security and Terrorism Prevention Act
- Border Security Enhancement Act
- Port and Maritime Security Act
- Seaport Security Enhancement Act

The US Customs is initially focusing on 20 major ports, since nearly 70 percent of all US-bound sea containers pass through these 20 seaports around the globe. The CSI will not be restricted to these locations, however and container traffic destined for the US will not be limited to CSI ports. Furthermore, the US Government expects that advance targeting of containers destined for the United States should, under normal circumstances, result in those shipments clearing Customs rapidly since they present no identifiable risk. Consequently, from 1 February 2003, the U.S. Customs Service is requiring ships to provide cargo declarations 24 hours before loading.

The US Customs has also started a new co-operative effort with the private sector to improve security along the entire supply chain, known as the Customs-Trade Partnership Against Terrorism, or C-TPAT. It is open to U.S. importers, brokers, forwarders, and non-vessel-operating common carriers. At a later stage, port authorities, terminal operators and manufacturers will be able to join. In return for expedited processing and other benefits, businesses participating in the program agree to:
- Conduct a comprehensive self-assessment of supply chain security using guidelines jointly developed by Customs and the trade community.
- Submit a supply chain security profile to Customs.
- Develop and implement an enhanced security program.
- Incorporate security procedures in its relationships with other companies in the supply chain.
Rail

Criminal activities targeting railway infrastructure and rolling stock have remained relatively infrequent on a world-wide basis, although several countries, notably the United Kingdom, have a long-standing security framework to deal with terrorist acts targeting rail. Railroad police forces have been established in many countries with independent authority and co-operation agreements with government law enforcement agencies. On an international level, the rail security association COLPOFER brings together railway police and security services from 19 European countries to exchange experience and information on railway security and acts as an advisory body to the International Union of Railways (UIC) on security issues.

International responses

The UIC is fostering exchanges among countries on emergency intervention plans, monitoring systems, and information-sharing, as well as financing research and examining security risks in railway stations.

Since the September 2001 attacks, the US Federal Rail Administration (FRA) and UIC have been working together on issues like communicating with the public. Maintaining public confidence in the rail system while taking measures to demonstrate rail company commitment to address the crisis was seen as a key short-term objective, with additional security and counter-terrorism measures to be proposed in the medium-to-long term.

On the freight side, protection of facilities and cargo is seen as the main preoccupation. A joint task force with the US FRA has been established to examine rail freight security issues. And a World Forum on Rail Security was held in Rome in November 2002.

National responses

Counter-terrorism measures implemented in the rail sector on a national level include the following:

− Improved co-operation between local law enforcement authorities and private security agencies, with involvement of the military where necessary;
− Reviews of company security procedures in light of the heightened security threat;
− Specific awareness training and emergency procedure drills for railway personnel;
− More rapid introduction of new security technologies.

Since September 11, the United States government has developed five “critical action” teams to undertake risk assessment in the rail sector in terms of i.) disruption to physical assets ii.) information technology and communications iii.) chemical and
hazardous materials transport iv.) Defense Department shipments v.) train operations. Particular challenges facing rail in the United States, but no doubt in many other countries as well, include the co-ordination of security options among modes and balancing security with operational safety and economic necessity.

Because of its history of terrorist attacks, there is considerable practical experience in rail security in the UK. The National Railway Security Programme concentrates on aspects such as station searches, security of left luggage, and security of non-public areas. The stations categorised according to established risk criteria, and measures applied according to the grouping; for example a Group A station will have much more stringent security requirements than a Group D station. Regarding the Channel Tunnel, “airport style” security has been implemented for passengers at Waterloo and Ashford stations and passenger vehicle security at Cheriton station (Shuttle) using Explosive Trace Detection Equipment and Under Vehicle Video, Heavy Goods Vehicle security using vehicle x-ray, and Trace Detection.4

The Italian railways have, among others, conducted a risk evaluation of its fixed assets in the rail sector, including stations, tunnels and bridges; updated emergency plans and conducted reviews and training drills in railway stations and offices. Private security services have been engaged to patrol stations, rolling stock yards, and chemical and hazardous material yards. Enhanced security measures in postal services have also been put in place, notably x-ray screening of mail.

Japan has implemented specific measures for its Shin-kansen bullet trains that include enhanced video camera surveillance and increased patrols in railway stations, in the trains themselves and in rail yards.

Road

The inherent openness of road and highway systems make them particularly vulnerable to terrorist activities, such as:

- Sabotage on roadways of vehicles carrying large numbers of passengers;
- Attacks on or using lorries carrying dangerous goods (explosive substances, hazardous materials, biochemical substances);
- Truck and car bombs in crowded urban areas, in tourist locations, or near sensitive industrial, military or politically significant infrastructure and buildings.

---

4. UK National Contribution, 14 March 2002
**International responses**

The International Road Union (IRU), whose members include truck, coach and taxi operators world-wide, has a long-standing programme of work addressing different types of road security issues, including road safety, security for drivers, cargo, passengers and vehicles, and commercial and customs security.

In the immediate aftermath of September 11, vehicle, cargo and driver identification checks at border crossing points increased, became more thorough and consequently more lengthy in some countries. Along the US-Canada border, for example, programmes offering pre-approved travel to frequent travellers were suspended. The obvious consequence of this was that congestion increased at many points of departure from and entry to the countries, with longer waiting times to cross at border points.

In December 2001, the US and Canada together implemented policies and measures to restore levels of mobility necessary to maintain their trading partnership. By passing legislation to fund and facilitate changes to the system, and by preparing joint declarations to put in place operational changes, these efforts have led to:

- Funding for significant increases in the number of federal inspection staff;
- Re-instatement of pre-approved travel programmes for frequent cross-border travellers;
- Increased use of information systems and inspection technology;
- Enhanced co-operation with industry to tighten security;
- Integration of intelligence, enforcement and data sharing between the countries.

**National responses**

In most countries, national and local governments took immediate steps to protect public buildings and sensitive infrastructure, military, industrial and commercial sites in the hours following the September 2001 attacks, notably by erecting barriers around and blocking road access to vulnerable sites, and carrying out vehicle identity and driver checks in and outside of cities. But the fact remains that it its virtually impossible to ensure security from road transport vehicles.

**Public Transport**

The open nature of Public Transport systems also makes protection against attacks very difficult. The main accent is placed on public vigilance and emergency plans in case of any incident.

The US Federal Transit Administration has implemented a number of specific security measures designed to enhance security provisions in place and assess remaining vulnerabilities in light of the attacks. They include:
− A series of security assessments on the nation’s 30 largest transit systems using threat and vulnerability methodologies. The assessments were carried out by expert teams made up of former Central Intelligence Agency, Federal Bureau of Investigation and counter-terrorism experts, among others, in coordination with local agencies.

− The provision of assistance and funding to transit agencies to conduct emergency response drills and regional training workshops on security.

The Japanese government has, among others, provided guidance to transit systems to increase surveillance patrols at bus stops near major railway and bus stations, especially when vehicles are parked and during boarding times. It is encouraging more frequent and thorough inspections of all equipment and facilities before and after operations, and has invited passengers to co-operate with authorities on identifying suspicious individuals.

**ECMT Work**

Before the events of 11 September 2001, ECMT work on Crime in Transport focused on, among others, the theft of goods and vehicles or fraud in transit systems. These are serious problems as shippers and transporters well know. We have concentrated on recommendations aimed at Governments and the profession to improve security for vehicles, for goods and staff.

Some of the lessons from this work apply also to combating terrorism; for example, better communication between Transport Ministries and police on validating operator identity, and the verification of driver identity for transport companies.

**Summary of Transport Sector responses**

September 11 has prompted fundamental reviews of the transport systems vulnerabilities and weaknesses. These show that much of the system is open and unprotected and is highly vulnerable to sabotage or attack. The means of transport themselves are also vulnerable to varying extents and can be used in potentially catastrophic ways as weapons of destruction. The attention given initially to aviation should not divert attention from the fact that other modes are even more vulnerable because of their open nature and the scale of the associated infrastructure.

It can be seen that many actions have been and are being taken to improve security and to reduce vulnerability in the different modes. There is unprecedented activity at international level on it.
But the experience reveals that most activities to enhance security have been concentrated within individual transport modes. Counter-terrorism in the aviation and maritime sectors -- though actively debated at present in multilateral organisations -- remains focused on those individual modes. Rail security appears to be largely focused on national-level initiatives, with little inter-governmental exchange to date. Terrorism in road transport has received relatively little attention. There appears to be no multilateral discussion underway on potential risks concerning inland waterway terrorism. And whilst there does appear to be significant experience in establishing an intermodal, public transit system-wide approach to counter-terrorist policies and measures, the debate remains logically focused on a local and national level.

This inconsistency is also a potential risk. In ECMT we saw that the successful efforts to reduce fraud in road transport transit systems resulted in a shift of some of the fraud to railways. The same is true of terrorism and the weakest links risk to be the next targets. It is therefore necessary, in addition to the specific measures affecting the individual modes, to maintain a system wide view of security in transport.

Given these circumstances, the next section sets out some of the challenges that remain to be met.

**Challenges and Opportunities**

The declarations by Governments, by shippers organisations, by customs authorities and security agencies all refer to the need to improve security while protecting trade and commerce. The reality, inevitably, is that the security requirements will impose extra costs, additional delays and more bureaucracy on trade transactions. It is also very difficult to be certain that they are effectively improving security. But in the present climate this has more or less to be accepted. There are some very important issues that will need to be resolved if we want to make efficiency and security gains at the same time. I believe it can be done but it poses a number of major challenges. These include:

**Inter-agency problems**

Different authorities and agencies, even including those under Government control, pursue different objectives. The main task of customs authorities is to check that international trade respects the rules for cross border activities and to ensure that dues and taxes are paid. Security bodies will want to eliminate all risks of an incident, and will give absolute priority to threats or perceived risks. Transport authorities also have several objectives including the assurance of safety in the sector, supervision of competition provisions, registration of companies, and support of trade. In the short term it is clear that the events of September 11 have given an absolute priority to security objectives in transport and other authorities are going to have to adapt to this heightened focus on security. But it is essential to keep the dialogue among different authorities open, to maintain a concept of proportionality and to evaluate all measures based on their
costs and benefits. Trading interests need to show that they are improving security, reducing risks but also asserting their case when ineffective measures are proposed.

**Multilateral framework**

It would be preferable to develop solutions on an agreed international basis but current experience is making this difficult. The United States has passed at least six major new pieces of legislation affecting trade and transport. It has acted with unprecedented effort using enormous resources and at a speed that international bodies cannot even dream to emulate. From the other side, that is from the side of those trading with the United States, we have also seen that there is not the will to wait for international solutions. Several countries have gone ahead with agreements with the US on a bilateral basis. It is logical that the European Commission would seek a mandate to negotiate on behalf of all the Europeans but the speed of events as well as a certain instinct for self preservation among the leading ports meant that the momentum of the occasion took over. The risks for smaller ports are not yet clear and the competitive impact of the measures risks to strengthen even further the economic weight of large ports.

**Goods and documentation flows: More synergy**

Goods transport has four components—the physical movement of the goods themselves, the payment arrangements, the documentation about the goods and information about the goods along the journey. The latter three components—payments, documentation and information can be handled electronically. Despite this, the delays for goods are often due to problems with the paper work. Failure to carry out tasks that can and should be done in advance to facilitate smooth movement results in goods being delayed on quaysides or terminals. While the new security environment imposes additional costs, it is also an opportunity to improve and streamline the documentation and information flows for trade. The fact is that there is too much paper work, that it is fragmented and inconsistent between modes and results in many problems especially at interchange points. Even for single modes, there is an astonishing amount of documentation. A haulier from Eastern Europe has to have 27 different documents on his truck to take a load to Western Europe. A container can have up to 40 separate documents.

A major problem is that customs authorities in many countries are in general poorly equipped for the modern electronic age. The security needs might be a spur to have them move into this age. Certain inefficiencies must not block the trading system.

**New concepts for control**

Shippers move goods from a seller to a buyer and use several modes and different carriers. Shippers know the contents of what is being moved, but carriers do not always. Carriers’ responsibility therefore should be to ensure the integrity of the load between all actors involved; to deliver what they are given; and verify that seals are not broken. In this spirit, a maritime shipping leg may be one component of the trip, but the ports do not
need to be the focus of attention they are at present. Checking and verification can move further up the supply chain, but it appears clear that this will entail better flows of more precise information.

**Costs and benefits / Risk assessments**

Many traders and shippers are concerned that the measures introduced by the US will not deter terrorists but will delay and impose extra costs on every one of the millions of trade transactions that take place. Transporters and shippers are prepared to contribute to security costs but need efficiency and transparency from the customs and security activities. It is essential that new measures are evaluated for cost-effectiveness. Some of the new initiatives in C-TPAT programme try to go in this direction. But the 24-hour rule introduced on 1 February this year has caused concern in Europe and the fear that this will result in serious problems and delays. We need to see if it is really that costly.

**Conclusion**

The new security environment is imposing extra costs on trade and transport. There is a relatively limited possibility to change these given the strength of the concern in the United States. But there is an opportunity to work with these requirements to improve some of the weaknesses in the transport chain and simultaneously to improve quality in all aspects of shipping and transport. But it will require a concerted effort from all of those involved.