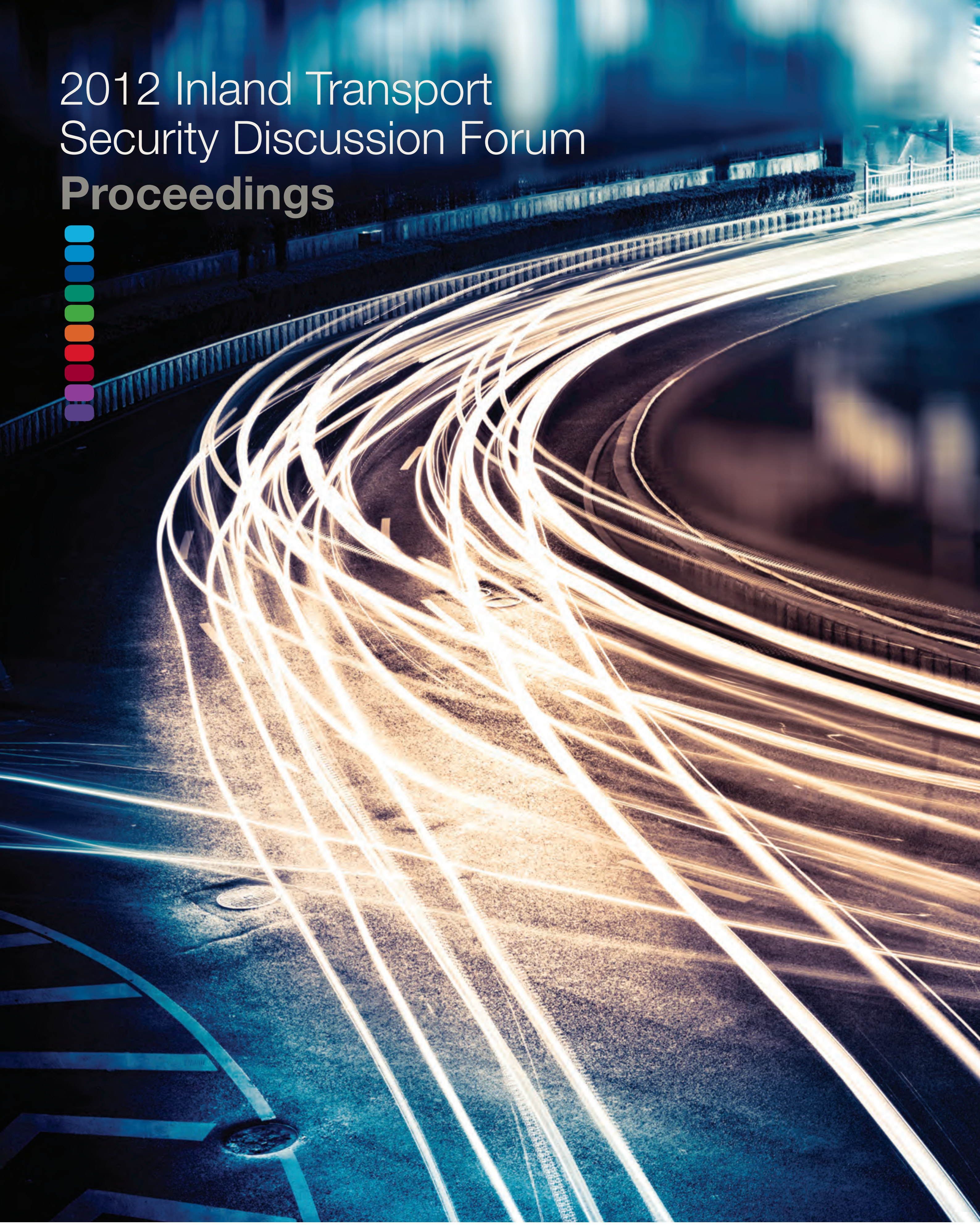
2012 Inland Transport Security Discussion Forum

Proceedings



Organization for Security and Co-operation in Europe

UNITED NATIONS
ECONOMIC COMMISSION FOR EUROPE

The materials in this publication provided are for ease of reference only. Although the OSCE and the UNECE have invested the utmost care in its development, they accept no liability for the accuracy and completeness of the information, instructions and advice provided, nor for misprints. The contents of this publication, the views, opinions, findings, interpretations and conclusions expressed herein are those of the authors and contributors and do not necessarily reflect the official policy or position of the OSCE and its participating States or the UNECE and its member States. Neither the OSCE nor the UNECE may be held responsible for any loss or harm arising from the use of information contained in this publication and neither the OSCE nor the UNECE may be held responsible for the content of the external sources, including external websites referenced in this publication.

In particular, the individual authors/contributors and their organizations/institutions are responsible for the choice and the presentation of the facts contained in their research, resource materials and articles as well as for the ideas and opinions expressed therein, which are not necessarily those of the OSCE and UNECE and do not commit these two organizations. For these reasons, no claims can be made against the OSCE or the UNECE with respect to potential consequences from the reliance on information or conclusions contained in this publication.

ISBN 978-92-9234-184-8

[Author(s), name of the article]
2012 Inland Transport Security Discussion Forum
OSCE/UNECE Project Team and Editors
2012 © OSCE, UNECE

Design: red hot 'n' cool, Vienna
Print: Imprimerie Centrale S.A.
Cover picture: Fotolia

As this publication is a compilation of papers written by external experts the text has not been edited according to the OSCE or United Nations editorial guidelines.

Members of the joint OSCE/UNECE Project Team and Editors:

Alexey Stukalo, Deputy Co-ordinator/Head, Economic Activities; Roel Janssens, Economic Adviser; Gabriel Leonte, Economic and Environmental Adviser; and Zinaida Ligay, Project Assistant; Office of the Co-ordinator of OSCE Economic and Environmental Activities/OSCE Secretariat.

Eva Molnar, Director of the UNECE Transport Division, and Robert Nowak, Economic Affairs Officer.

The project received financial support from the following delegations to the OSCE: Belgium and Kazakhstan as well as from the OSCE.

OSCE Secretariat
Wallnerstrasse 6
A-1010 Vienna, Austria
Tel.: +43 1 514 360
info@osce.org

UNECE Secretariat
Palais des Nations
CH-1211 Geneva 10, Switzerland
Tel.: +41 22 917 44 44
info.ece@unece.org

2012 Inland Transport Security Discussion Forum

Proceedings

OSCE Organization for Security and Co-operation in Europe

UNITED NATIONS
ECONOMIC COMMISSION FOR EUROPE

About the OSCE

With 57 participating States in Europe, Central Asia and North America and 11 Asian and Mediterranean Partners for Co-operation[1], the Organization for Security and Co-operation in Europe (OSCE) is the world's largest regional security organization. It offers a forum for political negotiations and decision-making in the fields of early warning, conflict prevention, crisis management and post-conflict rehabilitation. It has a unique network of 15 field operations across South-Eastern Europe, Eastern Europe, the South Caucasus and Central Asia. The OSCE takes a comprehensive approach to security that encompasses the politico-military, economic and environmental, and human dimensions. Since 2004 the OSCE and the UNECE have been linked by a Memorandum of Understanding (MoU) that provides for close co-operation, particularly – as exemplified by the present publication – in the field of economic and environmental affairs.

About the UNECE

The United Nations Economic Commission for Europe (UNECE) is one of five regional commissions of the United Nations. Its principal aim is to promote pan-European economic integration, which it pursues by bringing together 56 member States from the European Union, non-EU Western and Eastern Europe, South-Eastern Europe and the Commonwealth of Independent States (CIS), and North America. Under the aegis of the UNECE, these countries engage in dialogue and co-operation on economic and sectoral issues. Drawing on the fruits of this common endeavour, the Commission provides analysis, policy advice and assistance to governments and, in co-operation with other global players and key stakeholders, notably the business community, gives focus to the United Nations global mandates in the economic field.

[1] Afghanistan, Algeria, Australia, Egypt, Israel, Japan, Jordan, Morocco, Republic of Korea, Thailand and Tunisia.

Table of contents

Introduction

We are pleased to present the **2012 Inland Transport Security Discussion Forum Proceedings**. This collection of papers on various aspects of inland transport security was written by distinguished experts from public and private sector organizations and has been compiled jointly by the Office of the Co-ordinator of OSCE Economic and Environmental Activities and the Transport Division of the United Nations Economic Commission for Europe (UNECE).

International terrorism and transnational organized crime pose serious threats to the transport sector and to our common safety and security. In recent years, ruthless terrorist attacks have made headlines by targeting inland transport in several countries of the OSCE/UNECE region with tragic results. Many unsuccessful attempts have not made the headlines. Inland transport systems are faced with a complex range of security risks, including all kinds of trafficking, illegal border crossings, and the theft of vehicles and high-value goods. Although air and water ports are also targets, inland transport is believed to be the least-protected link in the global supply chain. It is thus high time that more attention be paid at the international level to the multiple facets of inland transport security.

In the wake of 11 September 2001, preventing and suppressing terrorism have become major policy priorities and challenges for many national governments. International organizations have also responded by reviewing their work plans. At the Organization for Security and Co-operation in Europe, transport security has remained high on the agenda as part of the organization's comprehensive approach to security. Under the Belgian and Kazakh OSCE Chairmanships in 2006 and 2010, respectively, the OSCE Economic and Environmental Forum meetings focussed on strengthening transport security and OSCE Ministerial Council Decisions adopted in 2006 and 2011 include provisions on the subject.

The UNECE's Inland Transport Committee has conducted a review of security in its transport legal instruments and established a Multidisciplinary Group of Experts on Inland Transport Security. The Group has identified a lack of both political and technical awareness of inland transport security vulnerabilities and has recommended modifications to the legal instruments the UNECE administers and the creation of a platform for national authorities and other stakeholders to exchange information, share best practices and coordinate action. In response to these proposals, since 2010 the UNECE, with the support of the OSCE, has regularly organised Inland Transport Security Discussion Forum meetings which gather public and private sector representatives to address current issues in the field.

This volume compiles papers and presentations which were originally prepared for the OSCE-UNECE Round Table that took place on 12–13 December 2011 in Vienna in the framework of the annual UNECE Inland Transport Security Discussion Forum. The texts were reviewed and further revised in 2012 and are now available herein in the form of discussion papers. We find the contributions impressive and worthy of further dissemination among decision-makers, experts, and a broader audience. Both the OSCE and the UNECE plan to continue supporting states in developing and implementing a comprehensive and integrated approach to inland transport security.

We wish to express our appreciation to the Governments of Belgium and Kazakhstan for providing the financial support that made the December 2011 OSCE-UNECE Round Table and the subsequent review and revision process possible. We would also like to thank the Round Table participants for contributing their time and expertise to produce what we hope readers will find to be an interesting, thoughtful and useful volume on inland transport security.

Goran Svilanovic
Co-ordinator of OSCE Economic
and Environmental Activities,
OSCE Secretariat

Eva Molnar
Director, Transport Division
United Nations Economic Commission
for Europe (UNECE)

1

A contrarian’s overview

Mr. Roeland van Bockel | Convenor | CEN TC 379 Supply Chain Security

The myth[1]

Argos was a giant with a hundred eyes[2]. The goddess Hera engaged Argos to guard Io, the object of her husband Zeus’ amorous intentions. In her jealousy, Hera had turned Io into a cow. Hermes (the patron of merchants and travelers) managed to lull the ever-watchful Argos to sleep and then to kill him, thereby freeing Io. Hera transferred Argos’ eyes onto the tail of the peacock and Argos entered the language as a byword for vigilance.

Transport security

Transport security is a part of supply chain security. “A supply chain, boiled down to its basic elements, is the sequence of events and processes that take a product from dirt to dirt.”[3] The Supply Chain Council identifies five words: plan, source, make, deliver and return. Transport security relates to protection and prevention from interference related to “delivering” and “returning”. For public policy purposes, supply chain security is often called transport security. Given the multiplicity of tasks they are called upon to perform public authorities find it difficult to tackle the supply chain security problem holistically. The way that public administration is organized simply does not allow universal coverage of the supply chain. The public policy (organizational) framework is fragmented and has no authority to cover the lifecycle of products. Businesses cannot afford this approach.

In transport security, there are two domains:

- Public – the nation state, which includes participation in international legal regimes covering policy, inspection and law enforcement.
- Private – business, including operators in the supply chain.

The operators are:

- Shippers
- Forwarders
- Terminal operators
- Transport operators

In cooperation between the public and private domain, it is important to develop a coherent security approach. In transport security, public policy can impose two kinds of measures:

- Mandatory rules;
- Voluntary rules (the carrot-and-stick approach).

Whether a policy measure includes a mandatory or voluntary measure depends on:

- The threat;
- The market size of the transport mode or the transported goods or transport unit (i.e. container);
- Political importance of the issue;
- Opportunity for enforcement.

During the last decade, we have witnessed public authorities partly withdrawing from the public space. Policies have been adopted that devolve responsibility for the execution of security measures onto the private market domain (deregulation). This is especially the case for transport security, e.g. development of business certificates.

Since the 9/11 event, the business of security has thrived (i.e. defence contractors access the security market).[4] In Europe, transport security (i.e. aviation and maritime transport) has become an important issue on the policy agenda as far as it relates to terrorism. Within the EU, security policy has been integrated with the sustainability agenda.

The EU, in its efforts to modernize the EU Customs

[1] This paper is a personal perspective on transport security and does not represent the opinion of any official organization or institution.

[2] Argus in Roman legend.

[3] David Blanchard, Supply Chain Management – Best Practices, Second Edition, 2010.

[4] For example, the development of the European Organisation for Security (www.eos-eu.com) is a good example of convergence of the traditional defence industries and the civilian security market.

Code, has managed to implement major reform of parts of its trade facilitation policy by combining it with security imperatives. Without a terrorist threat the majority of EU member States might not have accepted the modernization of the European Customs Code, including the Authorized Economic Operator (AEO) concept. In practice, however, the execution of the Modernized Customs Code suffers from lack of coherent national implementation and enforcement. Furthermore, it is often not obvious what benefits the AEO certificate brings to business.

In a globalized world, facilitating an open trading system and ensuring security have become highly interrelated policy objectives.

The Investment climate

A prerequisite for a SWOT (key strengths, weaknesses, opportunities, threats) analysis on transport security is describing the context, i.e. the investment climate for parties involved – to grow, to prosper or to default. Various emerging issues should be considered.

Trust versus risk

According to one commentator "A revolution of sorts, which is toppling our faith in governments, is ongoing."[5] This is supposedly the result of attempts by public authorities to extend their reach into the private domain, not least because of security concerns (the War against Terrorism) and the need to cover the costs of the financial crisis. This revolution is not necessarily a bad thing. There are very few areas where one can acquire a government guarantee anymore. There are, however, instances where businesses have lost their public authority backing when taking risks on ventures. Government cooperation and involvement may help foster a sense of trust but that public trust often winces at the thought of taking risks which dampens the entrepreneurial spirit that motivates businesses. The balance between public trust and private risk is often precarious. This is also the case for transport security.

Safety versus security

Safety is protection against danger to your person or property. Security is a much wider concept than safety. It applies to your place in the world[6]. A shift in perception and policy is ongoing. Public policy has whittled down the wider question of security to a narrower focus on safety: the reason being that governments, at least in the developed world, possess the institutional capacity to ensure the safety and protection of people. Public authorities cannot unilaterally tackle issues like globalisation, migrant workers, illicit trade and financial market developments. In contrast international businesses can influence security policy in ways governments can't by demanding security arrangements directly with foreign powers such as in the oil and mineral sectors. To some, it appears that private forces, including the international elite that control them, can have more influence on security issues than nation states.

Fear versus power

It does not take a Machiavelli to understand that fear is an essential ingredient of power. A sufficient amount of fear within a society prevents most people from deviating from publically accepted rules of conduct. Since 11 September 2001, governments have increasingly sought to legitimize their policies with reference to security. However, power also requires legitimacy to be effective. The legitimacy of power in Hobbesian terms depends upon protection against threats, i.e. attacks against people. Since 11 September 2011, inhabitants of the Western countries increasingly inhabit a "state of emergency" within which citizens agree to increased restrictions and impositions on their liberty in return for increased protection from threats. Though this bargain should result in a more secure populace states find it harder to police an increasingly interconnected world. More security does not necessarily result in more protection. Fear of external threats in such a situation may in fact decrease the legitimacy of states that cannot be seen to protect their citizens.

The future of transport security breaches versus the state of emergency

The prospect for future terrorist actions is high. It is an asymmetrical conflict wherein an aggressor can be very effective simply by using what is available with very little funds and clever targeting whereas a defender must invest a great deal of wealth and resources to protect the entire population and prevent terrorism[7].

Nation states can never guarantee 100 per cent security to their citizens. The same applies to crime related transport security breaches. Transport can be an interesting target, especially when crossing national borders allowing assaulters a relatively easy way out as long as international police cooperation to fight crime in international transport is undeveloped. It is likely that the trans-

[5] Eric Fry, "Anarchy – An Investors' Best Friend", Safety & Survival Summit speech for Agora Financial Seminar, 14 November 2011.

[6] These thoughts are based on the works of Zygmunt Baumann, *Liquid* Life, (2005), *Liquid* Fear, (2006) and *Liquid* Times: Living in an *Age* of Uncertainty, (2007).

[7] Al Qaeda spent about 500,000 United States dollars in its attacks on the World Trade Center and the Pentagon. In reaction to this tiny investment and the trivial risk it represented, the United States of America spent 10,000,000 times as much The Daily Reckoning, "*Agora Financial*", 3 November 2011.

port crime rate will increase rather than decrease in the coming years, given the economic recession, which was foreseen in most industrialised countries.

In the United States of America, the Department of Homeland Security (DHS) has grown into a huge first responder security organization of approximately 2.2 million employees, incorporating various organizations such as the Customs Services – in 2003 renamed Customs and Border Protection (CBP) – and the Transport Security Administration (TSA). This has led to a trend in which a regulatory environment – held at almost a constant alert status – allows the authorities to instantly act and interfere in people's private lives and business activities. A law enforcement culture has emerged in which regular services, such as customs, have acquired enlarged remits under the Patriot Act aimed at fighting terrorism. Recent statistics show that most interventions are not terrorism related, but rather concern drug related[8] crime. Without a terrorist threat, these enlarged powers would probably not have been approved by the U.S. Congress.

Nation building versus business cooperation

The end of the Second World War has seen the proliferation and successful implementation of multi-lateral regimes and organizations to assist cooperation among states, especially in Europe. The political origins of the EU are security related: to prevent a war between states from happening again. The only possible way to achieve this goal was to develop an economic union.

In this respect borders are considered a threat to international business and the peaceful development of national economies. Since the establishment of an EU internal market only political cooperation through multilateral institutions can further assist the international community to develop effective measures against cross-border security breaches. However, national security legislation and other national issues – constitutional and cultural - prevent the states from merging their policy and executive powers into an overarching international (governing) body.

Within the business community, whose desire for (cheap) international procurement and sourcing is vital to their continued success, national borders have become less of an obstacle than the public authorities that control them. Successful supply chain business strategy is based on cooperation allowing companies to expand beyond national borders and also assist each other in developing effective security, i.e.,

- To prevent a transport incident from happening, or
- To aim at getting an interrupted supply chain back in shape as soon as possible.

In this respect it is very much up to the companies and business concerns themselves to develop and implement their own security measures if they wish to forestall what they consider to be damaging, or restrictive, intrusions into their domain.

Calculating investment opportunities in transport security

Within the public policy domain, it is up to the politicians and their constituents to determine whether it is worth investing in transport security. It is a question of balancing the benefits of participation- especially with regards to potential risks- with the costs of failing one's electorate; there is no other yardstick to measure. It is, after all, the taxpayer's money. Taxpayers will judge the value of security based on their perception of governmental efficacy in delivering public goods such as security and thus hold up those authorities to close scrutiny.[9]

In business, the basic assumptions about whether a transport security measure is worthwhile are different from those for the public domain. Too much or too less security investment can be a matter of profit or loss, which can immediately affect business continuity, performance, competitiveness and growth.

A useful concept for corporate risk management is to define whether a security investment is worthwhile in SROEI — Security Return on Energy Invested — terms. An SROEI analysis could measure how much energy you put in versus how much security you get out. That is, what levels of energy investment are required —risk management, management involvement, operational processes put in place, technologies applied, collaboration established – to deliver and upgrade a company's transport security performance.

Now, an important question is what is the price of transport security? How much would people want to pay for it? In general, the world is currently well sourced with regards to secure transport services. This is because sufficient transport operators are available. But, will sufficient and, more importantly for businesses, affordable services be available in the medium to long term? This is an especially pertinent consideration when searching for new markets in a recession. Furthermore, is it fair that the operators have to pay for the security costs involved?

[8] Delayed-notice search warrants issued under the expanded powers of the Patriot Acts between 2006-2009 show 1,616, drugs for fraud 122 and 15 for terrorism. Avalable http://mrwildman.wordpress.com/2011/09/07/warrants-issued-under-the-expanded-powers-of-the-patriot-act/.

[9] See paragraph 3, numbers 3 and 4.

Companies can still afford to invest X amount of money in transport security when the transport price remains at a stable and predictable level. But, how much more can the prices for transport services go up? When public authorities cannot assist companies in the task of securing the overall supply chain it might become increasingly expensive for companies to afford to invest in security or even to out source such tasks.. Because of the global trend towards outsourcing the effort required to keep track of this numeorous, and multiplying, transport nodes and transnational networks begins to resemble a tug-of-war between technological surveillance and monitoring and cooperation with state (through which resources must flow). This amount of complexity drives the cost of security up. It is unknown what the cost ceiling is at which the public will say “thus far and no more”. This further adds to uncertainty in the market place and serves to drive up prices fuelling a vicious circle.

This intersection between public and private domains, adding the often murky opacity of policy development within bureaucratic state institutions, means that any attempt at SWOT type analyses is doomed to failure without the necessary transparency such an exercise would require. Several studies have, however, been conducted on the actual and potential costs and benefits of transport security investments usually focusing on collateral benefits. However, even then it is difficult to specify the exact costs incurred. This might be an issue for further research a part of which should include suggestions and policy prescriptions regarding the transfer of transport security risks to the customer, possibly even the cargo owner.

European Union transport security developments/the weapons

The essential element of the EU policy on freight transport security transport is to prevent an attack on the supply chain and, in case of such an attack, to get the supply chain back operational as soon as possible.

Below is a list of issues which relate to EU policy in this area.[10]

Transport security threats can originate from a number, or perhaps even combination, of the following:

- Terrorism
- Cargo theft (including pilferage and banditry)
- Counterfeit operations
- Smuggling
- Illegal immigration and human trafficking

Freight transport security is defined as applying to infrastructure, cargo and modes of transport.

The European Council aims to strengthen the development of a cohesive EU security policy with regards to the security of its citizens as per article 3 of the Lisbon Treaty. This was reaffirmed in the “Stockholm programme – an open and secure Europe serving and protecting citizens” of 2010.

The EU endorses a transport security policy primarily aimed at preventing terrorism. Anti-crime/banditry and pilferage are covered in various initiatives such as research and pilot projects on secure parking spaces, scenario planning for logistic security analyses, demonstration projects and national police coordination activities (TISPOL, AQUAPOL and RAILPOL).

Since 2001, the EU has adopted transport security legislation in the following areas:

- Aviation: since 2002 the EU introduced comprehensive cargo screening with less disruptive screening available for companies complying with specific security legislation (such as regulated agents, known consigner and account consigner, etc.). This legislation has been regularly updated and enforced especially regarding airport security screening procedures and techniques (concerning such things as the carrying of gels or liquids).
- Maritime transport and port facilities: since 2004 the compulsory application of the International Ship and Port Security (ISPS) Code EU-wide.
- Ports: since 2006 the introduction of standardised security management into daily port operation practices.
- International trade: the existing provisions under the Customs Code were revised between 2004-2006 (Authorized Economic Operator (AEO)). These were aimed at simplifying trade and transport issues for companies that complied with minimum security requirements.
- Critical infrastructure protection (2008): since 2008 the identification and designation of critical European infrastructure and risk assessment of methods to further increase protection.
- EU recommendation on measures against piracy from 2010.

Legislation for aviation and port/maritime security is implemented throughout the twenty-seven EU member States. The EU Commission actively inspects and monitors implementation. Reporting and revision of legislation takes place on a regular basis. For instance, the AEO legislation implemented in 2008 and extended in mid-2009, included the requirement that operators forward pre-arrival and pre-departure data for operators

[10] For practical purposes, this list is limited and does not cover all actions. The specific numbering of the EC legislation has not been identified.

(between 24 to 1 hours in advance of transport) to the relevant national Customs Authorities.

In 2006, the EU Commission proposed legislation for supply chain security for the EU internal market (SCS), but it was rejected in 2009. In this proposal, the EU endorsed a freight transport policy that helped companies incorporate sufficient security measures into their business operations by fulfilling minimum requirements thereby avoiding later costs. Criteria for fulfillment of conditions would have included provisions for security labeling, which also need to be recognised within the EC AEO procedure.

The WCO has also advocated the mutual recognition of internationally recognized security labels and has urged its members to establish common practices with regards to risk mitigation and security policy as well as a standardized approach on minimum security requirements. Foremost among these suggested common practices is the thorny issue of transparency. The promising USA-EC agreement which allows for automatic mutual recognition of the most important transport security certificates, such as AEO and C-TPAT took a long time to materialize.

Several EC initiatives on public transport security have been studied. Between 2008 and 2010, the EC organized various meetings facilitating the regular exchange of information on best practices. Since 2008 the EC has actively supported crisis management studies and research to obtain information on crisis management tools for various transport modes.

In its recent White Paper on Transport, "Towards a Single Market for Transport" (2011), the EC has reiterated the importance of transport security and its willingness to update freight transport security measures where weaknesses have been identified. An EC Green Paper on Freight Transport Security to discuss the future policy and requirements was due at the end of 2011.

The feasibility of developing possible freight transport security standards had been studied between 2008 and 2010 within the framework of the European Committee for Standardisation (CEN). It reported that business leaders did not wish to propose standards which could enhance the security performance of all surface transport modes, nor were they willing to invest in plugging existing interconnectivity security gaps between the various transport nodes in European port facilities. A standard on a crime incident reporting system has been proposed, however, and was due for decision in 2012. A CEN Good Practice Guide on Supply Chain Security for Small and Medium-sized Enterprises (SME) is in the final stages of development.

The EU has allocated a substantial amount of money for EU-wide security research. Technology can be very helpful in assessing risks and developing tools to monitor and inspect the flow of goods, i.e. container seals, GPS, transponders, information technology platform technology. Technology remains a means to an end —the enhanced supply chain security — rather than the opposite despite the often frantic search for a magic bullet that will solve all the problems.

The private sector has not been lax on this issue either. Many private sector initiatives have been developed and proven successful, like the TAPA/TSR label. However, as these initiatives have no governmental recognition, they cannot be officially recognized by member states. Such initiatives might actually cover gaps in transport security and alert authorities to breaches better than publicly recognized labels because of rims natural desire to protect their valuable merchandise.

On a business level, a list of possible transport measures can be identified, some of which are elaborated in EU legislation (maritime and aviation security, and AEO). These measures relate to issues such as:

- Training and education (i.e. awareness training, skills);
- General best practices (such as the involvement of managers) and risk management practices (how to judge a threat);
- Procedures (licences, controls);
- Physical barriers (i.e. fences and locks);
- Technology (i.e. closed-circuit television (CCTV), radio frequency identification (RFID), information technology (IT).[11]

Evaluation

Tailor-made measures

The future of effective public policy action in transport security is poor. The major reasons for this are that public authorities and governments:

- Simply lack the means to develop suitable legislation;
- Lack the power to do something useful;
- Are not really interested in developing a coherent approach (also due to internal squabbling but also an inability to approach the issue from a holistic life-cycle perspective).

[11] As this paper served as a provocative introduction to a two day Round Table on Inland Transport Security, an extensive list of measures has not been included in this paper. The measures will be mentioned in other papers and presentations during the Round Table.

Public authorities can substantially influence transport security within certain areas. Enforceable measures can be enacted:

- Within a specific transport operation or;
- Relating to specific requirements for modes of transport.

However, such an approach would disregard the connectivity of the complete supply-chain operation. A suitable transport security policy requires that every link within a supply chain be sufficiently secured. This involves harmonization and standardization within a multilateral environment in which states and business act in unison. A level playing field between all actors in the supply chain forms the first requirement for this to be effective.

Green lane treatment

National public authorities can support business in securing supply chains by offering green lane privileges. Thereby standards can be developed in mutual cooperation and be continuously fine-tuned. The benefits of green lane treatment to business should be constantly promoted.

Securitization of transport security

A securitization of transport has emerged amounting to a cottage industry of professional organizations producing a plethora of practices, theories, labels and concepts. These are in turn validated by those same professional organizations. It is very difficult to judge whether the principles and measures being defined by the various transport security specialists actually increases physical transport security. The proliferation of labels, concepts and procedures (often sold as best practices) can easily lead to confusion, a reduction in security or a false sense of security. It could also create conditions ripe for exploitation by non-regular trade, illicit, or illegal trade. The practice of processing security labels can create a sense of virtual security in which the label not the cargo takes centre stage which does not necessarily correspond to the physical business security needs.

Other possible risks of the securitization of the supply chain are:

- Dispersion of accountability; one party performs different roles (AEO: audit, approval, execution) none of which are coordinated;
- Market Incomprehension as regards to the actual value of any given label;
- Dependency on experts whose livelihood rests on fostering the sense of insecurity they are meant to be mitigating.

The issuing of transport security labels has even created a stock market of sorts that allows for the trade in labels. Some companies have obtained security labels, spending a substantial amount of money, in order to enter markets from which they were previously barred but in which they may not necessarily be compliant with legal requirements. This merely highlights the need for a universally recognized system of labelling.

Conclusion – Key recommendations

Like the myth in transport security, Hermes outpaces Argos. Transport security development is primarily a business concern. They are the primary stakeholders and should ask for assistance from governments when necessary. Public authorities have a very limited reach.

With respect to public policy:

An effective and coherent EU transport security policy has yet to be established. It is unlikely. One should rather look into what can be done to exploit present measures to their maximum potential. There are several major issues which need more attention at the EU level:

(a) EU transport security measures still lack a coherent security perspective addressing the interconnection between the various modes of transport and supply. For instance, the ISPS code is applicable to seagoing vessels and terminals, but does not apply to continental transport like barges, which load and unload in terminals/ports under ISPS jurisdiction;

(b) The AEO status still does not clearly show the major benefits to all transport operators nor motivate them to participate. Operators, which are not involved in the import or export business, cannot apply for an AEO status in all EU member States;

(c) Mutual recognition of security certificates and labels should be pursued which should result in the following positive effects:

- Proliferation of labels will stop (to be done in a Public Private Partnership)
- The benefits of the labels in relation to physical security will be transparent
- Relating business, the basic question is: Who pays the ferryman? Further measures will assist businesses in costing transportation providing predictability.
- Provide the first step in formulating a holistic and sustainable approach to transport security

Comments

Dr. Garland Chow
Associate Professor, Sauder School of Business
Director, Bureau of Intelligent Transportation Systems
& Freight Security
(BITSAFS – Sauder)
Associate, Centre for Transportation Studies
University of British Columbia, Canada

Roeland van Bockel has produced a concise and insightful commentary on the state of inland transport security in the EU. There are many similarities between the EU and the North American situation in security and public policy, through there are differences as well. I will highlight a few similarities and differences from which we, from both sides of the ocean can learn from. I will comment on some of the specific observations he makes on transport security and his overall recommendation for which I will have to be a contrarian to the contrarian[12].

The State of Transport Security Policy

"The future of effective public policy action in transport security is poor. The major reasons for this are that public authorities and governments:

- *Simply lack the means to develop suitable legislation;*
- *Lack the power to do something useful;*
- *Are not really interested in developing a coherent approach (also due to internal squabbling but also an inability to approach the issue from a holistic life-cycle perspective)."*

At first glance, we in North America are disappointed to hear such an observation. Many in North America mistakenly view the EU as more than an economic union and mistakenly think that some monolithic authority exists that magically makes decisions for the whole union with respect to non-trade and non-economic policy. Proponents of a unified policy in North America frequently point to the 25 countries in the Schengen area as a benchmark, but the reality is that the United States of America has a 52 state Interstate Commerce Act that guarantees free commerce across all state borders. As Roeland aptly points out, the Department of Homeland Security in the United States of America with its enabling legislation and culture has no trouble in implementing a security agenda that often lets security "trump" trade or privacy. It is pointed out that, what some might consider, draconian legislation may never have occurred without the disaster of 11 September 2001. Similarly, the majority of EU member States might not have accepted the modernization of the European Customs Code, including the authorized AEO without a security rationale based on a terrorist threat. I am going to assume that an event of the magnitude of 11 September 2001 is not going to happen again in the near future, and that transport security policy must develop within the institutions that exist today, which include the public's perception of the importance of transport security.

In contrast, transport security policy governing transport between the United States of America and Canada does suffer from a lack of effective policy action, but that depends on whose point of view one adopts. The primacy of security concerns in the United States of America has resulted in the thickening of the border and an increase in the cost of trade between nations. But this has primarily impacted Canada, rather than the United States. As I will describe in more detail in my own presentation tomorrow, the holy grail of an efficient, but secure border, has been sought since the Smart Border Declaration and Action Plan in 2001, to the Security and Prosperity Partnership (SPP) of 2005, and continues with the Shared Vision for Perimeter Security and Economic Competitiveness in February 2011. The "Beyond the Border Vision" (BBV) is to be unveiled this month.

The situation is no different in the EU for which Roeland observes "borders are considered a threat to international business and the peaceful development of national economies. Since the establishment of an EU internal market only political cooperation through multilateral institutions can further assist the international community to develop effective measures against cross-border security breaches. However, national security legislation and other national issues – constitutional and cultural - prevent the states from merging their policy and executive powers into an overarching international (governing) body."

I view the development of transport security in North America more optimistically and submit that there are many lessons to learn on how institutional barriers are overcome. Let me highlight a few:

- The focus of the transport security policy debate and development in North America has been on border management. If the lack of progress in transport security policy is in the area of inland transport security within the EU, the EU should refocus the freight security policy debate on the borders of the EU where a stronger common interest and consensus on security lies;
- Public policy development needs to understand and address underlying institutional barriers. The failure of the SPP of 2005 to make any progress

[12] Mr. Roeland van Bockel, Convenor CEN TC 379 Supply Chain Security.

despite having a high level of leadership from both countries was that security and trade issues were dealt with separately by two different working groups in the expectation that somehow they were to magically come together. That appears not to be the case for the new Shared Vision for Perimeter Security and Economic Competitiveness, but to know for sure, we anxiously await the Beyond the Border Vision report scheduled for release this month. In addition, the issues of privacy and immigration need to enter the discussion early, not late. Roeland is right on target when he asks "Am I prepared to give away a chunk of my freedom in order not to suffer from violence, stress and so on". As he suggests, recasting security as a safety policy has much merit, especially in the realm of public opinion;

- Public policy changes often build on, and are the culmination of, discussions and negotiations over a long period of time. Many of the action items in the Smart Border Action Plan in 2001 had already been discussed at both the implementation and the strategic level prior to 2001. It would be nice if policy changes could be made immediately, but that simply isn't realistic. It may be the case that some of the transport security initiatives that have been considered in the EU should be like the constantly lit flame on your water heater ready to turn on when the (hot water) flow of freight security needs to be heated up;
- Public policy responds to public pressure. One of the top reasons that the discussion continues with respect to managing the United States of America–Canada border effectively is the united pressure brought to bear from business groups in the United States of America and Canada such as the respective Chamber of Commerce organizations in both countries, both of whom have considerable clout. What has been the role of comparable organizations in the EU in this debate?

In summary, I would like to look at the development of freight security policy in the EU as a cup that is half full, rather than half empty, and progress is still to be made.

The Private Sector Role in Transport Security - 1

"During the last decade, we have witnessed public authorities partly withdrawing from the public space. Policies have been adopted that devolve responsibility for the execution of security measures onto the private market domain (deregulation). This is especially the case for transport security, e.g. development of business certificates."

The role of the private sector in transport security cannot be underemphasized and Roeland recognizes the key responsibility of the private sector, whether they are operators of transport, or they are customers in the supply chain. It might be an overstatement though to characterize public authorities as withdrawing at all from the public space in freight security, as few governments previously micromanaged transport operations. Government continues to set minimum standards and enforce them or provide incentives to meet them and certainly, security controls at borders have increased. That is why Roeland's observations on progress in developing valid security certification and providing recognition are very important. The private sector is driven by the bottom line and freight security investment is driven by financial self-interest. Firms, perhaps begrudgingly, invest in security to meet mandatory rules and regulations, but the carrot-and-stick approach is needed for voluntary rules. An integral component of current public certifications such as C-TPAT and FAST in the United States and PIP in Canada (and I assume AEO in the EU) is that governments can reward participants in the transport chain with reduced security burdens at borders. Roeland points out that AEO status still does not clearly highlight the major benefits to all transport operators to motivate them to participate more fully, and that is also true for C-TPAT, PIP and FAST. Public policy can seek rational means for increasing the benefits of policies, to reduce the costs of certification, and support rational analysis. Certification, for example is an important criterion considered in green lane treatment at borders. National public authorities should be encouraged to expand these programmes creating the momentum needed for the development of common standards which should be continuously fine-tuned. The benefits of green lane treatment to business should be constantly validated. Roeland also mentions that mutual recognition of various security certificates should be further developed allowing firms to leverage the investment to obtain one certification to obtain other certifications resulting in more benefits. To recognize the benefits of certification, Roeland alludes to the concept of SROEI or Security Return on Energy Invested. I am not sure what progress is being made in Europe, but the U.S DOT Freight Operations Management Office has developed the Freight Technology Assessment Tool (FTAT) which provides a rigorous approach to evaluating the return on technology investments. I see no reason why this tool can't be adapted to security investments especially since technology plays a key role.

At the same time, Roeland warns us to be wary of the potential proliferation of the labels, which can be prevented with the proper Public-Private Partnership. The time to start that effort is now, since without any confidence in the certification process the foundation for the public sector to reward compliance and the motivation for the private sector to adopt are both lost. I wonder if the USA-EC agreement, which allows for automatic mutual recognition of the most important transport security certificates, like AEO and C-TPAT, would not have materialized if widespread recognition of a standard certification within the EU by both the public and private sector had already been in place.

The Private Sector Role in Transport Security - 2

"The way the public administration is organized simply does not allow overall coverage of the supply chain".

Roeland refers to the Supply Chain Council classification of supply chain processes: plan, source, make, deliver in the SCOR model, to emphasize the small segment of the total supply chain that transport has a direct influence on. This insight has profound implications for freight security, as the supply chain is a total interconnected system where downstream members have an impact on upstream members and vice versa.

In fact, freight security starts at the beginning of the supply chain, which is not where the product began its trip, but where the product was designed and suppliers selected. For example, the packaging could be designed to be less susceptible to unnoticed insertion of unwanted material, or the product can be designed to be consistently uniform in weight so that unexpected weight changes of products in transit can be detected. Security, like quality, starts at the source. For many supply chains, it is easier to prevent a security problem than it is to detect it. Thus it is very important that suppliers can be selected to minimize freight security risk based on their own risk footprint. This includes logistics suppliers as well as product suppliers. In fact, certification does include elements of supplier sourcing certification. For example in C-TPAT, importers must evaluate their supplier's security efforts and footprint. In other words, the normal working of a well-functioning supply chain is the mechanism for encouraging increased supply chain security upstream.

This increases the need to develop and gain widespread recognition of a valid system or standard of certification for supply chain security, for which transport and even logistics security, is only a subset. One can foresee security being an element in supplier scorecards and total landed cost analysis, where the security factor can be formally accounted for.

The same process is in fact going on right now in the field of supply chain sustainability, where the environmental (typically the carbon) footprint or rating or score or other Corporate Social Responsibility (CSR) assessment is an integral part of the supplier selection process. Some of you are familiar with the Scope 1, Scope 2, and Scope 3 framework for measuring a firm's environmental impact. The same framework is applicable to freight security. It is noted by Roeland that "Within the EU, security policy has been integrated with the sustainability agenda". I wonder if their similarities, such as both being externalities produced by economic activity and the role of the whole supply chain in producing these externalities are reasons for this treatment.

One fact remains for firms in the supply chain: to seek security from its suppliers and invest in security for its own direct processes, they either have to fulfil some regulatory requirement or do it in their own self-interest. Government can only wield a carrot and a stick where it has some form of control. At this time, control is really only effective at borders entering a country or trade zone. Security at the border is the key location in the supply chain where public policy can be implemented. If transport operators and importers want the green lane, they will need to be a trusted member of the supply chain. Certification is a component for assessing that trust. But to achieve certification, the transport operators and, in particular, the importers, need to have secure suppliers. If they have an incentive to choose such suppliers the hand of public administration can indeed reach deep into the supply chain.

Conclusion

"Like the myth, in transport security Hermes outpaces Argos. Transport security development is primary a business concern. They are the prime stakeholders and should ask for assistance of the governments when necessary. Public authorities have a very limited reach."

The myth of Argos on one hand could be interpreted as letting Hermes, the businessman, take care of security because it is primarily a business concern. But it could also be a warning that the public sector must remain diligent and play a crucial role in transport security, if not supply chain security. Public authorities may have a limited reach, but they also have unlimited responsibility which they cannot walk away from by going bankrupt.

Transported Asset Protection

Thorsten Neumann | Chairman of the Transported Asset Protection Association, Europe, the Middle East and Africa (TAPA EMEA) | On behalf of the TAPA EMEA Board & Association

Delivered by **David Reid** | Corporate Supply Chain Security Manager, Europe. Middle East, Africa and CIS, Panalpina Company

This submission has been prepared as a discussion document - in response to the invitation of the United Nations Economic Commission for Europe (UNECE) and the Organization for Security and Co-operation in Europe (OSCE).

Transported Asset Protection Association (TAPA EMEA)

The Transported Asset Protection Association (TAPA) is a non-profit trade body operating globally. TAPA EMEA operates in Europe, the Middle East and Africa. TAPA was formed over a decade ago, initially by a small group of manufacturers in the hi-tech industry who were all victims of cargo crime; EMEA now consists of over 300 member companies and over 700 member companies worldwide. TAPA has created a unique forum that unites manufacturers, logistic providers, freight carriers, law enforcement agencies, the insurance industry and other stakeholders with the common aim of reducing crime-related losses from international supply chains.

TAPA Security Requirements

TAPA Security Requirements are recognised globally as a leading industry standard for cargo facility and transport security, notably:

- FSR (Freight Security Requirements)
- TSR (Trucking Security Requirements)
- PSR (Parking Security Requirements)
- TACSS (TAPA Air Cargo Security Standards)

These standards which are regularly updated were created by security and logistics specialists to help TAPA members reduce losses, and provide a platform for more uniform conformance with a higher level of security. TAPA certified carrier hubs and facilities guaranteed minimum security standards for manufacturers and are, for example, suitable for inclusion in contractual agreements.

TAPA's Security Requirements have been established by security professionals within the high value high risk product sector to address the nature by which goods are handled, warehoused and transported as they move throughout the globe. They specify the minimum acceptable security standards for assets travelling across the supply chain and the methods to be used in maintaining those standards. In addition, they outline the processes and specifications for companies to attain TAPA certification for their facilities and transit operations.

TAPA security requirements provide a valuable quality and security benchmark for manufacturers and shippers that want to choose logistics providers that meet or exceed TAPA's certification requirements. The successful implementation of these standards is dependent upon suppliers, TAPA certified auditors and customers working together to accurately interpret, adopt and audit security standards against these requirements. Where applicable, all TAPA standards are independently audited.

TAPA – Crime intelligence

When it comes to preventing crime, fast and accurate intelligence is critical. TAPA's Incident Information Service (IIS) constantly captures and shares data, enabling members to use the latest cargo crime intelligence to avoid incident 'hotspots,' protect valuable goods in transit and, if required, to report and trace stolen property. IIS intelligence is provided to the service by individual TAPA members and law enforcement agencies (LEA) and is made available to members using fast incident information e-mail alerts as soon as new incidents are reported. In addition IIS issues quarterly bulletins, has an online database and shares information via TAPA EMEA's monthly newsletter.

IIS acts as a centralised resource of knowledge in criminality of freight in transit within the EMEA region, facilitating the dissemination of this information to member companies and to LEAs.

Additional benefits of IIS include:

- Rapid dissemination of incident reports support the investigation process and recovery of stolen items;
- Statistical analysis of 'high risk' routes and geographical areas to allow corrective and pre-emptive actions;
- Increased awareness of cargo theft problems at local, national and international levels;
- Access to a database of incidents against members' freight shipments can be stored in a common format, analysed and made available to all members and to relevant law enforcement agencies;
- Use of a managed directory of contacts within LEAs, manufacturers and logistics security personnel;
- Links to sources of manufacturers' product descriptions to support investigative activities;
- Mapping location tools.

Key Areas for UNECE/OSCE discussion

- Member States' initiative on Drivers' ID;
- Member States' commitment for secured parking;
- Member States' having a designated Prosecutor for Cargo Crime; Member States initiative on data sharing between members and TAPA IIS;
- Safe and Secure lanes for cargo.

UNECE/OSCE initiative on Drivers' ID

One of the many challenges that our members face, especially those involved in the transport sector, relates to driver IDs. Due to the ease with which the EU workforce can move within member States, it is difficult to know if a driver has been involved in supply chain crimes elsewhere before being placed in charge of a high value or a sensitive consignment of goods or materials.

The Driver Identification Database (DIDb) is a cross-border voluntary quality assurance system for drivers (as members) and for companies (as partners) having transported assets in the supply chain.

The system, which has been in operation for approximately three years, objectively, but rigidly, evaluates the drivers during the registration process and prior to accessing membership within the DiDb database. Once the vetting process is completed, the driver will be registered in the database and receive a unique pin number. Currently, there are just over 4,000 drivers registered in this database (July 2011).

The Driver Identification Database is a new initiative: a complex system which consists of reliable and trustworthy drivers. The service is provided to transport organizers, manufacturers, factories, vendors, forwarders and other companies, which are usually unable to check and identify the driver beyond doubt prior to the handover of goods.

DIDb is a simple and independent security system of assurance processes and protocols. The use of DIDb can decrease the risk factors for human resources in land transportation to a minimum level.

DIDb is an online, closed system, which records drivers working on or contributing to a forwarding process. This 'white list' of reliable and trustworthy employees is updated immediately, as needed, and the partners of DIDb can use it whenever they want to begin transportation.

Currently, drivers from the following countries have registered (July 2011):

- Bulgaria
- Croatia
- Czech Republic
- France
- Germany
- Hungary
- Italy
- Mongolia
- Netherlands
- Poland
- Romania

- Serbia
- Slovakia
- Slovenia
- Spain
- the former Yugoslav Republic of Macedonia
- Ukraine

For further information, please visit www.sectran.eu

Recommendation

Although this initiative has been developed by commercial entities within the supply chain industry, TAPA and its members would welcome a statutory database in which it would be mandatory for drivers who wished to work in the supply chain industry to register for inclusion in the database after an appropriate vetting process, and, therefore, TAPA and its members would urge member States to consider how it could embrace this private public partnership to help to mitigate crime risks within the industry.

UNECE/OSCE commitment for secured parking

One of the biggest challenges facing the supply chain is how to protect a stationary vehicle. Over the last few years, TAPA members have seen an increase in the numbers of attacks on stationary vehicles as they fall easy prey to a would-be thief. This type of crime has accelerated since 11 September 2001 given that many facilities are now much “harder” targets; crime has displaced to the road. After the publication of the Secure European Truck Park Operational Services (SETPOS) best practice handbook and the LABEL project, TAPA introduced its Truck Parking Assessment Programme, which includes the uses of its Parking Standards Recommendations to assess the security provision found at parking locations throughout the EU.

Currently, TAPA has just started assessing parking sites (77 to date). TAPA has issued information guidance to its members on the status of the security provisions found at these locations.

In addition, TAPA has been working with ESPORG (European Secure Parking Organisation), who currently operate thirteen sites in Belgium, Germany, Italy, Serbia, Spain and Sweden, all of which have obtained LABEL level 3 status to increase awareness and the need for more secured parking sites.

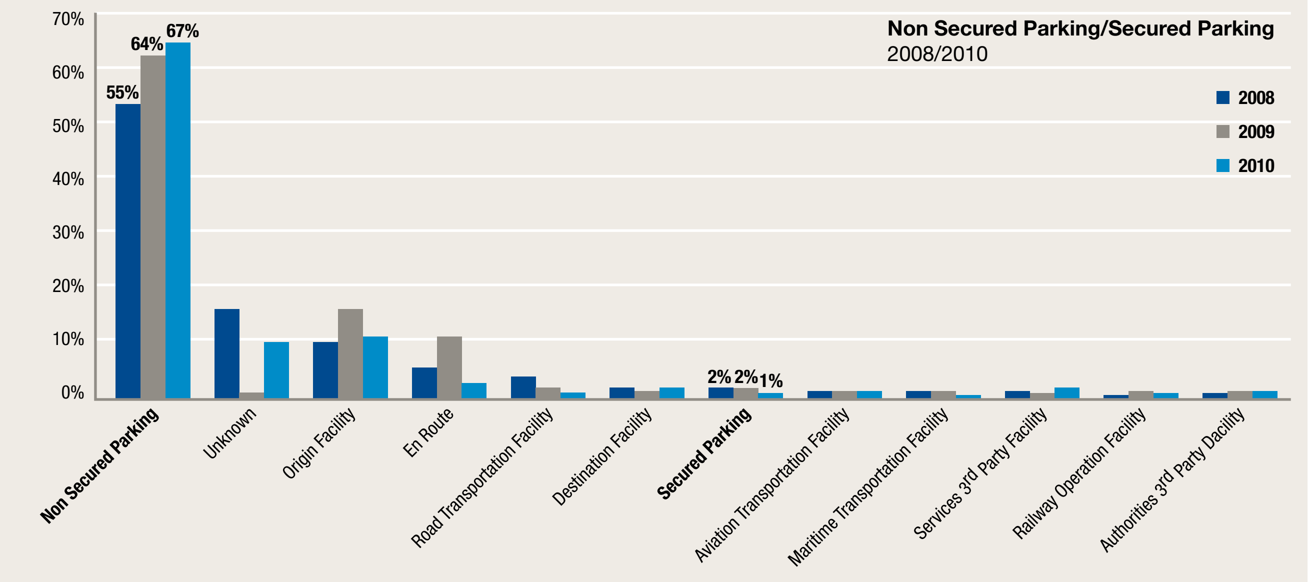
From our data, we have identified that most incidents of theft occur while vehicles are parked in non-secured locations, as opposed to secure parking locations; a trend which appears to be on the increase.

Location Type	2008	2009	2010
Authorities 3rd Party Facility	1	8	0
Aviation Transportation Facility	34	11	23
Destination Facility	43	34	17
En Route	152	342	46
Maritime Transportation Facility	30	14	9
Non secured Parking	1,352	1,923	1,074
Origin Facility	251	522	195
Railway Operation Facility	2	2	7
Road Transportation Facility	115	42	8
Secured Parking	43	50	12
Services 3rd Party Facility	8	21	41
Unknown	417	13	176
Grand Total	**2,448**	**2,982**	**1,608**

Location Type	2008	2009	2010
Authorities 3rd Party Facility	0 %	0 %	0 %
Aviation Transportation Facility	1 %	0 %	1 %
Destination Facility	2 %	1 %	1 %
En Route	6 %	11 %	3 %
Maritime Transportation Facility	1 %	0 %	1 %
Non secured Parking	55 %	64 %	67 %
Origin Facility	10 %	18 %	12 %
Railway Operation Facility	0 %	0 %	0 %
Road Transportation Facility	5 %	1 %	0 %
Secured Parking	2 %	2 %	1 %
Services 3rd Party Facility	0 %	1 %	3 %
Unknown	17 %	0 %	11 %
Grand Total	**100 %**	**100 %**	**100 %**

One of the main obstacles affecting the development of secured parking sites, especially in the current economic climate, is the ability to secure the additional funds required for installing any additional security equipment.

Any assistance from member States in grant funding to enable parking site owners to obtain EU LABEL level 3 status would be eagerly welcomed by the industry, and would assist in reducing crime when vehicles are stationary.



Recommendation

TAPA recommends that Member States participate in a consultative process with TAPA and Truck Park Owners to assist in creating more secured parking places in their countries.

Each member State should have a designated Prosecutor for Cargo Crime

In November 2009, the Secretary of Justice for the Netherlands announced that as of 1 May 2010, a National Prosecutor would be appointed for the coordination of the activities against cargo crime. This appointment followed a motion in Parliament, which was adopted by a wide majority in both governmental and opposition parties after much procrastination between the Parliamentary Committee of Justice and the Secretary. The main concern for the Committee had to do with questions over the volume of incidents and if there would be a sufficient number of incidents reported formally to the Police to warrant the post.

During the discussion process the TAPA EMEA Taskforce Netherlands called upon the Chair of Transport & Logistics Netherlands (one of the largest industry bodies within the Netherlands,) and the CEO of TNT to sign a letter for the Secretary of Justice requesting a meeting wherein the transportation industry could inform the Secretary of its concerns. During this meeting, of 17 November 2009, the industry took advantage of the excellent opportunity to explain the need for a National Prosecutor against Cargo Crime on the basis of the numbers of incidents, the amount of (insurance) damage, the displacement of crime from inside the perimeter into the public area, making private parties much more dependent on the authorities to ‘maintain law and order’, and the loss of traffic for the Netherlands (gateway to Europe!) due to the fact that the flows of traffic would bypass the Netherlands and be flown into neighbouring countries such as Belgium Germany, and the United Kingdom.

Following the meeting, the TAPA EMEA Taskforce Netherlands was invited to assist the Ministry of Justice in drafting a letter from the Secretary of Justice to Parliament explaining his decision to appoint a National Prosecutor against Cargo Crime and a Special Intervention Team, tasked to assist regional police forces across the country in investigating cargo crime.

We are pleased to announce that the National Prosecutor against Cargo Crime is also liaising with prosecutors in any other country where may appear to aid in the fight against cross-border crime or may comply with any foreseen requests for legal assistance in cases that would be prepared for trial abroad. We would recommend that the European Commission look at this appointment as a best practice to help fight cross-border cargo crime.

Recommendation

TAPA would like to recommend that the member States examine this best practice and strongly encourage member States to appoint a designated Prosecutor with special responsibilities for cargo crime.

UNECE/OSCE initiative on data sharing between members States and TAPA IIS

The TAPA incident information service (IIS) has collected a database of over 19,000 incidents, since its inception, giving TAPA members and its Law Enforcement Agency (LEA) partners invaluable information on cargo crime trends and patterns. However, even with this data, we are aware that this is only a small part of the whole picture. For example, LEAs at TAPA conferences or in our debates have indicated a baseline willingness to share more incident data and reports subject to having appropriate legal and other arrangements in place.

The challenges sometimes come down to terminology, using common data fields to capture and store data, and financial resources, as we recently discovered in the United Kingdom of Great Britain and Northern Ireland, when TAPA was removed from the circulation list of Truckpol (UK): this being due to budget restrictions and also a political decision.

TAPA EMEA has strived over the past years to build close relationships with key LEAs who have been responsible for crimes to carry out investigations in the supply chain. TAPA has been fortunate to receive periodic historical data from a number of national police forces, which have assisted us in this project. However, gives the impression that cargo crime is higher in certain countries, whereas this just represents the fact that crimes are better reported or statistics are easier to obtain.

TAPA has shared its data openly and the data has been used and published by Europol.

Sample data overview provided in Figure below.

Recommendation

TAPA EMEA would, therefore, strongly recommend that UNECE/OSCE consider asking member States to record cargo crimes and make the data available, through a centralized agency, who in turn can work with TAPA to include this data in the TAPA IIS. This would value to the existing data which would be available for all LEA's within the region when looking for patterns of crime and criminal behaviour. It would also allow TAPA members to make risk assessments and take preventative measures when required, in their endeavours to reduce crimes within the supply chain.

Safe and secure lanes for cargo

Following the inaugural conference in the Netherlands in 2008, a TAPA task force was created to work with the Dutch authorities to find various ways of reducing cargo crime within its borders.

The Second Covenant on the Prevention and Repression of Transport Crime (December, 2009) commits public and private parties in the Netherlands, amongst others, to realise secure transportation via the Dutch motorways. A pilot secure lane project on the corridor from Venlo (Dutch-German border) to the port of Rotterdam has shown a massive reduction in transport crime: (74 incidents in 2009 to 4 incidents in 2010).

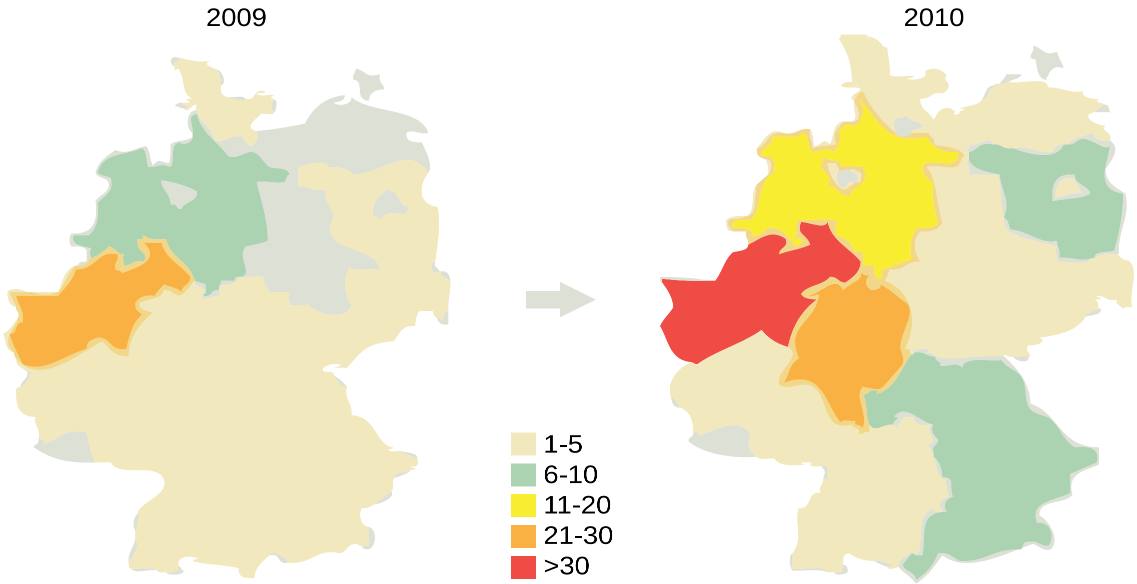
This was achieved through the implementation of cameras, connected to a police database, with the capability to recognise both license plates and vehicle movements on and between parking areas, truck stops and restaurants along the corridor.

The cameras sent a signal to a regional control room for any suspect license plates or vehicle movements, where private parties observe and assess the information in real time. Any required follow-up on their findings would be initiated by the police from the same control room.

A displacement of transport crime was also noticed into industrial zones, company yards and across the border. An overall reduction of crime by 25 per cent a year appears to be realistic.

On the basis of these results, a business model assessing the economics of a rollout across the motorway network of the Netherlands has been undertaken.

Metal Thefts in Germany



This model has been presented to the Dutch Ministry of Security and Justice and a new steering group will prepare further rollout with public/private funding and management.

Connecting secure lanes with industrial zones will be part of this rollout in order to reduce any displacement of crime from the motorways into these areas.

The Dutch Government views this project as being vital to the infrastructure of the country and to the position of the Netherlands in the European economy.

Neighbouring countries have shown interest in this project as well as opportunities to connect their motorways to it.

Recommendations

TAPA would like to recommend that member States examine, in-depth, the Netherlands 'secure lane' project and promote this as a best practice amongst the member States.

Finally, private industry considers current and emerging regulatory security requirements for air cargo as very important, but more could be done to harmonize these programmes between the EU and the rest of the world. In a global economy shippers standardize controls to transport goods while still ensuring their safety and security. Programmes such as AEO & CT-PAT give a solid platform but so much more could be done to align and mutually recognize the security requirements of various national governments. The standardization efficiencies that are gained would include making goods easier and less costly to ship in and out of the region.

3

Road transport and security

Mr. Umberto de Pretto | Deputy Secretary-General | International Road Transport Union (IRU)[14]

The overall performance and efficiency of the road transport industry depends on the security environment in which transport operators undertake their domestic and international activities.

Security in road transport encompasses closely interrelated elements:

Physical security

Physical security is the material conditions for drivers, vehicles and the passengers and goods transported. This directly relates to the level of protection required to avoid or prevent theft, hijacking, violent attacks, intrusion and/or manipulation of goods in the load compartment.

Commercial security

Commercial security relates to the practical and legal conditions under which road transport operators can operate. This aspect directly relates to the ability of road transport operators to secure – from the legal point of view – the sustainability and profitability of their commercial relations with their clients, including their financial dimensions. Thus, it includes legal certainty and predictability. For example, this covers the ability to check the reliability and solvency of commercial partners in order to ensure the legitimacy of the operations undertaken to prevent illegal transport such as prohibited or illegal goods.

Customs security

Customs security refers to the Customs procedures applied to vehicles and goods transported internationally guaranteeing compliance with Customs and fiscal regulations, as well as with new requirements focusing on global supply chain security and anti-terrorist measures. Although terrorist risks must be considered, road transport operators are more directly impacted by other types of security threats, which seriously impair the safety and security of their drivers, vehicles' passengers and consignments. A study by the IRU and the International Transport Forum (ITF) has shown that criminal activities are increasingly life-threatening for professional drivers. From 2000 to 2005, one driver in six has fallen victim to an assault or other form of organized crime; in most cases when the vehicle was stationed in insecure service stations or parking areas. The current lack of secure parking areas for commercial vehicles and of accurate information about their location significantly increases drivers' risks and facilitates criminal activities. Moreover, overall security in the road transport industry can only be ensured by implementing harmonized regulations and best practices that guarantee an appropriate level of physical, commercial and Customs security in order to:

- Prevent the occurrence of high risk situations;
- Treat incidents in an efficient and rapid manner;
- Apply appropriate corrective measures when necessary.

Many international multilateral, regional or bilateral instruments contribute to creating an appropriate legal framework for the security of road transport operations. The IRU has worked with international organizations, governments, Customs authorities and road transport operators to ensure the realisation of this framework.

However, it should be regrettably highlighted that, despite the significant efforts deployed at the international level to negotiate and approve international instruments, the number of contracting parties is often too limited to be effective even though most instruments are potentially global. In addition, their actual implementation is often either partial or incorrect, thus depriving the stakeholders of the full benefit of the foreseen facilitation and exposing the consignments to unnecessary security risks.

[13] The IRU is the world road transport organization that groups 180 members on the five continents. The IRU and its worldwide network of members have over 60 years of experience and expertise in facilitating and securing trade and international road transport.

Institutional framework and its contribution to road transport security

Several international multilateral, regional or bilateral instruments developed by various international organizations, (e.g. WCO, ITF and UNECE) aim at facilitating and securing international road transport of passengers and goods:

Regulations on access to the profession and market

Many regions and countries have developed legislation to regulate access to the profession in order to ensure that road transport companies meet necessary professional training and financial conditions, as well as good repute for the managers of those companies.

Contribution to security

These regulations have directly made the road transport industry more professional, reliable and qualified. By focusing on the professional competence and sustainability of the transport companies, these regulations contribute to reinforcing security in road transport.

Convention on the Contract for the International Carriage of Goods by Road

(CMR) Convention

The primary objective of the CMR Convention is to organize, in a harmonized manner, the contractual relations between the road transport operators, the shippers and consignees.

Contribution to security

Its contribution to security mainly concerns provisions relating to the consignment note that should accurately describe the goods transported as well as the shippers and consignees, thus facilitating, in particular for control authorities, the identification of persons and legal entities, as well as goods, involved in a given transport.

Lost opportunities

The CMR Convention, which should be a global instrument, only has 55 Contracting Parties mainly in Europe, despite its proven contribution to harmonizing trade and transport practices even in a multimodal environment. The additional Protocol on e-CMR only has seven Contracting Parties.

ADR for transport of dangerous goods by road

The ADR Agreement regulates the international carriage of dangerous goods by road.

Contribution to security

The ADR directly contributes to increasing the overall security of transport of dangerous goods through appropriate identification and marking of goods transported and by imposing technical requirements for vehicles and professional competence certificates for staff involved in the transport of dangerous goods.

Lost opportunities

The ADR only counts 47 Contracting Parties. Despite its proven contribution to security, the enlargement of its geographical scope is clearly hampered by the fact that its title refers to “Europe Agreement”. States from other regions consider that the title limits the Agreement to Europe, which leads to non-harmonized national or regional regulations, which compromise global security.

Customs Convention on Containers

The Containers Convention allows the temporary admission of containers involved in international traffic, thus reducing to a minimum the related Customs procedures. This Convention also provides for sets of technical conditions that the containers should meet to benefit from an internationally recognised mechanism for their approval for transport under Customs seals.

Contribution to security

By providing the technical construction requirements to which the container must comply to be approved for transport under Customs seals. This Convention directly contributes to the overall security of the global supply chain.

Lost opportunities

This Convention has only 38 Contracting Parties.

International Convention on the Harmonization of Frontier Controls of Goods

The primary objective of the Harmonization Convention is to facilitate border crossings by harmonizing and coordinating the various types of border controls. Annex 8 of this Convention specifically refers to road transport.

Contribution to security

The Harmonization Convention also directly focuses on security aspects by encouraging its Contracting Parties to exchange information, share experience, organize joint border controls and ensure mutual recognition of controls.

Lost opportunities

This Convention only has 55 Contracting Parties, mainly in Europe. In addition, the implementation of the Annex 8, dedicated to international road transport, is not effectively monitored.

TIR Convention

The TIR Convention is the only global Customs transit system, which combines fiscal and Customs security by providing, on the one hand, the establishment of an efficient and cost-effective international financial guarantee system and on the other hand, appropriate mechanisms and procedures to ensure controlled access to the TIR System to allow secure multimodal door-to-door transport under Customs seals.

Contribution to security

The TIR Convention directly contributes to security of the global supply chain through its provisions related to the technical security conditions of the TIR vehicles and containers, the conditions and criteria to be met by the international road transport operators to be authorised to the TIR procedures, mutual Customs recognition of control procedures on accredited operators and the effective TIR IT Risk Management tools, as foreseen by the Annex 10 of the Convention and in line with international security regulations.

Lost opportunities

The Convention, which has 68 Contracting Parties, is only implemented in 57 states. Its global scope and its ability to handle multimodal transport have not been promoted sufficiently at international level. As such, its contribution to global security of the supply chain could be even greater if expanded to other regions.

WCO SAFE Framework of Standards and related regional or national legislation

The WCO SAFE Framework of Standards, while not an international treaty, is the international reference for global supply chain security. As such, its provisions related to advanced cargo information, authorized economic operators' programmes, risk management are of direct relevance for international road transport operators.

Lost opportunities

The WCO Safe Framework of Standards is not a legally binding document and does not provide for mutual recognition principles. Its implementation is left to the discretion of national authorities and mutual recognition of security programmes is entirely dependent on bilateral agreements.

International Road Transport Union (IRU) tools for ensuring security in road transport

The IRU and its members have developed a variety of tools aimed at facilitating the task of road transport operators to comply with security regulations and to reach a required level of security.

IRU Road Transport Security Guidelines for goods and passenger transport (www.iru.org/en_services_checklist)

These IRU voluntary guidelines address both terrorist related and conventional security (theft of cargo and vehicles, attacks on drivers). The Guidelines are for managers of road transport companies, drivers, shippers/consignors and companies transporting dangerous goods by road.

The IRU Road Passenger Transport Security Guidelines include general recommendations for the managers of bus and coach companies and their drivers on improving security in day-to-day operations. IRU checklists for truck, coach and taxi drivers list tips and best practices to ensure the highest security and safety standards at all times.

Basic International Incident Report Form (BIIRF) (www.iru.org/en_biirf_public)

The IRU has defined a Basic International Incident Report Form (BIIRF) to assist drivers and road transport operators in reporting any incident that was faced during a road transport operation in a standardised and organised manner to police and competent authorities. This BIIRF is available for easy reference in several languages on the IRU website and is increasingly used and recognized as a useful tool by both operators and authorities.

TRANSPark (www.iru.org/transpark-app)

One of the main preoccupations of road transport operators, including compliance with driving time regulations, is to be able to find and use secure parking areas in order to avoid exposing drivers, goods and vehicles to theft and intrusion. To that end, the IRU, in partnership with the International Transport Forum (ITF), has developed TRANSPark: an online tool, which is accessible free of charge by road transport operators via the IRU and the ITF websites. TRANSPark is also available for Smart Phones for ease of use from the truck cabin. TRANSPark enables truck drivers, logistics planners, transport managers and others involved in road transport operations to search, locate, select and contact truck parking areas in over 40 countries – from Portugal to Kazakhstan. TRANSPark users can search for truck parking areas by country, around a location within a 100-km radius or along their planned routes. All facilities available at the selected parking area are listed (security features, truck repair, vehicle wash, hotel, restaurant, etc.), and can be used as parking search criteria. Full contact details and location maps are also provided.

Lost opportunities

The required data on the location of secure parking areas is not systematically transmitted to the ITF/IRU, thus limiting the positive impact and contribution to security of this free of charge tool.

IRU Border Waiting Times Observatory (BWTO) (www.iru.org/bwt-app)

Facilitation of border crossings and reduction of border waiting times are of course one of the main preoccupations of road transport operators, not only for economic, social and environmental reasons, but also for security purposes. Indeed, long waiting times at borders in a non-secure environment exposes drivers, vehicles and goods to a high risk of theft, intrusion and violent attacks, seriously compromising the security of shipments. To assist road transport operators and authorities, the IRU has developed the IRU Border Waiting Times Observatory (BWTO) as a practical tool used to identify congested border posts and organize operations in an optimal and secure manner. Data is compiled from Monday to Friday, from information mainly supplied by IRU national associations.

Lost opportunities

Despite the online capability of this application, which allows real time updating and a worldwide coverage, the required data are not transmitted systematically for many key border posts thus limiting information available.

IRU TIR Electronic Pre-Declaration (IRU TIR-EPD) (www.iru.org/en_iru_tir_epd)

In response to the increasing demand for electronic transmission to Customs authorities of advanced cargo information for Customs and security purposes, as provided by the World Customs Organisation's SAFE Framework of Standards and regional and national regulations, the IRU has developed, in partnership with many Customs authorities, the IRU TIR Electronic Pre-Declaration application (IRU TIR-EPD). TIR-EPD facilitates the submission of TIR electronic pre-declarations by the authorized TIR Carnet Holders in a simple and standardised way through this free of charge TIR Single Window application. The IRU TIR-EPD is already operational in 23 countries, namely: Belarus, Belgium, Bosnia-Herzegovina, Bulgaria, Czech Republic, Estonia, Finland, France, Georgia, Germany, Hungary, Latvia, Lithuania, Moldova, Poland, Romania, the Russian Federation, Serbia, Slovakia, Slovenia, Turkey, Ukraine and Uzbekistan.

It should be noted that the implementation of the TIR-EPD in the Republic of Belarus has now opened facilitated and more secure road transport operations with the entire Customs Union between Belarus, Kazakhstan and the Russian Federation, enabling TIR Carnet holders to submit advance cargo information to these three countries, free of charge. The IRU TIR-EPD contributes to increasing security in road transport by allowing Customs authorities to receive advanced cargo information from TIR authorized operators and allows them to carry out their risk analyses and risk assessments in advance of the presentation of the vehicles and goods transported.

Lost opportunities

While TIR-EPD is operational in countries representing 94% of TIR volume, the fact that TIR is implemented in only 57 states limits the global security benefits which can be provided by TIR and thus TIR-EPD.

Real Time SafeTIR (RTS) (http://www.iru.org/en_rts)

SafeTIR is the IRU's response to the UN Recommendation of 20 October 1995, to better manage and control the use of TIR Carnets. In 2006, Annex 10 of the TIR Convention was adopted, making the SafeTIR procedure mandatory for Customs. Real Time SafeTIR (RTS) was developed by the IRU, in partnership with Customs authorities, to automate in real time the exchange of data foreseen by Annex 10. RTS also provides Customs authorities, through computer to computer connections, with up-to-date information on the TIR Carnet's status and validity for the prompt detection of possible irregularities and risks for security. Several Customs authorities worldwide have already successfully integrated the Real Time SafeTIR into their Customs IT systems. Customs from Azerbaijan, Bosnia and Herzegovina, Bulgaria, France, Georgia, Kazakhstan, Moldova, Morocco, the Russia Federation, Serbia, Turkey, Ukraine and Uzbekistan are already benefitting from the increased security provided through RTS.

Lost opportunities

Despite its proven contribution to security of international transport and despite the provisions of Annex 10 to the TIR Convention, the implementation of RTS is hampered by the absence of international public support and is left to bilateral initiatives, which slows the process dramatically.

WCO-IRU TIR Distance Learning Package (www.iru.org/en_iru_tir_seminar_customs#1)

In order to develop capacity building to facilitate online training of Customs officials, national Associations and transport operators and to ensure a harmonized implementation of the TIR Convention, the IRU, in partnership with the World Customs Organization (WCO), has developed a TIR Distance Learning Package. This Distance Learning Package consists of 15 modules that cover the fundamental elements of the TIR system and, in particular, its main security features. Customs authorities can access the modules on the WCO website.

Strengths, weaknesses, opportunities and threats in the area of road transport security

General and global perspective

From a general and global point of view, the strengths, weaknesses, opportunities and threats in the institutional framework governing road transport security could be summarized as follows:

Strengths: the institutional framework and the tools to implement it exist. They have demonstrated their capabilities to efficiently facilitate and secure international trade and transport. Those multilateral instruments and tools are global.

Weaknesses: despite the global scope of the institutional framework, the number of Contracting Parties to the multilateral instruments is still limited and mostly concentrated in Europe. This European focus led the other continents to understand that the existing multilateral instruments were not relevant to them and national or regional solutions were developed independently, thus impeding appropriate global harmonization of rules and procedures.

Opportunities: the existing global instruments are easy to implement and experience as well as know how are available to assist all countries that would want to join and implement them. The wider implementation of the existing global instruments would have a major impact and a significant contribution to global security.

Threats: the economic and financial crisis situation, as experienced since 2008-2009, may favour protectionism and unilateralism, which could win over multilateral solutions. As such, there is a direct threat of governments choosing to develop national or even regional regulations, multiplying the number of national AEO and security programmes. This will lead to an infinite variation in security data requirements, which are concrete and direct obstacles for international road transport operators. This non-harmonized proliferation of security regulations and requirements only results in a multiplication of unnecessary procedures to be carried out at borders, creating waiting times and unnecessary risk exposure for vehicles and consignments, thus jeopardising global supply chain security.

This general and global overview of strengths, weaknesses, opportunities and threats can be further detailed as follows.

Uncoordinated initiatives and dispersion of efforts

Security of the global supply chain has become a priority issue for all involved. However, over the past few years, a multitude of initiatives have emerged in this area under the uncoordinated leadership of a number of international, regional or national institutions.

These uncoordinated initiatives are generating dispersion and duplication of efforts, jeopardising concrete, coordinated and harmonized measures to be adopted globally.

Furthermore, this dispersion of initiatives and efforts seriously compromises the ability to define globally agreed measures and even more importantly, impedes international mutual recognition.

Promote and implement what exists instead of reinventing the wheel

The above-mentioned uncoordinated initiatives and the resulting dispersion of efforts very often result in the definition of completely new systems or mechanisms, which ignore the already existing, tried and tested tools and mechanisms, which have demonstrated their effectiveness in securing the global supply chain.

Implement multilateral mutual recognition of Customs security programmes instead of bilateral Agreements

The WCO SAFE Framework of Standards establishes the basic principles to be respected to set up Authorized Economic Operators' programmes. However, the WCO SAFE is not an international treaty that countries have to respect and as a consequence, neither provides legally binding provisions to ensure mutual recognition of controls nor mutual recognition of AEOs.

Indeed, the implementation of the WCO SAFE Framework of Standards, as well as AEO security programmes, is only achieved through the goodwill of countries which are committed voluntarily to adjust their national legislation to align it with the WCO SAFE principles. Accordingly, the US has developed the CTPAT Program, the EU has modified the EU Customs Code (Modernised Customs Code), and EU member States, on this basis, have adjusted their national legislation. Canada, Japan and New Zealand have implemented similar reforms.

However, while these national (and regional) security and AEO programmes have been developed to reflect the same (WCO SAFE) principles, each programme has its own national (and/or regional) style – which results in quite different conditions, procedures, methods and approaches being applied across the globe. These differences are a direct result of the non-binding nature of WCO SAFE. The mutual recognition of national security and AEO programmes, in the absence of multilateral legally binding rules, can only be achieved at bilateral level through bilateral negotiations and agreements. This will mean, in practice, that an economic operator established in the EU who does business in China, India, Japan, New Zealand, the Russian Federation, the United States of America and so on, would have to comply with a multiplicity of bilateral agreements to have their AEO status recognised by all their trade partners. Despite the efforts of the WCO to define guidelines to assist countries in negotiating bilateral Agreements for ensuring recognition of respective AEO programmes, no international multilateral mechanism is envisaged to date. Therefore, each country will have to negotiate with all its main trade partners bilateral Agreements to ensure mutual recognition of AEO programmes at bilateral level, meaning that worldwide, thousands of bilateral mutual recognition Agreements will have to be negotiated and agreed and later on implemented.

Indeed, the issue of multilateral mutual recognition of AEO programmes is crucial to ensure, on the one hand, a high level of security within the global supply chain and on the other hand, avoid distortion of competition or even exclusion from the market for the operators that would not qualify for such programmes. The absence of internationally agreed mechanisms to ensure mutual recognition of AEO programmes may have dramatic consequences on the fluidity of international road traffic, border congestion, and jeopardise the overall objective of increased security.

However, this situation could be facilitated through a multilateral mechanism for mutual recognition of national security and AEO programmes. The TIR Convention is based on mutual recognition as well as the authorisation of operators which is internationally recognised. It also mirrors most of the WCO SAFE principles. Through making limited adjustments to the TIR Convention (for example through a new Annex on security) a "TIR operator" could be granted the additional status of "AEO/TIR operator" that would, by virtue of the mutual recognition principle of the TIR Convention, be recognised by all the Customs Authorities of the TIR Contracting Parties. Such a mechanism would be particularly beneficial to international traders in Europe, Central Asia, the Middle East and Africa, where multiple borders often need to be crossed – as it would avoid the need to comply with numerous (and possibly conflicting) bilateral agreements and accreditation processes.

The increasing need for the provision of electronic declarations to Customs authorities requires harmonization of data and communication protocols

One of the main components of security policies is the provision by traders of data electronically to allow competent authorities and, in particular, Customs to undertake in advance a risk analysis and risk assessment for each and every consignment. For some years, these new obligations have been implemented nationally or regionally. However, despite the adoption of the "Data Model" by the WCO, implementation at national and regional levels is not harmonized. As a result, international operators are faced with a variety of non-harmonized Customs systems and even worse with non-harmonized data requirements. This situation forces road transport operators to carry out unnecessary procedures at borders, thus creating unnecessary waiting times and exposing goods, vehicles and drivers to unnecessary security risks.

Security requirements must not jeopardise the facilitation of trade and international road transport

An appropriate balance between security and facilitation should be maintained in all security initiatives. Security compliant road transport operators should be granted with sufficient facilitation benefits, in particular through preferential treatment at borders, such as through the use of green lanes, in particular, when they operate under TIR.

Way forward and key recommendations

The implementation of the following key recommendations could ensure an appropriate level of security in road transport to overcome the above mentioned weaknesses, threats and challenges:

Ensure international coordination for transport security

A multitude of security requirements and programs jeopardise road transport operator's abilities to deliver their services in a timely and economically viable manner.

All security initiatives should be either:

- concentrated under the competence of a global international intergovernmental organization; or
- coordinated appropriately amongst the various international organizations and agencies involved.

Develop appropriate cooperation and coordination amongst authorities and road transport representatives at the national level

The prevention and efficient fight against transport security crime acts of all nature needs the bring together representatives of the police, judicial, tax and Customs authorities, as well as representatives of the road transport industry. They could implement mechanisms aimed at identifying and punishing the perpetrators of transport crimes.

Promote the existing international instruments

All actors at the international, regional and national levels, involved in transport security, should promote the implementation and enlargement of the geographical scope of the key international multilateral instruments contributing to increased security in international trade and transport.

In particular:

- Rules and regulations for access to the professional market;
- CMR Convention;
- ADR;
- Customs Convention on Containers;
- International Convention on the Harmonization of Frontier Controls of Goods;
- TIR Convention.

Organize multilateral mutual recognition of security programmes through existing multilateral international instruments

The US Chamber of Commerce Study (available from the UNECE website www.unece.org/fileadmin/DAM/trans/bcf/wp30/documents/ECE-TRANS-WP30-2009-01e.pdf), concluded that the TIR Convention was one of the most appropriate international multilateral instruments used to ensure mutual recognition of security programmes. As foreseen by the WCO SAFE Framework of Standards, TIR Contracting Parties and UNECE Secretariat, in partnership with the IRU, should urgently draft the necessary amendments needed to allow the TIR Convention to be fully compatible with the WCO SAFE Framework of Standards requirements.

Such adjustments to the TIR Convention would, at least, provide TIR Carnet Holders that qualify for the additional security requirements, an international mutual recognition of their TIR and security status that is equivalent to AEO.

Jointly promote the use of the existing IT tools developed in Public-Private Partnership to contribute to increased security of international trade and road transport

All actors involved should promote at the international, regional and national levels, the use of these tools developed by the IRU with many governments and authorities. They are available free of charge to transport operators and governmental authorities and would facilitate and secure international trade and transport by reducing border formalities, border waiting times and thus contribute to increasing global supply chain security. In particular, efforts should be undertaken jointly by national authorities and national road transport associations to:

- Ensure the timely provision of data to the Border Waiting Times Observatory (BWTO);
- Systematically provide data on the location of secure parking areas through the TRANSPark application;
- Ensure the deployment of TIR-EPD and RTS in all TIR Contracting countries.

Railway security is a fairly new concern which is gaining in importance, be it from the point of view of passengers, staff, goods carried by rail or from the point of view of the intellectual or physical property of the transport company or the state to which it belongs.

4

Rail transport security

Mr. Jacques Colliard | Manager, Security Division | International Union of Railways (UIC)

The notion of security encompasses all malevolent acts against which railway companies, infrastructure managers or owners and operators need to take preventive action – ranging from ordinary damage and everyday delinquency to highly orchestrated acts of terrorism.

The railway sector, in general, is very much aware of the need for a satisfactory level of security. As a reflection of this, the first UIC world congress on security was held in Madrid in 2000 under the heading "Security and the stakes at play" and whose purpose was to demonstrate to railway companies the importance and urgency of taking action.

Contrary to railway safety, which rests mainly on the way railways are organised and is governed by clearly defined standards set by specific bodies, security is shared by railway companies, the State and competent international organisations. The latter therefore depends on the implementation and fostering of suitable cooperation, as well as partnerships between the various players. Security should not create distortion in the competition between transport modes.

General passenger and staff security must also be guaranteed within certain limits in order to ensure respect of privacy. As such it can only be assured if people opting for one of a selection of possible modes of transport for a single journey accept certain constraints.

Security of ordinary or hazardous freight transport is limited by transport profitability and minimum cooperation between all players in the logistics chain – from the initial consignor to the final consignee. Security should also contribute towards punctuality as consignees are particularly sensitive to timely delivery of their goods in good condition, given the way in which production is organised today.

Strengths, Weaknesses, Opportunities, Threats (SWOT)

The strength of both freight and passenger railways is their capacity: two coupled double-decker high speed train sets, for example, can carry up to around 1,000 passengers at 300 km/h or more along some sections of its route. A suburban train at rush hour can carry over, 2000 people every 2 minutes along a single line when equipped with the necessary signalling and safety technology.

These facts illustrate the crucial role of railways in weaving social ties and creating the fabric underlying urban planning. As such railways form a target for terrorists seeking to destabilise the proper running of a country and its economy by launching attacks directed at symbols of technology and creating a maximum number of victims or aiming at sensitive goods.

The scale of transport flows, the size of installations and infrastructure are obvious security related weaknesses: the systems to organize security and technology that are available today are insufficient to guarantee security in the face of permanently changing external threats. The pressure of threat weighing upon the railways usually exists for reasons which are unrelated to the sector: nonetheless railway companies have the obligation to provide some means of safety for staff and customers, even if they cannot be held to account for all the consequences (which is not the case for safety).

Another strength lies in the continuing development of railway passenger transport: fast development of high speed lines and networks implies construction of new or completely renovated or reorganized stations, offering the chance to deeper the organisation of security into the system. It is always difficult to protect existing facilities and technically and financially more feasible to offer protection in a new service or one yet to be designed.

On the other hand, changes in transport mean that more players are involved in Europe and beyond in the transport chain requiring additional international cohesion in order to arrive at a satisfactory result before being able to think about moving onto further international consistency. More players on the railway scene working alongside public organizations such as the police, the army, border guards, customs and other forms of transport mean that the overall system is vulnerable until each and every role is clearly defined, accepted and controlled.

Transport security institutional framework in the railways sector

Passenger railway transport is set to grow on a national level (urban or suburban traffic, regional or national traffic). International traffic may also grow if one takes into account the development of the high-speed network creating a tighter web of connections over a broader European and intercontinental area.

The future of railway freight lies in international corridors, in particular, between Europe and Asia: shorter journey times compared to maritime transport and the creation of new routes to previously inaccessible countries will be important (once transport security along the logistics chain can be satisfactorily guaranteed).

Railway infrastructure security also depends on a minimum level of cooperation in order to avoid being a detriment to interoperability of the end–to–end transport. The European Parliament and Council Regulation (EC) No. 1371/2007 dated 23 October 2007 on the rights and obligations of railway passengers confirms the right to secure transport.

Consistency should be guaranteed in the provisions set by the various players of railway sector players in different states within the European Union. Bilateral agreements, while being a step in the right direction, are not sufficient to ensure security throughout an entire journey if the route crosses more than two neighbouring countries or an external European border. Further consideration should be given to the latter, in particular for routes going eastwards. To this end, work with the OSJD on this subject is crucial.

Better security means more efficiency in crossing borders (e.g. common consignment notes) and control procedures for freight. Indeed, the credibility of Europe-Asia corridors is underpinned by reduced journey times, especially by punctuality of transport as well as the guarantee that loads are delivered in good condition. In this context, cooperation needs to be reinforced along the entire transport chain from the initial consignor to a final consignee.

There are examples of regional cohesion either in the form of structures or in practice. There is no guarantee however of a broader world consistency to face the increasing complex railway transport system. It is, therefore, crucial to deploy the means to take into account environmental constraints and incorporate priorities linked to sustainable development.

Transport security initiatives in the railways sector

UIC regularly organizes a world security congress covering general topics and holds seminars on more specific subjects in order to ensure exchange lessons gained through experience and good practices, and disseminate useful information. The growing audiences from railway companies and high level participants of these events demonstrates the relevance of such gatherings which save time in establishing one's own strategy of preparing for new external constraints.

Furthermore, future work planned in recent agreements signed by UIC and its involvement with large international organizations (eg. United Nations, OSJD) explicitly pave the way to ensure improvements in international railway security.

The latter should be reflected in the establishment of cooperation frameworks or suitable organizations, failing which it will become necessary to constantly reinstate the issue of international consistency in security policy on the agenda. Efficiency/inefficiency will be measured through progress in cooperation and its duration over the long term.

In other words, it is clear that the coordination of international railway passenger transport security along the same lines as civil aviation security organisation is crucial to foster the development of international traffic.

This could be in the form of an international authority: either new, or mandated to existing bodies, such as UN regional or thematic committees, working with the support of a professional structure such as UIC – which is the only world organization bringing together all aspects of the railway sector. Other competent organizations in the railway transport sector would also have a place in this framework depending on the development of their role in this area.

Taking into account the European Union's law on passengers' right to security, and other texts which may exist in other jurisdictions, it is clear that some thought must be given to producing an international document applicable in all countries incorporated into or in addition to existing local security policy. The latter would set a common minimum set of conditions, common standards for ensuring security in transport, leaving each state or company the freedom to take measures beyond that basic limit.

Given that international freight traffic is mainly concentrated to well-defined corridors, the proposal is to manage security on a corridor-by-corridor basis, resting on partnerships among authorities and railway stakeholders for each corridor as a whole.

For anti-terrorism, a joint programme of work should be launched with the help of the European Union Anti-terrorism Coordinator, with a view to extending this action to neighbouring countries, having adapted it to local conditions. Each state obviously could retain its sovereignty in relation to determining the route to be taken by information through the relevant specialized departments, in particular when it comes to intelligence, and for informing the railway sector in times of threat. The state is always responsible for validating the way in which anti-terrorism is organized, which will encompass railway players, especially when achieved through specialized plans.

A way forward, action plan

Ensure a "bottom-up" approach to use sector reality and constraints as a base, which are also an illustration of specific needs and demonstrate the purpose of solutions, and a "top-down" approach to raise sector awareness about policy decisions which may have been taken.

Examples:

- Passenger: UIC work on crossing Schengen borders in Europe; alternation between concrete field border point studies and discussions with the European Commission and with the Frontex Agency on the subject (possible form of special ID for cross-border traffic railway personnel);
- Freight: a study on the implementation of train safety tests applicable to trains about to enter into service on international corridors.

The objective would be to define a target organization, determine the roles of various political or professional international organisations with the appropriate competences in this field (regional or technical commissions, United Nations, OSCE, ITF, OSJD, WCO, ILO and perhaps others) and schedule policy decisions to be made in order to guarantee their implementation.

A core working group would then be tasked with steering this work. UIC, given its professional status, is ready to take an active role. UIC security related events, such as world congresses can also serve as a means to maintain the pace in steering this work and/or a congress can be specifically organized to deal with this topic: the 2012 congress may, in this respect be an opportunity.

Comments

Mr. Andrew Cook

Head of Land Transport Security
International Policy Development
Department for Transport, UK

This is a critique of the International Union of Railways paper titled Rail Transport Security. The paper introduces the subject of railway transport security, particularly passenger rail services, though it also considers freight traffic.

The point is made that railway security is a fairly new concern and specific reference is made to the Union of International Railways (UIC) conference on security held in 2000 in Madrid. Mention of the Madrid 2004 and London 2005 international terrorist bombings helps demonstrate the increased interest and concerns by governments (states), the public, owners and operators of railway networks in transport security. Most recently, in 2011 there were incidents in Germany from 'domestic' terrorism. It should be noted that the railway sector has been subject to many different types of aggression from very early times.

While terrorist activities are the most disruptive and severe acts of aggression, arguably that the definition of railway security should also encompass minor acts of social interference through to international terrorism. This would include graffiti, vandalism, metal theft, etc. Essentially, security could be defined as any act of unlawful interference. The section points out that the international railway organizations like Union of International Railways have been actively engaged in discussions on measures to prevent terrorist attacks and security more generally.

The paper does not set out the rationale for a broad definition of security but there are several arguments that could justify this. To make the definition of security too narrow would mean that the benefits gained from an integrated approach may not be achieved. Security countermeasures in one area can often reduce vulnerability in another. This is certainly the case for terrorist countermeasures, which tend to be more onerous and expensive. Given that these can be more difficult to justify from a pure business perspective, it is important to consider the wider benefit to security they provide for an organization, as well as society. Similarly security measures that help prevent antisocial behaviour like security patrols and Closed-circuit television (CCTV) could also deter terrorists.

This paper draws a distinction between railway safety and security. Safety standards are set by specific bodies and implemented by the railway sector. Whereas it is argued that security is a more shared responsibility between railway companies and the state, which necessitates the need for good cooperation. It is not clear why there is such a distinction, other than the absence of security legislation.

In examining cooperation, it would be useful to expand on the above statement. For example, at the strategic level there is a need for the state to make the railway sector aware of the threat from extremist activity so that the appropriate security measures can be set up. Often security is a matter for Home or Interior Ministry officials, while the main contact between state and rail operators is through transport officials. There is, therefore, a need for a three way dialogue. At a tactical level there is a need to share information between police and the railway sector who need to work closely together. The special nature of the railway sector means that there is a dedicated police unit or force assigned to it.

It is suggested that security should not distort competition between modes. Everyone should also expect a level of security but with accompanied certain constraints to privacy. The privacy issue is not expanded upon but would be defined by state legislation or more global rules. Perhaps the important point here on competition is that each mode should be subject to a risk assessment process to define the level of security necessary. Whether the level of risk would be the same across each mode also needs to be considered as does the specific threat circumstances in each state.

With a few exceptions, the rail sector, unlike aviation, is largely an open network. This is due to the large numbers of passengers and the relatively short journey times and travel. The security risk, therefore, has to be balanced with what the public would accept as proportionate measures. If the time taken to go through security is longer than the journey, this is unlikely to be considered acceptable – unless there was a very high risk of an attack.

Here, the section infers that the railway sector is aware of the need for satisfactory security. It goes to say that security is shared by railway companies, the state and competent international organizations. What is not highlighted is how this works in practice. There are arguments on both sides on who should be responsible and who should pay for those security measures. Some states take the view that it is the user that should pay while others consider that it should be either funded through a specific or general tax. For the rail sector, a further complication is whether or not it receives state subsidies.

Railway and infrastructure operators increasingly work on a business model where the needs of the board and shareholders dictate where money is spent. Security has to compete against other corporate initiatives. Even if money is available efforts are likely to concentrate on conventional and more obvious day to day problems such as graffiti, vandalism and metal theft rather than the less visible threat of terrorism. These are more easily justified to the Board of a company and shareholders – unless of course their company is attacked by terrorists.

There is reference to the lack of a global body or international standard to cover passenger railway security; however there is a standard for dangerous goods freight and this is mandated within Europe. It could be stated that there is an important distinction between the two regimes which is that dangerous goods are themselves hazardous and could be used as a weapon, whereas the passenger rail sector is actually a target for terrorist attacks or other criminal acts.

Strengths, weaknesses, opportunities, threats (SWOT)

This paper highlighted that the strength of rail transport is its ability to move large numbers of people and freight quickly. High speed rail services, whether as a direct competitor to aviation or not, are also expanding domestically and internationally. These large numbers of passengers and the economic benefits of railways make them an attractive target for certain terrorist groups. Not mentioned is the iconic nature of some infrastructure and the psychological impact of an attack, which together with their vulnerability adds to the attraction. Also, densely populated areas make the railways attractive to others that wish to commit crimes and increasingly stations contain retail and food outlets, which bring both increased revenue but also additional and competing demands on security.

Building new stations, and redeveloping existing ones, provides scope to improve security by embedding it into the project at the outset. In this way the costs are significantly reduced. To expand on this, hostile vehicle restraints, screening areas, clear sight lines and better CCTV coverage are all potential measures. Where practicable the building's design should be flexible enough to accommodate further technology developments such as screening of people. However there are limitations as major stations tend to be old and architecturally significant, so obtaining approval for such changes can be difficult. Because it is not always possible to prevent attacks, it is wholly appropriate for the rail sector to build in mitigation measures such as blast resistance features to reduce injuries and provide good access for emergency services.

The argument that there is no direct link between terrorism and the rail sector is correct but this can also be said for the other transport sectors. It is acknowledged throughout that the transport sector provides the right circumstances for terrorists to draw publicity for their political ideology. Nevertheless it is acknowledged that railway companies have a responsibility for the safety of passengers and staff.

Transport security institutional frameworks in the railways sector

The reference to freight corridors in particular between Europe and Asia as an alternative to maritime transport is highlighted in the paper. Suitable cooperation agreements, consignment notes and satisfactory transport security are all highlighted. The European Union's approved Economic Operator (AEO) scheme, which is designed to facilitate trade between the EU and other States, is not referred to. Also whether the OSCE has a role here is not expanded upon.

This paper points out that the railway passenger market in Europe becomes more complex with the separation of infrastructure, railway operators and security functions. This also applies, in some instances, to the role of private and state railway police. What is not mentioned is whether this is simply within the EU or something that is happening globally. The argument is put forward that bilateral agreements, while a step in the right direction, are not sufficient for the whole journey if it crosses several member States.

There is no illustration of how a multilateral agreement could work in the paper. The Channel Tunnel between the UK and France has a bilateral agreement in place. With the recent opening up of the market to other railway operators in Europe, the UK and France have begun discussions with a new operator and state authorities to ensure that appropriate and comparable security measures are in place for the new passenger railway routes through the tunnel.

An advantage of bilateral or multilateral agreements is that proportionate and appropriate security measures for risks are put into place for those countries concerned. But in order to achieve this there is a need for transparency, and a willingness to work with new operators and states and to prevent barriers. There is, therefore, a difficult balance between bilateral agreements that have different standards for different cross border rail services and a common approach to facilitate cross border rail services, through global standards and agreements.

Transport security initiatives in the railways sector

This section of the paper mainly describes the role of UIC in organizing a world congress on security and the dissemination of useful information. Progress continues to be made by forging agreements with other organizations. What is not clear is what role these organizations would have if a single global standard setting was taken forward as suggested in the next section.

The paper argues that to foster international traffic, the railway sector needs a body similar to a civil aviation security organization. This could be either a new international authority or through an existing one such as the United Nations. The suggestion is that a common set of base line standards be developed, but at the same time allowing each state or company freedom to put into place measures beyond the minimum. As freight traffic tends to be through defined corridors, the suggestion is that standards be managed on that basis with partnerships between authorities and railway stakeholders.

The railway operator organizations have examined the issue of security. One advantage of these organisations is that they are able to concentrate on delivering the most relevant initiatives for their respective areas but this is not highlighted in the report. It is clear that there are common areas of interest, for example terrorism and copper theft to name just two that affect them all. Collaboration between organizations has prompted good coordination and cooperation on initiatives such as European research proposals but has not fully met their needs.

There is no mention of the United Nations Economic Commission for Europe (UNECE), the European Union (EU) and the Organization for Security and Co-operation in Europe (OSCE) who have each reviewed land transport security. The consensus from the States involved in each of these reviews is the dissemination of best practice rather than mandatory requirements as the preferred option. Both the EU and UNECE continue to hold meetings which include dissemination of information.

There is also the International Working Group on Land Transport Security (IWGLTS), which was set up by the Group of Eight (G8) countries to specifically disseminate information between those States that have been the target or have an interest in terrorism. This group now includes twenty one states and several observer groups like UNECE, the EU and railway organizations such as UIC and UIPT.

The group's format provides for open dialogue between states but it is not designed to set international standards and has not, so far, disseminated information more widely than to its members and observers. In one sense, it is a global organization but without the remit to set standards as are being proposed in this paper.

In the aviation sector, the International Civil Aviation Organization (ICAO) sets international standards, while in maritime it is the International Maritime Organization (IMO). It could be argued that passenger railways are different in that they are not global in exactly the same sense. Railways tend to be categorised as urban, interurban (regional) and high speed. The latter includes both international and domestic travel.

The first two carry far greater numbers of passengers than high speed rail. The threat to, and cultures of, cities throughout the world can vary quite considerably. While international high speed railways span one or more borders, they would normally be on a continent, e.g. Europe, Asia, etc. – and not global in the same sense as aviation and maritime transport. Having said that, there are areas of common interest and in that respect they could be considered to be global.

The proposal set out in the paper is to have a single base line standard and still allow States to set rules above that. Whether this would be sufficiently flexible and worthwhile for states to sign up to is difficult to judge. In part, it would depend upon the appropriateness of the base line standard and how easy it would be to vary it by the states and operators. The reality could be that to reach an agreement the base line standard would be too low to be meaningful. It could mean that each state and company would introduce its own additional measures which could defeat the objective. Such a proposal would need consensus from all parties for it to work.

One aspect of security, the terrorist threat (both domestic and international), can vary quite considerably within a state, between states and continents. Many states also see the setting of security measures on their railway network as a matter of sovereignty because it is land based. To get states to sign up to a single global standard could be challenging.

One approach that has not been discussed is whether a 'tool box' or 'catalogue' of best practice measures could be compiled. This would be based upon is selection of scenarios, and it could include all acts of unlawful interference. A range of best practice – physical and operational measures – would be considered for each scenario together with mitigation actions that could limit the impact of an attack (e.g. equipment such as hostile vehicle restraint measures, operational techniques such as explosives, screening by dogs, searching, etc.).

A risk assessment would consider threat, impact and vulnerability. An important aspect of ensuring that they are robust and accurate, especially for the terrorist threats, would be ensuring that all relevant State and railway organizations are involved. By using a tool box approach States and operators would be able to choose the most appropriate measures for the scenario and risk. This can be carried out at a local level or if there are a number of States at a more global level. This type of approach could have the advantage of driving standards up rather than down to a common base line.

A way forward, action plan

The paper argues for both a bottom-up approach to understand the practical constraints and a top-down approach to raise sector awareness on policy decisions. It suggests setting up a core working group to define a target organization, determine roles and ensure policy decisions to guarantee implementation. The UIC would be willing to take an active role in this.

This section could benefit from better definition of what output is to be achieved and more in the action plan including a time line and milestones.

5

Security in inland waterways

Mr. Victor Vorontsov | Senior Expert, Russian River Register | Russian Federation

Since 2002, UNECE has been dealing with security in inland navigation by addressing transport and security issues within its various working bodies. Indeed, following a request by the Inland Transport Committee (ECE/TRANS/139, para. 19), the Working Party on Inland Water Transport (SC.3), at its forty-sixth session (22-24 October 2002), asked the secretariat to prepare a synthesis of the initiatives in the field of transport and security undertaken within international organizations concerned with inland navigation (TRANS/SC.3/158, para. 4).

Accordingly, the UNECE secretariat produced a document on the actions and activities undertaken within UNECE, ECMT, IMO, ILO, CCNR and ISO with a view to enhancing the security in inland navigation (TRANS/SC.3/2003/12).

In considering this subject, UNECE stressed from the very beginning, that it should avoid duplicating the work of other competent regional or international organizations.

Document TRANS/SC.3/2003/12 presents complete and interesting information, especially on steps already undertaken at the time within IMO, thus defining a general scope where work needs to be carried out in this area.

Further to this brief introduction, let us focus on the definition of the term “security in transport”. To my knowledge, the UNECE Working Party on Railway Transport was the first to provide a useful definition of safety and security by adopting the following two definitions at its fifty-sixth session in October 2002 (TRANS/SC.2/198, para. 6):

Railway safety – the socially required level of absence of risk of danger in the rail transport system where risk relates to personal accident, injury or material damage;

Security in railways – the protection of human beings, transport means and transport infrastructure against unauthorized and unexpected actions of any kind. The issue was quite new for UNECE and was not easy to deal with. At the same time, it was clear that, given the circumstances, it was to be tackled without delay.

That is why, following the example of IMO, the Working Party SC.3 decided as a first step to review main legal instruments of relevance to questions of security and requested its auxiliary body, the Working Party on the Standardization of Technical and Safety Requirements in Inland Navigation (SC.3/WP.3), to study a need for amendment of the European Agreement on Main Inland Waterways of International Importance (AGN), European Code for Inland Waterways (CEVNI), Recommendations on Technical Requirements for Inland Navigation Vessels (annex to Resolution No. 17, revised) and of any other UNECE instruments aimed at enhancing safety on-board vessels, both under way and in ports, and formulate its recommendations for further consideration.

Adoption by IMO of a number of efficient measures aimed at enhancing security and, in particular, amendment of SOLAS Convention of 1974 and adoption of the International Ship and Port Facility Security (ISPS) Code gave the Working Party SC.3 an idea to start considering of amendments to the AGN Agreement.

It was agreed, and without much discussion, to introduce into the preamble of the Agreement relevant additions underlining the importance of the issue of security and of the protection of the network of inland waterways. Currently, these additions or, to be exact, new formulations of paragraphs have already been adopted.

As to the substantive provisions, it was agreed that, based on proposals by Governments on the protection of the network of E waterways and ports from external influence, new Annex IV to AGN would be elaborated with the help of a consultant that would reflect the provisions in question.

It was envisaged that the Annex IV would contain general requirements applicable to the technical measures designed to protect inland waterway infrastructure (the waterway itself, navigation signs and marking as well as hydraulic works such as locks, bridges and other facilities along the waterway, port complexes and so forth) from intentional external influence that might cause harm to navigation.

Proposals from Belarus, Belgium, Republic of Moldova, United Kingdom, Ukraine, European Commission, Danube Commission and European Barge Union had been received during the forty-ninth session of the SC.3.

The analysis of the information received demonstrated different approaches to the issue and, first of all, revealed a concern that the measures taken should not become an unbearable burden for inland water transport.

Information from the Danube Commission particularly emphasized that it would be difficult to reach any tangible results since the structure of existing national services responsible for emergency operations differs considerably.

Other proposals underlined that it would be unreasonable in inland navigation to follow the provisions of the ISPS Code in full.

Nevertheless, in spite of difficulties, the work within UNECE went on and by the fiftieth session of the SC.3 (11-13 October 2006), a draft of the Annex IV was presented (prepared by the secretariat with the help of a consultant (document ECE/TRANS/SC.3/2006/7/Add.1)).

Its content is as follows:

“Annex IV

Protection of the Network of Inland Waterways of International Importance from the Intentional External Influence

Inland waterways used for international shipping and their infrastructure should be adequately protected from intentional external influence that might cause harm to navigation, health and human life as well as to the environment.

The Contracting Parties, governmental bodies, local authorities and basin administrations, shipping companies and ports should take effective measures with a view to revealing the threat of, and preventing, the intentional external influence that might cause such harm.

The implementation of such measures shall require the development, on request by the Government of a Contracting Party, of relevant security plans for inland waterway infrastructure and ports that should provide for the security of the above-mentioned objects and of the vessels situated on them.

These plans should contain as a minimum:

- measures designed to prevent unauthorized access to the area of the port through organizing physical protection, installation of barriers, fences and technical means of control;
- measures designed to prevent weapons or any other dangerous substances intended for use against persons, vessels or ports and the carriage of which is not authorized, from being introduced into the port or on board a vessel;
- measures designed to supervise and effectively control the shore-based and floating aids to navigation, their sources of energy and other supplies by using mobile means of control and other techniques;
- procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port or vessel/port interface;
- measures designed to ensure an effective liaison and coordination between the port authorities and responsible ship’s officer and the consistency of security activities of port authorities and crews;
- procedures for evacuation in case of security threats or breaches of security;
- duties of port personnel assigned security responsibilities and of other port personnel on security aspects;
- procedures for interfacing with vessel security activities;
- procedures for the periodic review of the plan and updating;
- procedures for reporting security incidents;
- identification of the port security officer;
- measures to ensure the security of the information contained in the plan.

Port security officers and appropriate port security personnel shall have knowledge and have received training, taking into account the provisions in paragraph 4 above.

The port security assessment is an essential and integral part of the process of developing and updating the port security plan. The Government of a Contracting Party within whose territory the port is located shall carry out this assessment. The Contracting Party may authorize a recognized security organization to carry out the security assessment of a specific port.

The port security assessment shall be reviewed and updated".

The draft of Annex IV to AGN was studied in the course of several sessions of the Working Party on the Standardization of Technical and Safety Requirements in Inland Navigation (SC.3/WP.3), was approved as an optimum version and was transmitted to the Working Party SC.3 at its fiftieth and fifty-first sessions (11-13 October 2006 and 17-19 October 2007) for consideration.

At its fifty-first session, SC.3 observed that although no comments or proposals on the draft Annex IV had been received from member Governments it would be premature to adopt the provisions of the draft before ensuring their correspondence with relevant initiatives undertaken within other competent bodies, such as EC and IMO. Since then, this important document has been shelved within UNECE due to lack of final approval.

In parallel with the work on amendment of AGN the Working Party SC.3 introduced certain amendments to CEVNI and to the annex to Resolution No. 61 "Recommendations on Harmonized Europe-Wide Technical Requirements for Inland Navigation Vessels". This work is ongoing, particularly on passenger vessels.

It is worth noting that, in the meantime, a number of measures of a legislative character have been undertaken in certain member countries aimed at ensuring security in the field of transport. Since the hydraulic works on inland waterways (such as locks, dams, bridges) are protected, as a rule, by specialized security services independent from ship owners or from waterway administrations, the proposals from member countries transmitted to the secretariat usually speak of protection of vessels and ports from unauthorized intrusion and possible illegal acts.

Here in addition to the above-mentioned draft Annex IV, a proposal from the European Barge Union represents a certain interest (TRANS/SC.3/2005/4). The proposal gives a comprehensive description of the existing situation and at the same time contains a concise draft document on security in inland navigation inspired by the ISPS Code.

Here are the main provisions of the document submitted by the European Barge Union:

Introduction

The inland shipping industry is a professional sector which takes its responsibilities in the field of terror prevention and therefore gladly participates in the development of the Intermodal Directive.

Basic assumptions/principles

In the development of this Directive, the inland shipping industry departs from the assumption that the security measures to be taken should be realistic and proportional.

In other words:

- The security measures should actually make a meaningful contribution towards security, so no 'paper tiger';
- The security measures must be transparent and clear;
- Where possible they should fit in with already existing quality systems, procedures and rules;
- It must be taken into account that an inland navigation vessel is not only a floating company, but also a floating home;
- The measures should lead to minimal extra (administrative) burden for the sector;
- Uniformity of the measures, Europe-wide, both within the ports and on terminals, is a 'must'.

Security measures can be used as an opportunity to improve the position of the inland shipping sector. By enhanced co-operation between carriers, governments, shippers and other parties involved, 'secured lanes' can be developed which may benefit all parties in the logistic chain.

Objective of the security measures

The aim of the security measures is to prevent unwelcome persons and goods from getting on board.

Possible measures for the inland shipping sector

The inland shipping sector is, by nature (a vessel is not only capital equipment but also a residence) and because of its economic scale (a relatively large volume of cargo per transport unit), an intrinsically safe transport mode.

Therefore, the sector is able to reach a high level of security by taking relatively simple measures. The possible measures can be divided into the following categories:

- Physical security of a vessel and its crew;
- Organization/procedures;
- Communication;
- Creating awareness.

The most important measures can be summarized in the following central points:

Defining responsibilities

Each company has to nominate a security officer. The security officer is responsible for:

- an index of the measures being available on board;
- all measures being well known by the crew-members; and
- all measures being observed.

The security officer has to be familiar with the measures for the protection against terrorist attacks in other transport modes (e.g. ISPS Code).

In addition, responsibilities are assigned to the persons, who possess the required competences and qualifications and are equipped with the necessary authorities.

Estimation of the dangers potential

Each company has to work out a self-estimation of possible threats based on the nature of the goods and on the waterways used and has to adapt the measures if required. The standard processes are to be valued with regard to possible threats.

Securement of the vessel

The vessel has to be secured with operational, technical and organizational measures against improper use. The vessel has to be inspected at regular intervals with respect to suspicious persons and goods.

Access control

The stay of unauthorized persons on board is prohibited. On board of each ship a list is available with people actually being on board and with the people normally on board. Persons who intend to proceed on board because of official or personal reasons have to indicate so beforehand. Both crewmembers and persons who are on board only temporarily have to be able to prove their identity with a photo identification card on demand. In areas with a temporary or permanent threat certain zones of the ship have to be blocked for non-crew-members.

Creating awareness

The staff has to be instructed regularly about the measures for terrorism prevention and the required behaviour in the event of an attack.

Communication of observed suspicious behaviour

Observations of suspicious behaviour and security-related events have to be communicated immediately to the responsible authorities.

Checking of the reliability of contracting partners

Before a company enters into new business relations with suppliers or subcontractors (within or outside the logistic chain) their reliability has to be checked.

Documentation of measures

Staff instruction dates must be documented as well as the names of the participating persons. Reports with possibly security-related observations have to be documented.

Observance of secrecy

Specific measures against terrorist attacks (e.g. silent alarm, fixing of a code word in case of terrorist attack) have to be kept secret.

Observing the security level

The security officer has to be familiar with the measures for the protection of logistic chains against terrorism. The security officer informs himself regularly, whether there is a special threat on the waterways or in the harbours, to which a vessel is steaming up. The persons on board have to be informed immediately about special danger situations.

Observance of the measures

The security officer has to check regularly in a suitable manner that the crew members are informed about measures against terrorist attacks and that the measures are observed.

Finally, it should be noted that the two documents mentioned above could become a subject for discussion at the OSCE-UNECE Transport Security Forum in Vienna as most practical ones. A delay in their adoption is due to some extent to the position of the European Community.

Comments

Dr. Istvan Valkar

Secretariat of the Danube Commission

It can be stated that the paper quoted by Mr. Vorontsov provides a comprehensive overview of the state of affairs and represents a good answer to the question of where we are. All the activities carried out in the framework of the UNECE, are outlined with insight on the works done in other international organizations. The key conclusions that can be drawn are:

- the threat which may be caused by terrorist actions is estimated by the stakeholders of the inland waterway transport as being relatively moderate;
- security-related measures shall be cost-effective and shall not cause disproportionate financial and/or administrative burden for the actors of the inland waterway transport system;
- preventive measures shall be developed and introduced in the first place.

The Danube Commission maintains the item of security of the Danube inland waterway transport on its agenda as well. The Commission has not adopted any related recommendations so far. Nevertheless, it can be found that a considerable unity exists among the international organizations concerned, particularly concerning the approaches and methods of dealing with problems of the inland waterway transport security. Commission experts have been elaborating a document called “Declaration of Security” in the framework of an international working group since 2007. This group pays – among others – special interest to the rules adopted by IMO which serve as a starting point to set out recommendations for the Danube. Beyond that, it takes into account the existence of the so-called “maritime Danube” in the estuary region of the river, where the IMO rules shall be applied. As far as the Danube Commission is entitled to deal with the infrastructure of the Danube navigation, recommendations can be developed to ensure an appropriate security level of this infrastructure. The outcomes of works done by the UNECE and the European Commission have to be taken into consideration in this respect.

All further activities aiming at strengthening security of the inland waterway transport on the Danube may be based – among others – on the following considerations. It shall be recognized that inland waterway transport has never been the target of a serious terrorist attack. Generally speaking, inland waterway transport seems not to be a ground for preparing or developing terrorist activities. It can be noted that the same also applies for Danube waterway transport. In addition, the Danube as such and the navigation on the Danube enjoy a very good, peaceful image – it is enough to refer to the well-known “Blue Danube feeling” which has been so impressively reflected in the music of Richard Strauss.

Terrorist activity is a very special kind of crime. As a rule, terrorist movements communicate to the public ideology (or “philosophy”), are organized and have their own prepared activists to commit attacks. This is why the terrorist action can be distinguished from other unlawful acts such as the robbery (theft) for instance. The intention of establishing an effective and proportional security system for the Danube waterway transport needs an overview into the “spirit” of terrorism and its possible link to the inland waterway transport. First of all we have to learn that terrorist movements have more or less clearly defined aims at an ideological and/or a political level, consequently, the violence of terrorist attacks are not the goal but merely the tools to reach the principal aims.

As far as inland waterway transport is concerned, from the point of view of the terrorist groups, it may be an option target or serve as a means of accomplishing actions. It is important to see that while a general scheme of a potential link between the terrorism and the inland waterway transport can be formulated, concrete threats and options for a particular waterway have to be defined separately.

Special attention shall be paid to the transport of dangerous goods on the Danube as being a potential threat to the environment. Having in mind possible terrorist attacks, a ship carrying dangerous goods may potentially be used in the role of a weapon. On the other hand, however, it can be recognized, that it might be very difficult to explain to the public the meaningfulness of an attack on the Danube environment – even on the grounds of the principal goals and drives of a terrorist group.

It is self-explanatory that passengers on - board a cruise ship might be endangered if hit by a terrorist action. At the same time existing tools aiming to keep security on the required level – at least for the time being - can be assessed as working properly.

An eventual use of the Danube navigation as a "Trojan Horse" might pique the attention of terrorist movements. Indeed, transport of containers, as well as passengers on - board cruise ships and also ship personnel might provide an opportunity to smuggle weapons and/or activists in to the area of a planned action. Apart from how we evaluate the probability of the Danube subregion being a target of a terrorist attack, the case of the "Trojan Horse Effect" must be carefully analyzed.

We have two possible options to keep the risk level for the Danube water transport as low as possible: strengthening the self-defence abilities of the region against terrorism – that means to minimize the threats – on the one hand (task at a political/governmental level) and to minimize the vulnerability of the Danube water transport on the other hand (that represents a task of the competent administrations, responsible for the inland waterway transport).

The importance of the EU Strategy for the Danube Region as a general framework that can contribute to stabilizing the terrorism-related risk along the Danube to a very low level has to be stressed expressively. Achievement of the principal goals of the Strategy, namely the development of the Danube region as a region of welfare, mutual understanding between people and cultures, peace and tolerance can ensure a base for high-level security.

The development of RIS along the Danube can become a further powerful tool for minimizing the terrorism-related risk on the Danube. Communication options, ship tracking and tracing provided by RIS, indeed, can lower the vulnerability of the Danube navigation.

A specific situation may arise in the transport of dangerous goods, passengers and containers on the Danube. On one hand, the development of these kinds of transport activities can offer an outbreak point for developing the Danube water transport. For this, transport of containers, passengers and dangerous goods represents a segment of the Danube water transport market which has large and promising development potentials. On the other hand, even this possible and desirable development may have a negative effect in terms of the Danube water transport security. This is why the development potentials on the Danube must be evaluated carefully, keep in mind the complexity of the market and security aspects.

Poor infrastructure conditions of the Danube navigation are unfavorable not only in terms of the economic performance of waterway transport but also on its security. Interruptions of the transport flow caused by navigational hindrances may have an effect that Danube navigation become at some extent assailable.

Last but not least, the importance of international cooperation in the field of security has to be underlined. Prevention should be the primary aim of this cooperation since the most effective strategy in this respect is to keep the threat away.

Institutions: Barrier or Enabler for Inland Transport Security

Dr. Garland Chow | Associate Professor, Sauder School of Business
Director, Bureau of Intelligent Transportation Systems & Freight Security (BITSAFS – Sauder)
Associate, Centre for Transportation Studies University of British Columbia, Canada

Background and Scope of Discussion

Trade and exchange are particularly important for a trading nation like Canada. Its number one trading partner is its U.S. neighbour to the south, bilateral trade with the U.S. exceeding $500 billion in 2010. There is more exchange of goods and services between Canada and the United States of America than between the 10 provinces and 3 territories within Canada. Like many other developed countries, Canada has increasingly sourced manufacturing from low-cost countries in Asia, such as China. Canadian ports of entry were efficient competitors to U.S. ports, as the port of entry for imported goods to the U.S., just as U.S. ports are competitors to Canadian ports for imports to Canada. As a result, the Asia Pacific Gateway and Corridor (APGC) has become a primary land transportation corridor connecting Asia to the U.S. and Canada (see Figure 1). In addition, highly integrated regional economies – for example, in the Pacific Northwest and the Great Lakes regions – have developed along the 8,891 km U.S.–Canadian border.Specific industries are spatially integrated across both countries, e.g. the automotive sector, where a vehicle can cross the U.S.–Canadian border 5 times during assembly. Finally, the North American Free Trade Agreement (NAFTA) led to the continentalization of production–distribution networks across Canada, the U.S. and Mexico. Major north-south highway and rail corridors serve the North American trade network connecting all three countries (See Figure 2 for highway corridors). These include the Cascadia Corridor that connects Western Canada with the U.S. Pacific Northwest, and the West Coast Corridor, which connects Western Canada with the Western United States

Global, continental and regional trade requires the efficient and effective movement of goods, services and people; otherwise the gains from trade are lost to the transaction costs of exchange. There was an immediate outcry for tighter enforcement of immigration and customs regulations immediately after 11 September 2001, which “thickened” the border, leading to higher costs and greater uncertainty for freight crossing the borders. The impact was particularly hard for southbound Canada to U.S. movements, for both freight, which originated from off-shore or from within Canada. The private sector felt the impact immediately, and stakeholders in national and local levels of government realized the urgent need to take action on securing the border, while minimizing the impact on trade. Canada and the U.S. signed the Smart Border Declaration and Action Plan (also known as Ridge-Manley agreement) on 12 December 2001.

Figure 1 **Asia-Pacific Gateway and Corridor**

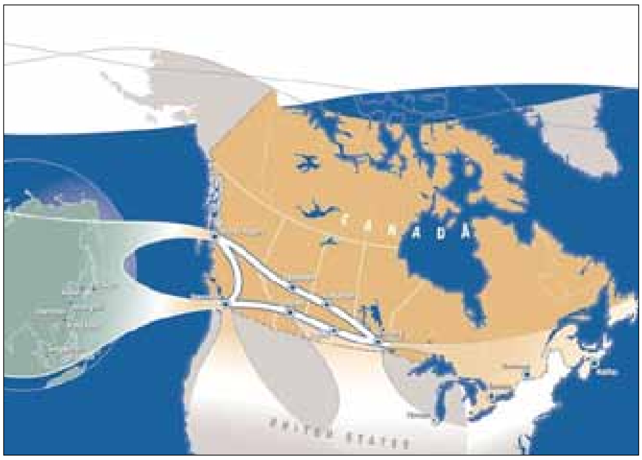
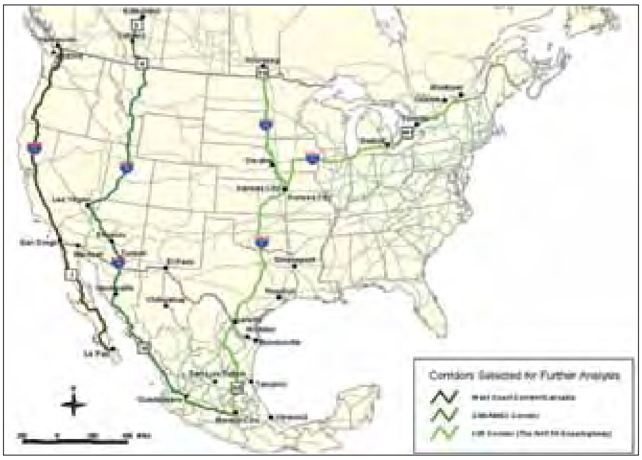


Figure 2 **Selected North American Highway Transportation Corridors**



The Smart Border Declaration set out the principles and shared vision of an efficient and secure border. Within a year, the Smart Border Declaration was expanded into a 30-point Action Plan, which addressed urgent border issues and had wide consensus at both the federal and local levels. By 2004, the agenda of the U.S.-Canada Smart Border Action Plan was largely complete, but many issues remained. It was widely perceived and documented that border procedures and border capacity constraints were still a drag on the economies of North America. The Security and Prosperity Partnership (SPP) was created to renew the agenda of the Ridge–Manley agreement. The SPP was a new institutional model for coordinating the governance of North American integration and its attendant security risks. The SPP established high level working groups that ensured attention to border issues at high levels of government, and established organizational mechanisms for communicating and coordinating across departments and governments. However, by the end of 2008, little progress had been made administratively, and it was widely held and confirmed by numerous studies, that despite additional infrastructure and border processing budget and improvements in security and customs processing, including the adoption of information technologies, the border continued to be a barrier to effective trade and commerce between the U.S. and Canada. This has held true even during the economic downturn in 2008 and 2009 where the demand for border capacity decreased.

This led to the joint declaration by the leaders of both countries, of a Shared Vision for Perimeter Security and Economic Competitiveness in February 2011 (United States, 2011). The Beyond the Border Vision (BBV) included the establishment of a Beyond the Border Working Group to develop a Joint Action Plan with specific initiatives to address the areas of work identified in the Declaration. The Working Group:

- is led by a senior official from each country;
- includes representatives from relevant departments and agencies of the respective federal governments;
- leads are responsible for ensuring inter-agency coordination and consultation.

The Working Group was tasked to solicit input from government, industry, academics and other stakeholders. An announcement of the Working Group's recommendations is expected in December 2011.

The objective of this paper is to provide a perspective on the development of freight security policies and strategies affecting freight crossing the border between the U.S. and Canada. It seeks to critically evaluate how government policy and institutions have been both a barrier and an enabler of both, economic and secure freight movement across this border. Specifically, it focuses on the Smart Border and Perimeter Concept for implementing freight security with the least impact on trade. The paper does not consider in detail parallel issues in traveller movement, whether for business or leisure or shopping.

The Management Freight Security at the U.S.–Canadian Border

Beginning with the Smart Border Declaration and Action Plan (2001), there has been continued emphasis on managing the border "smartly". It was envisioned that border policies and procedures, enabled by information technology and the right infrastructure, could be reengineered and designed into Smart Borders.

An overarching approach for managing the Smart Border and specifically for the movement of commerce across the U.S.-Canada border is risk management.14 The risk management approach separates commercial goods, containers, vehicles or personnel into high-risk and low-risk categories for differential treatment at borders. High-risk trade would be subject to more intensive border inspection, allowing limited border processing capacity to concentrate on the most likely violators. Low-risk trade would be subject to less inspection, minimizing the impact on legitimate trade.

Two core strategies were pursued to effectively implement the risk management strategy: Trusted Partners or Trusted Traders, and Pre-screening. Trusted partner programmes included the Customs-Trade Partnership against Terrorism (C-TPAT) in the U.S., the Partners in Protection Programme (PIP) in Canada, and the Free and Secure Trade (FAST) programmes jointly implemented by both countries. Each of these programmes provides incentives to participants in border supply chains to adopt and embed trade security best practices and compliance into their business practices. All of these programmes are voluntary and participation is based on the benefit-cost perceived by the participants involved in cross border trade. For example, participants in the C-TPAT programmes are the ultimate owners of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers. Importers apply to the U.S. Customs and Border Protection (CBP) to have their security practices evaluated, and if they meet the criteria set by the CBP, receive benefits such as reduced inspections, reduced border wait times at borders, priority processing for CBP inspections when possible, reduced selection rates for Compliance Measurement Examinations and exclusion from certain trade related local and national criterion for selection under the Automated Commercial System. Similarly, the PIP programmes are part of the Canadian Border Services Agency’s (CBSA) trusted trader strategy. To raise and standardize the security level of the supply chain, while enhancing cross-border trade, the PIP and C-TPAT programmes have signed mutual recognition arrangements with each other, and with equivalent programmes in other countries such as Japan, Singapore and South Korea. This is possible because these countries use criteria similar to those used by Canada and/or the U.S. when granting companies membership to their respective cargo security programmes. Both PIP and C-TPAT are aligned with international standards, such as those established for Authorized Economic Operators by the World Customs Organization[15]. This helps to prevent contraband smuggling, combat organized crime and terrorism, and secure the international supply chain. Given their current similarities and the significant number of companies that choose to join both the C-TPAT and PIP programmes, the introduction of a single application process was endorsed by both the CBSA and the U.S. CBP. The goal is to further reduce duplication, wherever possible and feasible, for the benefit of all parties.

Both importers and carriers, which are C-TPAT certified, can subsequently apply for the Free and Secure Trade (FAST) certification, which provides access to designated FAST lanes at the border where cargo processing is expedited. FAST is a joint initiative between CBSA and U.S. CBP that requires all participants (drivers, carriers and importers) to undergo and pass a risk assessment. When a FAST-approved driver arrives at the border, he or she presents three bar-coded documents to the border services officer (one for each of the participating parties: the driver, the carrier and the importer). The officer can quickly scan the bar codes, while all trade data declarations and verifications are processed at a later time, away from the border. Under FAST, eligible goods arriving for approved companies and transported by approved carriers using registered drivers are cleared into Canada or the United States with greater speed and certainty, which reduces costs for FAST participants.

Pre-screening is the process of receiving information about the goods, the means of conveyance, and the owner of the goods to allow the timely evaluation of high- versus low-risk trade prior to arriving at the border. The U.S. Container Security Initiative (CSI) for example, deploys U.S. customs inspectors at foreign ports to pre-screen overseas containers in the port of origin, and for that to work the U.S. Customs and Border Patrol (CBP) needs information about the contents of containers in order to determine whether or not they should be x-rayed and/or physically inspected. To effectively obtain that information, new regulations were instituted requiring advanced electronic submission of cargo manifests twenty-four hours before U.S.-bound sea containers are loaded. Similarly, electronic manifest information must be submitted two hours before arrival into the United States by train and one hour prior to arrival for trucks, unless they are in the FAST programme, which can submit data up to thirty minutes before arrival. Thus, trusted partner and prescreening are interrelated, though the former is voluntary while the latter is mandatory.

The 30-point Smart Border Action Plan sought institu-

14 There are of course, numerous other strategies, such as increasing border-processing capacity with more properly trained personnel and the appropriate infrastructure. I acknowledge the importance of those factors but do not explicitly discuss their impact in this paper.

[15] Though comparable to US C-TPAT, the EU AEO differs in several key areas: 1) EU AEO certification is only available to companies (or “economic operators”) with status as a legal entity of a European Union member country (and certain airlines and steamship lines outside of the EU), whereas US C-TPAT makes allowance for certain foreign-based manufacturer and carrier entities. The EU AEO also addresses both import and export transactions while C-TPAT is strictly import-focused at this time.

tional changes to improve border effectiveness in the form of inter-governmental cooperation, process harmonization, and information sharing without requiring full policy alignment on each country's basic laws. A case in point was the evolution of the NEXUS programme to incorporate a single bi-national application form and fee structure. The same form may be used, but each country can use and weight the criteria for NEXUS approval that suits their needs. Another case was the In-Transit Container Security Initiative between the U.S. and Canada, which was a Smart Border Accord action item that located U.S. Customs inspectors at the Canadian ports of Halifax, Montreal, and Vancouver to work with Canadian counterparts to inspect shipping containers bound for U.S. destinations. This was a reciprocal effort, allowing Canadian Customs inspectors to operate at major U.S. ports (Seattle-Tacoma and New York-New Jersey) to inspect containers unloaded there and bound for Canada. In addition, U.S. and Canadian customs teams work together in overseas ports such as, Rotterdam, to inspect cargo containers before they leave Europe bound for North America. Under CSI, containers are unsealed and inspected by the local customs agents, but decisions about which containers to inspect are made jointly and the information is shared between them. U.S. Homeland Security Strategy has been largely based on the combination of pre-screening and "pushing the border out" beyond USA territorial boundaries. The mutual recognition of each other's trust trader programmes, and the joint administration of FAST are other examples of cooperation and harmonization of specific border security practices.

Harmonization however, frequently received a negative response driven by a political drive within the Canadian government to not acquiesce to the will of the U.S. government when harmonization required Canadian policies to match the U.S. policy. More importantly, Canadian policies with respect to immigration, privacy and asylum reflect differences in culture and social institutions that are not easy to change. Border security was more than securing goods movement; it was also securing the large volume of travel of business and leisure travelers between the two countries by citizens, landed immigrants and visitors. A case in point is that the list of countries that Canada approves for travelling Canada with no visa is larger than the list for the USA.[16]

There was also a fundamentally different objective being sought by each country in managing the border. Border policy in the U.S. is driven by security concerns with respect to terrorism, illegal immigration and illicit cargo such as drugs. The focus is on preventing entry. Canadian border policy had evolved from trade administration (e.g. the collection of tariffs and duties) to trade facilitation given its dependence on the U.S. as a customer. Canada's new found vision of cross border security is primarily to assure the U.S. that movements from Canada can be secure in order to prevent unilateral "thickening" of the border.

Finally, the efficacy of both pre-screening and Trusted Partner programmes, as well as direct processing at border locations are highly dependent on information technologies for effective operational implementation. These include wireless technologies such as:

- Dedicated Short Range Communications (DSRC) for recognizing vehicles and communicating with vehicles;
- Biometrics for recognizing persons;
- The internet for submission of advanced information;
- High capacity, secure and accessible data storage;
- Data analytics for processing large amounts of information quickly.

The Perimeter Concept

The land border between the United States and Canada is made more secure by inspections and law enforcement activity that occurs away from the border. The phrase-perimeter security, in the U.S.-Canada context, made an initial appearance just prior to the terrorist attacks of 11 September 2001. Then USA Ambassador to Canada, Paul Cellucci in 2000, suggested that a shared focus on our shared perimeter could allow a reduced level of attention at our shared internal border, leading to the 49th parallel becoming more of a North American main street, than the inspection point it was, even in 2000. Thus in response to the conflicting security and economic imperatives following September 11, "…discussions between the United States and Canada increasingly explored the possibility of building a "North American Perimeter" modeled after the European Union, whereby internal border controls are lifted as a common external border is established. These talks shifted focus toward international cooperation that would leverage information technology, yielding an "Action Plan for Creating a Secure and Smart Border" (Koslowski, 2005).

Some of the elements of a perimeter clearance strategy were integrated into the 30-point Smart Border Action Plan with the core principles of cooperation, maximizing process harmonization, and information sharing, but not necessarily striving for full policy alignment. The concept of a North American security perimeter was officially blessed at a trilateral leaders' summit, and included in

[16] Some of these differences and Canadian initiatives to accommodate U.S. policy are discussed by Sands (2009) and reproduced in Appendix A.

the Security and Prosperity Partnership of North America announcement by Presidents George Bush and Vicente Fox, and Prime Minister Paul Martin (Wark, 2005). There was increasing recognition by security officials of the value of perimeter security solutions as the availability of large amounts of data from passenger and cargo manifests, for example, demonstrated the potential for joint risk assessments. Unfortunately, the SPP made little progress in advancing border security, as noted above.

The Harper-Obama Washington Declaration of 4 February 2011 followed in the steps of the failure of SPP. Labelled the Beyond the Border Vision (BBV), it stated the intent to pursue a perimeter approach to security, working together within, at, and away from the borders of the two countries to enhance security and accelerate the legitimate flow of people, goods, and services between the two countries. It is notable that little of the supporting detail in the initial strategy statement aligns with common understandings of the word, perimeter, but rather, seems to define the term in more familiar themes of cooperation, partnership, and integration (Conroy, 2011). Actions listed in the BBV that most strongly illustrate the notion of a perimeter approach include.[17]

- An integrated United States-Canada entry-exit system;
- Shared border management facilities and border infrastructure where appropriate;
- To integrate our efforts and where practicable, to work together to develop joint facilities and programmes–within and beyond the United States and Canada;
- Build on success of current joint programmes [NEXUS, FAST]… harmonizing existing programmes… automating processes at the land border [more e-manifest];
- An integrated cargo security strategy that ensures compatible screening methods for goods and cargo before they depart foreign ports bound for the United States or Canada.

With respect to passenger travel, the text of the BBV does not indicate an appetite for an uncontrolled internal border (such as is the case in the 25-country Schengen area) nor does it indicate an interest in creating the level of institutional structure behind Schengen (currently administered and regulated under the laws of the European Union).

A Vision for the Smart Perimeter Border Strategy

We have reviewed how security is managed at the U.S.-Canadian border and its policy evolution in the previous sections. This section describes what a perimeter strategy for freight would look like that would improve freight security at the U.S.-Canadian border for freight with the least impact on trade (See Figures 3 and 4).

A container load of product is sourced from overseas for delivery to a U.S. distribution centre, by an importer who decides to route the container through a Canadian entry port based on total logistics costs of that routing.

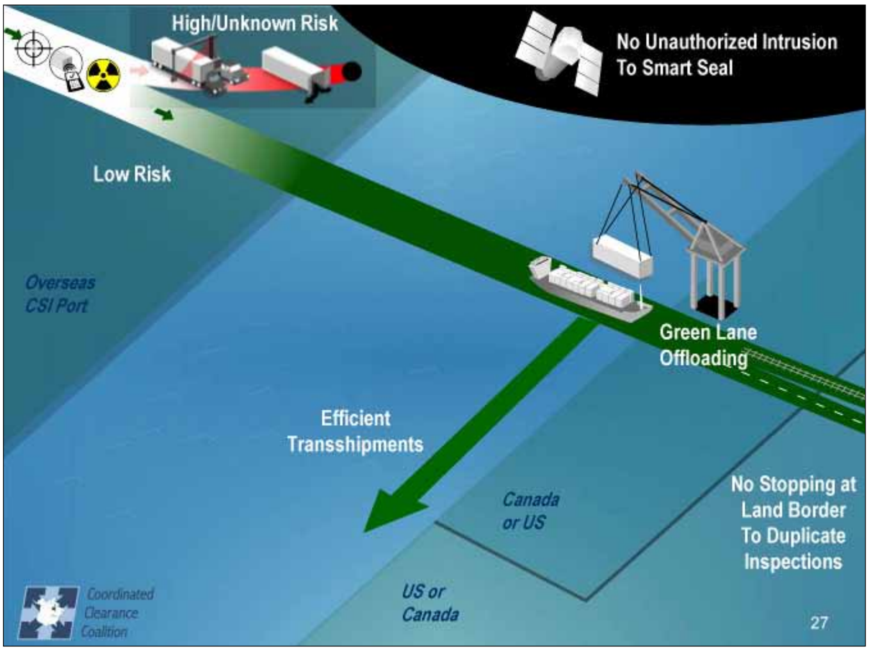

High/Unknown Risk
No Unauthorized Intrusion To Smart Seal
Low Risk
Overseas CSI Port
Green Lane Offloading
Efficient Transshipments
Canada or US
No Stopping at Land Border To Duplicate Inspections
US or Canada
Coordinated Clearance Coalition
27

Figure 3 **Perimeter Securities Operational Vision at Point of Entry into Canada**

[17] Retrieved from Conroy, 2011.

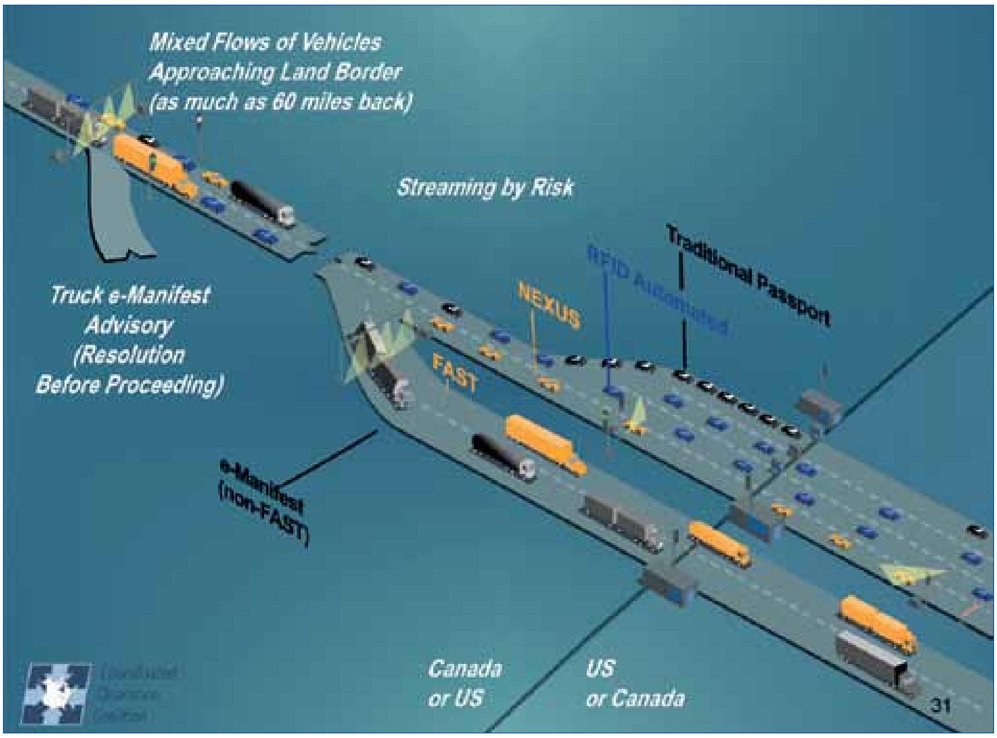


Figure 4 **Perimeter Security Operational Vision at Canada-U.S Border**

The container is shipped to a port of exit for the off-shore supplier, which happens to participate in a Container Security Initiative (CSI) of either Canada or the U.S. Canadian and U.S. customs teams already work together in overseas ports, such as Rotterdam, to inspect cargo containers before they leave Europe bound for North America. The vision is that this cooperative experience has already resulted in the mutual validation of the off-shore risk assessment of each country and will evolve from joint overseas pre-clearance to the leveraging of each other's clearance evaluation results partially or in full. This would expand the overseas port network for which pre-clearance benefits could be available if Canada and the U.S. implemented CSI initiatives at different ports. But most importantly, this would reduce the necessity of having two pre-clearance processes for goods moving in transit through Canada to the U.S. Canada has to decide whether a container is too risky to enter Canada, or requires enhanced inspection. The U.S also has to decide whether the container that landed at a Canadian port is too risky to send on to the U.S. Information sharing could make the two decisions easier to make, but harmonization could eliminate the time and effort needed to make one of the decisions.

At this port of exit, a full target and risk assessment is conducted. This was initiated by the filing of the manifest for the container, 24 hours prior to scheduled ship loading and starts with the pre-screening of the cargo movement and classification into risk categories such as high, low, known and unknown risk. This takes into consideration security risk factors associated with the relevant participants up to this point in the supply chain (e.g. shipper, freight broker importers, carriers, consolidators, licensed customs brokers and manufacturers). Trusted partner status as indicated by participation in C-TPAT or PIP reduces the probability of being classified as high risk. The vision is that the U.S. and Canada either harmonize or jointly implements their trusted partner programmes to ensure consistency and trust in each other's security evaluation. This would increase the foundation upon which pre-clearance decisions by one country would be leveraged by the other country. In addition, the transaction costs to participate in multiple security certification programmes are reduced, increasing participation in these programmes.

All containers pass through radioactive screening, but containers with different levels and types of risks are treated differently with respect to other screening procedures. Containers classified with a known risk go through VACIS inspection, are destuffed and inspected, as it would have been the case at the port of entry in Canada. Containers classified as high risk would at least go through VACIS inspection, but not necessarily be destuffed. Containers that are classified as low risk and those containers classified with high or known risks that pass further inspection, are e-sealed and sent.

The vision is that all containers are equipped with more than e-seals but with Smart RFID cards that can indicate the status of the container in real time or provide a record of events. While In-Transit the container is monitored with a Smart Container card to ensure that the container was not tampered with while in transit. An e-seal only indicates that it had been tampered with but a container can be entered from any side, top or bottom. A Smart Container card can potentially sense items attached to the container. Smart container technology has been concept of operations tested in Europe and North America, developed for cargo condition, cargo security and hazardous goods monitoring, and actively used for high value and critical product movements including military supply. Smart container cards can monitor security breaches in real time by satellite systems and report incidents to Canadian border and customs, which now have new information to change the risk status of the container. Containers can be more efficiently identified for additional risk processing via RFID identification. This real time monitoring of freight may be just as important for monitoring the condition of the freight as for security purposes. If the smart card can be used for multiple purposes, the costs of implementing Smart container technology would be offset by collateral benefits in the supply chain.

At the destination port of entry into Canada, the containers classified with low risk would receive Green lane unloading, which would expedite their transfer for pick-up by truck or movement to intermodal train. The only physical inspection necessary is to confirm that the container has not been tampered with in transit. If the container is equipped with a Smart card, the integrity of the container is already known in advance also facilitating their movement by making physical inspection of an e-seal unnecessary. Containers with high-risk, but not detained at the port of exit would potentially be subject to additional customs and security processing at this port of entry. The containers with known risk or which did not pass radiation or VACIS or destuffing inspection at the port of exit, never got to this point.

Containers that were cleared by U.S. or Canadian inspectors under the CSI procedures at the port of departure now proceed to the Canada–U.S. border by train or by truck. These containers are potentially pre-cleared and ideally, there is no stopping at the border for duplicate inspections, if the U.S. CBP can be confident that the container that had been pre-cleared in the departure port and passed through the Green lane at the Canadian port of entry reached the border without any security breaches. In part, the FAST programme that is jointly administered by both countries achieves this. FAST, like C-TPAT evaluates the risk profiles of the driver, the carrier and the cargo owner or importer. FAST certified movements are less likely to be receiving border inspection and are given preferential (quicker) access to border inspectors in dedicated FAST lanes.

The vision is that the technology that was utilized to ensure detection of security breaches of containers while on the ocean is leveraged for the same purpose while in transit from the entry port in Canada to the U.S. border. In addition to detecting security breaches of the container, intelligent transportation system technologies exist today to create a smart corridor which can demarcate a fence along the planned route of the vehicle and detect violations from the route or unplanned or excessive stop time. This information is only useful if the information collected is sufficient (e.g. meets the needs of) for the U.S. CBP to make a timely assessment. Thus, the U.S. CBP should be involved in the joint design of the programme, particularly in the requirements stage. This is applicable to both containers traveling by truck and by rail.

Drivers still have to be identified under the FAST programme. There have been substantial improvements in passenger processing in both U.S. and Canadian airports with the use of e-Passports and biometrically enabled visas. Biometric technology has the potential to improve the speed and accuracy of driver identification in the cross border trucking process. Canada, the U.S., and other countries have successfully shared biometric information in a number of ways, for example, to manage irregular migration as well as accurately identify individuals. More is needed to ensure proof-positive identification of foreign visitors and the standard is already there with e-passports.

Implementing the Vision of a Smart Perimeter Border Strategy

The overall border security vision is that of the U.S. and Canada working closely together to strengthen border security by managing risk at the point of departure of goods from off shore, to expedite lowest-risk people and goods at points of entry from Canada to the U.S. or vice versa. Pre-screening and trusted trading partner strategy is still the cornerstones for managing freight security risk smartly. This is greatly enabled by the utilization of information technology to identify and expedite the entry of low-risk travellers and goods.

The perimeter vision is to ultimately “push the border out” to the point of departure for both goods and people” to the shared border of both countries. This concept is not necessarily confined to off-shore movement of goods travelling in-transit through Canada to the U.S (or vice versa). For example, the U.S. CBP already operates at 9 of Canada’s largest airports, on Canadian soil to pre-screen passengers going to the U.S. from Canada. Upon arrival at a U.S. airport, passengers depart the airport as if they were arriving on a domestic flight.[18] One can envision a similar arrangement for freight transportation, but that is much more intricate. Both the U.S. and Canada have developed policies to process inbound cargo for customs purposes away from the border, for example, Canada allows trucking carriers to submit freight for customs inspection at sufferance warehouses located inland within a specified time after crossing the border. This is particularly convenient for less than truckload (LTL) carriers and Canadian customs when the LTL freight terminal is co-located at the sufferance facility, since the LTL freight has to be unloaded anyway, and customs inspection can occur during or shortly after the unloading process. But while the goals of customs processing is to ensure that customs duties are properly assessed and collected, the goal of security processing is to prevent entry onto U.S. or Canadian soil of unwanted cargo. The perimeter concept would only work if freight could be pre-screen at a location in Canada and the integrity of the vehicle and freight after pre-screening is maintained from the processing location to the U.S. border.

This possibility has been explored at the Peace Bridge crossing along the Canada-U.S. border, which is the third busiest for commercial, and the busiest for passenger traffic. It was advocated that a joint pre-clearance facility be built on the Canadian side of the crossing to reduce congestion at the bridge. The facility would house U.S. customs, which would relocate from downtown Buffalo (U.S.) to land on the Fort Erie side of the border. The Canadian and U.S. governments ended negotiations for a pre-clearance pilot project in 2007, citing sovereignty concerns around placing American border and customs agents in Canada and other issues. Recently (2011), the head of Homeland Security confirmed the assessment that "a joint pre-clearance facility would result in a "lower level of security" for the U.S. and would have required Canada to accept actions contrary to its Charter of Rights and Freedoms." These institutional barriers appear to be as firm today as they were four years earlier.

We suggest two opportunities for achieving some of the benefits of perimeter clearance for freight movement originating in Canada. A technology-based solution envisions shippers and carriers who already participate in C-TPAT or PIP and FAST, participating in a new programme entitled "Security Assurance at the Source." In this programme, video monitors are strategically placed from the end of the production line, along the conveyors to storage locations and from storage locations to the outbound staging area for loading containers or trailers destined to the U.S. A complete video record of the products handled and loaded into a conveyance and the sealing of the conveyance with an electronic smart seal is made. This video surveillance compliments access controls to prevent theft or unauthorized tampering of the products and recordings are routinely examined on a sampling basis. The video recordings are provided to U.S. customs authorities on request or real time monitoring can be permitted virtually to any U.S. CBP location. The system can be designed to allow CBP inspectors to request visual examination of specific containers, boxes or individual units. Today's video technology and high speed transmission of quality video images can enable timely, virtual inspection and pre-clearance before reaching the border.

An alternative proposal is to outsource or subcontract pre-screening and clearance to trusted partners such as the CBSA. If pre-screening criteria and pre-clearance procedures can be harmonized and accepted reciprocally by the CBSA and CBP as posited in the vision of an expanded CSI abovewhy can't these same institutional changes be implemented within North America?

The success of the perimeter vision posed depends on many factors. The perimeter initiative builds on key successes by CBSA, CBP and other agencies since 2001 and the development of new technologies and risk management capabilities. These included further coordination of data sharing and systems integration, building on joint risk assessment pilots and bi-national data sharing protocols.

Institutionally, there is a requirement for coordination within and between governments, coordination of public and private sector activities, and coordination of transportation, commercial and border security efforts. This would eliminate some of the silos within governments and coordination between governments– locally, regionally, and nationally. But fundamental questions about a country's value and culture, which are reflected in government policy. For the U.S. can it move away from the "Security trumps trade" or is this a non- discussion item embedded in organizations (the DHS), existing regulations and popular support? For Canada, can it retreat from previous positions on immigration, privacy and sovereignty that have prevented institutional changes which would have put Canada more in line with U.S. policy and facilitated more cross border cooperation and harmonization that would have enabled perimeter clearance? With respect to the latter, these issues seem to be more important when the discussion is about managing people movement across the border. Although they are related, perhaps, a better strategy is to keep freight security and border issues separate from passenger security border issues.

[18] See Appendix A for a more in depth discussion of passenger pre-clearance issues.

Conclusion

In summary, the development of a perimeter freight security policy and strategy for the Canada–U.S. border since 11 September has progressed in small increments. A renewed focus on the perimeter border concept is implied by the title of the latest joint U.S.–Canada vision for border management, Beyond the Border Vision (BBV). It remains to be seen from the BBV report anticipated in December 2011, how perimeter clearance will be defined, what actions will be pursued and what policy alignments will be pursued. This paper has suggested some potential actions and a vision for how the perimeter approach could work. It has identified some of the potential opportunities and barriers to an effective perimeter approach for managing the Canada–U.S. border with respect to freight and it was concluded that effective freight security and border policy depends on institutions.

Full realization of a perimeter border strategy will require intergovernmental dialogue, mechanisms, and procedures that are not currently acknowledged or declared in the BBV declaration. So while many will say “We‘re not doing anything like Schengen here…, making progress (at long last) on goals listed (actually several are relisted) in the BBV will not necessarily be easier to achieve. But that is to be expected. The last several years have seen the emergence of new types of formalized dialog, which should be seen as new and deeper sources of institutional capacity for the advancing U.S.-Canada border facilitation. Nothing occurs instantaneously in such a complex environment.

The perimeter border challenge does have some implications for the European Union even though the most frequent references to Europe are what North America can learn from the European Union experience and Schengen, not the **other way around!** The inability of Canada and the U.S. to develop a coherent perimeter border strategy and to collaborate on a transborder partnership may provide some lessons for inland cross border transport between the European Union and its neighboring trading partners. Many of these neighbors are low-cost countries to which the more developed European Union members may near source labour-intensive manufacturing. Even individual EU countries may have relevant policies that are inconsistent, either in principle or implementation, with policies of other EU countries with which they are interdependent. Institutions were both barriers and enablers in the evolution of the Smart border and the perimeter border in North America and they will be no less in the EU.

References

Conroy, Hugh (2011) “Declared Perimeter-goals Will Require Undeclared Approaches “ in Seminar Proceedings: Perimeter Security and the Beyond the Border Dialogue: Perspectives from the PNW-Western Canada Region, Border Policy Research Institute, Western Washington University, Bellingham, Washington, July 20, pp. 24 – 28.

Christopher Rudolph (2008) “A Smart Border? The American View, Chapter 10, in www.fraserinstitute.org. pp. 183 – 209.

Koslowski, Rey (2005) “Smart Borders, Virtual Borders or No Borders: Homeland Security Choices for the United States and Canada” SMU Law Review (Vol. 05) pp. 1 to 55.

Sands, Christopher (2009) Towards a New Frontier: Improving the U.S. – Canadian Border, Metropolitan Policy Programme, Brookings.

Szabo, David and Todd Walters, (2005). The Canada-U.S. Partnership: Enhancing Our Common Security, Workshop Report by Rappateurs , Institute for Foreign Policy Analysis.

Wark, Wesley (2005) “Smart Trumps Security: Canada’s border security policy since September 11” , paper presented Canada-Mexico Big Picture Realities: NAFTA Plus, Immigration, the Security-First Border, The Bush Revolution in Foreign Policy and The Global South, Panel 4, Canada Mexico Seminar Robarts Centre for Canadian Studies, York University (Nov.)

United States (2011) “Declaration by President Obama and Prime Minister Harper of Canada – Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness.” The White House, February 4.

Appendix A

Importance of Perimeter Gateways in the USA-Canada Relationship Excerpted from Sands, Christopher (2009) Towards a New Frontier: Improving the USA–Canadian Border, Metropolitan Policy Programme, Brookings

Individuals seeking to enter the United States by air preclear U.S. Customs and Border Protection before heading to their airplanes at nine of the largest Canadian airports.

U.S. airport pre-clearance allows CBP to determine the admissibility of an individual prior to their entering U.S. airspace. Canadian airports were among the first to host U.S. Customs pre-clearance, and have invested millions of dollars to upgrade airport facilities to secure the U.S. departures gates and provide space for CBP to operate. In addition to Canada, only Aruba, the Bahamas, Bermuda and Ireland have U.S. passenger pre-clearance agreements, which provide airlines with the major benefit of being able to fly directly to any domestic U.S. airport rather than being limited to those with a U.S. Customs presence for screening inbound international travelers. U.S. concerns over Canadian immigration policies were one reason for the United States to seek a presence at Canadian airports to pre-screen U.S.-bound travelers. A Canadian Supreme Court ruling in 1986 (the Singh ruling) made it more difficult for Canadian authorities to deport non-citizens who had entered Canada seeking to remain as refugees or prospective immigrants. In 2002, the Canadian Parliament overhauled its immigration legislation to require potential immigrants in most cases to apply from their home country or a safe third country prior to coming to Canada–a practice similar to that of the United States. The 2002 Canadian immigration reform also improved the background checks on potential immigrants to Canada by requiring officials to consider intelligence reports from friendly foreign countries including the United States where applicable and appropriate.

Despite these reforms, an unknown number of individuals who had previously entered Canada were a source of concern for U.S. officials. Although none of the individuals who carried out the 11 September 2001 terrorist attacks on the United States came from or through Canada, there were several previous terrorism cases with Canadian connections. Canada has a larger list of countries whose citizens do not require a visa to visit or transit through Canada than the United States post-2001, and the two countries require different information from visa applicants, visitors without visas (those from countries with a visa waiver), and refugee and asylum applicants. The United States requires mandatory detention for refugee and asylum applicants until their status has been determined; Canada does not. Legal rulings on privacy rights in each country have limited the sharing of information with officials in the other. These differences have become the focus of concern in the United States in particular, where officials rely on information and intelligence from friendly allies like Canada to make risk assessments that underpin a host of border security measures.

This points to the reason why the Perimeter gateway is in some ways the most critical for the United States and its relationship with Canada: stopping individuals and attacks as far from intended targets as possible requires active international cooperation, which Canada has been willing to provide through security cooperation as well as domestic reforms.

Comments

Ms. Susanne Aigner

Deputy Director Compliance and Facilitation

World Customs Organization (WCO)

Dr. Chow's paper focuses on the cooperation at the border between Canada and the US, in particular in view of responding to increasing security threats and ensuring smooth flow of goods and passengers.

The paper summarises measures taken since 11 September 2001, and includes information on the recent agreement between Canada and the US (Prime Minister Harper/President Obama) to implement Joint Action Plans to Boost Security, Trade and Travel. The paper also describes a vision as to how to improve inland transport between Canada/US, proposing concrete measures.

The measures described in the paper highlight the need for:

- Intelligence-driven risk management, based on advance reporting and sharing of information;
- Use of technology (e.g., radiation detection equipment, scanning), not in isolation, but based on and coupled with IT supported risk management;
- IT-supported risk analysis;
- Focus on high risk consignments and rapid release of low and no risk goods;
- Streamlining of controls and focus between both sides;
- Coordination between relevant regulatory agencies nationally as well as internationally (CBM); addressing passenger and goods in a more encompassing way;
- Structured information exchanges/information

sharing to better target but also facilitate legitimate trade. (A reply could be the WCO initiative on Globally Networked Customs (GNC) where United States as well as Canada Customs are very active.);

- Partnership B2C, AEO programmes and equivalent, in particular if both sides recognize each other's programmes and have trust in both sides' programmes (mutual recognition);
- Joint Cooperation police/customs/immigration (CBM nationally and need for information sharing);
- Pushing the border out (this raises obviously also questions relating to extraterritoriality and sovereignty; the CSI agreements signed between EU MS and United States did lead to certain problems).

The paper also describes the Perimeter concept (which is part of the joint action plan USA/Canada which was agreed very recently):

Ideally, United States and Canada would agree on one stop/joint border posts in order to facilitate trade and enable joint targeting (both seems at this stage only a vision – presumably, the agreement to implement the Joint Action Plans will hopefully enable both);

Mutual recognition of controls – the paper indicates that this is currently not a reality; however, it refers to pushing out borders and ensuring that – at some stage – the export controls by one side would be recognized on the import side, which would enable both sides to focus controls more efficiently and effectively on high risk consignments/passengers. The "my export is your import" in relation to goods is being discussed in the WCO fora as well as between EU and some partner countries, including China, United States, Canada (in WCO discussions, Members insist, however, that this does not imply a transfer of liability to the other side). The EU-China Smart and Secure Trade Lanes (SSTL) project and a number of projects under the EU 7th Framework Programme for Research and Development are testing the concept;

Creating secure areas (like Schengen in the EU) – the paper indicates that this would be the ideal solution. In the EU, the experience with Common Customs-Police Centres (CCPC) that have responsibility for immigration issues but also land border security and crime is very positive; it requires certainly an alignment of legislation (examples are Switzerland/Italy and Switzerland/France CCPCs which allowed to more efficiently handle the huge immigration flows during the Arab spring). The EU and Andorra, Norway and Switzerland did also agree on common areas of customs security, based on the mutual recognition of controls and AEOs. The neighbouring countries of the EU had to implement equivalent measures to the SAFE/EU legislation on customs security. Both sides agree joint risk rules and ensure that equal levels of security controls apply on both sides;

Dr. Chow's paper indicates that without such policy and legal alignment, no further alignment or "rapprochement" would be possible, citing Schengen and EU coordination as examples. This is certainly true: without negotiating eye-to-eye and without finding consensus on common objectives, no such agreements are possible. Certainly all measures need to be embedded in a wider political strategy, otherwise only a piecemeal approach is possible. SAFE promotes such comprehensive approach in order to facilitate and secure global trade.

The paper describes also a vision for the Smart and Perimeter Border. In the vision part, Dr. Chow describes scenarios, which will hopefully exist in the near future and which are being tested in pilot projects, e.g. mutual recognition of controls/risk analysis results that lead to joint decisions on controls and to the establishment of joint secure perimeters/areas. While the thinking is not new, the implementation between countries is certainly a challenge and has so far only materialized (without being fully implemented) in the context of EU-Norway/Andorra /Switzerland. In the latter case, however, it has to be recognized that treaties to simplify border crossing exist for more than 60 years and the alignment/rapprochement has been implemented step by step, starting with small (at individual border crossings, relating to specific goods and specific trade lanes) before realizing bigger projects. Similarly, also ANZCERTA is based on longstanding cooperation between Australia and New Zealand that gradually expanded; also EU Internal Market and Economic Union started on a smaller scale.

Also Schengen started small and expanded step by step, before being fully integrated in the EU acquis in 2000, following obligations from the Amsterdam Treaty.

Information sharing is certainly recognized as one of the key elements to increasing security and facilitation of international supply chains. In its Customs in the 21st Century Strategy, WCO Members considered that "Globally Networked Customs" should be the first building block and should be seen as an enabler for many of the nine other building blocks (Coordinated Border Management/Single Window; Intelligence-driven risk management; Partnership with trade, etc.). While information is already being exchanged today, including in the mutual recognition of controls and/or AEO context, GNC aims at developing protocols, standards and guidelines that would allow "off-the shelf" solutions for countries/agencies that want to share information and can thus benefit from easily adaptable but ready-to-apply models, including legal models.

Dr. Chow raises the aspect of different political focus, e.g., security versus facilitation, which will always have an impact on the potential degree of alignment. Another important aspect, also mentioned in his paper, is trust in what the other agency does; without mutual trust, solutions will not be efficient – if mutual recognition of controls/risk management is agreed without sufficient trust among parties, duplication of controls will persist, and thus the objective of efficiency and facilitation has not been achieved. The Harper-Obama agreement to implement the two action plans is, therefore, a very important achievement as it shows a rapprochement of objectives.

One concrete example, taken from the Border Action Plan, where page 18 foresees the establishment of an electronic Single Window through which importers can submit electronically all information required by the participating government agencies. Canada Border Services Agency and United States Customs and Border Protection will assess data electronically, will take control decisions and will inform, also electronically, the trader. For that purpose, the data requirements of all participating agencies have to be converted into electronic format by 2013. This is certainly a measure, which will improve the movement of goods crossing the US/Canadian land border and will have impact on trade flows as well as on security.

The paper does not refer to more technical or procedural requirements but remains at a general level. IT does also not necessarily refer to ongoing activities in other areas, which have an impact, including the wider political context (for example, mutual recognition agreed between EU-US, US-Japan, US-New Zealand). The latter might not have a direct impact on land border security but will certainly have an impact on global perceptions and political approach towards supply chain security.

7

Customs Perspectives on Detection of Deliberate Regulatory Violations in Global Supply Chains - the Role of Information and Data in Risk Identification

Hintsa J.*, Männistö T., Urciuoli L., Ahokas J. | Cross-border Research Association, Lausanne, Switzerland
* corresponding author (juha@cross-border.org)

In collaboration with HEC University of Lausanne; (Prof. Hameri)
and Aalto University, BIT Institute, (Prof. Holmström Finland)

This paper has been developed with partial financial support from
FP7 projects INTEGRITY, FOCUS and CASSANDRA

Introduction

The objective of this Discussion Paper is to shed light on the complicated topic of customs risk management, specifically on the role of information and data in risk identification in global supply chains. The main motivation to develop this paper came from the observation by the authors during years 2008 and 2009: the growing public debate on advance cargo data requirements; sharing of "risk related" information and data between supply chain operators and customs administrations; among other related sub-topics; were lacking a proper foundation in the literature, a foundation where all parties could talk in the same language, within commonly understandable framework. This paper intends to deliver a tangible "communication platform" between supply chain operators and customs administrations (also policymakers) to effectively discuss about the current and the future of public-private collaboration in prevention and detection of deliberate violations of customs enforced regulations, in particular, how information and data from a variety of sources can best be fitted in.

Below, we provide a set of brief definitions on what is meant by the paper title, "Customs Perspectives on Detection of Deliberate Regulatory Violations in Global Supply Chains - the Role of Information and Data in Risk Identification":

Customs Perspectives

Customs administrations are assigned with a variety of responsibilities when it comes to duty revenue collection, protection of society, production of trade statistics, etc. The detailed roles and responsibilities differ between administrations across the globe. For this paper, "an average customs" position has been chosen.

Detection

A total risk management cycle can consist of following five stages: Identify – Assess & analyze – Plan action – Monitor & implement – Measure & control. This paper fits essentially in the Identification stage. In supply chain security management, sometimes a three-stage approach is used: Prevention – Detection – Recovery. In this paper, "detection" simply means that customs is able to realize that illicit activities are likely to take place in the specific (cross-border) supply chain / movement / shipment. This can then lead to further customs interventions in the supply chain, e.g. x-ray scanning, physical inspection, audit visit, etc. (which are out-of-scope for this paper).

Deliberate Regulatory Violations

Customs administration typically enforce a large number of regulations, part of them belonging to actual "customs law", and part of them to other areas of legislations. Illicit actors in the supply chain, for example, opportunistic duty fraudsters or serious organized crime focusing on narcotics trafficking, purposefully violate these regulations, for illicit fiscal or ideological reasons.

Global Supply Chains

By definition, customs focuses on cross-border trade and movements of goods, worth approximately 10 trillion euros annually. For example intra-EU trade and goods movements are not part of this "global supply chain figure".

Information and Data

Examples of information in the context of this paper include "country risk information on a government produced and shared document" and "an export country customs officer calling a shipment destination country customs officer and sharing intelligence verbally on the phone about a potentially dangerous shipment on its way to the destination country". Examples of data include "Harmonized tariff schedule (HTS) code in customs declaration"; and "Shipper address in Known Shipper database".

Risk Identification

"Risk" in customs context can be defined for example as "likelihood that something will prevent the application of customs union measures and/or national measures concerning the customs treatment of goods." In practical terms, risk in the customs context refers to illicit activities related to international supply chains: smuggling of restricted and prohibited goods across customs frontiers, duty evasion, a diverse set of frauds and so forth. By "identification" we mean simply that customs organization realizes – at an appropriate time – that something illicit is likely to be happening in the supply chain.

Very little has been published before on this topic, one likely reason being the difficulty of getting access to relevant information. This paper has been developed over a 2-year time period (December 2009 – November 2011), first by reviewing available practitioner and academic literature, followed by interviews of over 100 experts working at customs administrations and supply chain operators, worldwide. All the content on this paper is of non-sensitive nature and several issues are purposefully left on conceptual or illustrative level. The paper takes a "global approach", from "an average customs administration" view point (even though Chapter 5 contains illustrative examples on EU and United States risk management approaches).

From terminology point of view, this paper aims to be as simplistic as possible, taking a "layman approach", whenever feasible. In particular, when it comes to variety of "risk terms" – risk management, risk assessment, risk identification, risk profiling, targeting, risk rules, risk engines and so forth – this paper aims not to get lost in the jargon, but instead to rely on simple "risk identification", as whenever feasible. Detection of unintentional compliance errors made by supply chain operators is out-of-scope for this paper. The rest of the paper has the following structure:

Chapter 2. Bad actors – bad shipments & movements – bad consequences

Chapter 3. Violations of customs enforced regulations

Chapter 4. Information sources to detect bad actors, bad shipments & bad movements

Chapter 5. Illustrations on information and data driven risk identification

Chapter 6. Summary and conclusions

Disclaimer-1: the authors included purposefully people smuggling – when illegal immigrants are hidden in containers, ship structures, or any other means being essentially embedded into the "supply chain" – in this paper, even though in most nations it is the primary responsibility for border guards and border police to tackle. Despite the fact that customs plays typically only a secondary role when it comes to people anti-smuggling activities, the authors took the decision to include it (in particular the taxonomy in Chapter 3).

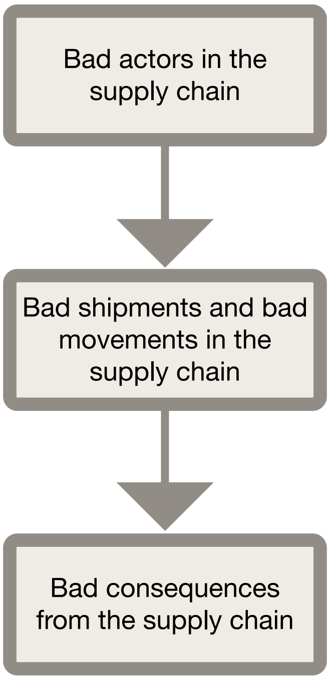
Disclaimer-2: due to the fact that publicly available information was available on US Transport Security Administrations (TSA) past approach to risk identification, the authors included a sub-chapter based on TSA´s approach in this paper, even though TSA is naturally not a customs administration.

Disclaimer-3: due to several reasons, the content of this discussion paper is mostly for illustrative purposes only. It is not meant to represent an accurate interpretation of customs enforced laws in any given country. This paper does not include security sensitive sections.

Bad actors – bad shipments & movements – bad consequences

Overview

The basic setting in all customs related deliberate regulatory offenses is the same - bad actors lead to bad shipments and movements that result in bad consequences. This simplistic causal logic, or, sequence chart, as visualized below, provides a baseline to explore further the concepts around information and data driven identification of bad actors and bad shipments and movements – before they cause actual damage for companies, governments and/or citizens.


Bad actors in the supply chain
Bad shipments and bad movements in the supply chain
Bad consequences from the supply chain

Bad actors

Bad actors in the global supply chains are individuals, organizations or networks deliberately violating laws and regulations governing international trade and logistics, with subsequent import/transit/export prohibitions, restrictions and so forth. These actors can be classified into two types according their main motivation to engage in illicit activity. The first is profit-driven criminals who commit crime when it pays off financially. They disregard laws and regulations when they plan how to generate illicit revenues or save in costs. Among other illicit activities, the profit-driven criminals trade in prohibited and restricted goods; smuggle otherwise legal goods like tobacco, mineral oils and alcohol to evade duties and taxes; and carry out various illegal schemes to collect unjustified export subsidies to get tax and duty exemptions, just to name but a few examples.

The second category of actors engaged in customs related illicit activities are motivated by other reasons than direct fiscal benefits: political agenda, ideology, revenge, etc. Some bad actors in this group, in particular terrorist organizations, exploit terror and destruction in order to get publicity for their ideas and put pressure on foreign governments and policymakers.

Bad shipments and movements

To reach their illicit objectives, the bad actors in international supply chains get involved with customs related illicit activities. In many cases they need to transport goods or people across customs frontiers in an illicit manner. Some bad actors move prohibited merchandise or restricted goods without appropriate licenses while the others smuggle otherwise legal goods for tax and duty evasion.

Bad shipments and movements can lead into violation of rules that prohibit and restrict international trade, in particular export and/or transit and/or import in certain goods. Even though each customs jurisdiction has their own catalogue of completely banned items and allow articles for imports and exports only under specific circumstances (= restricted goods which importation and exportation require licenses), many customs administrations ban or restrict cross-border movement of following articles:

- Examples of typically banned exports and/or transits and/or imports and/or stolen goods; merchandise violating intellectual property rights i.e. counterfeit goods; concept-wise also people smuggling can be considered to fall under this category;

- Examples of typically restricted exports and/or transits and/or imports: narcotics; precursor chemicals (can be used e.g. in refinement of illegal drugs); firearms; endangered animal and plant species defined under the CITES Convention, annexes I, II and III; dual goods (articles which can both civil and military purposes); hazardous waste.

Bad shipments and movements can also lead into violation of rules and regulations associated with duties, taxes and tariffs. These shipments contain otherwise legal goods which become illegal contraband if the goods are imported/exported without paying adequate duties and taxes to the fullest extent. Fiscal fraud, i.e. evasion of taxes and duties can be either partial or complete.

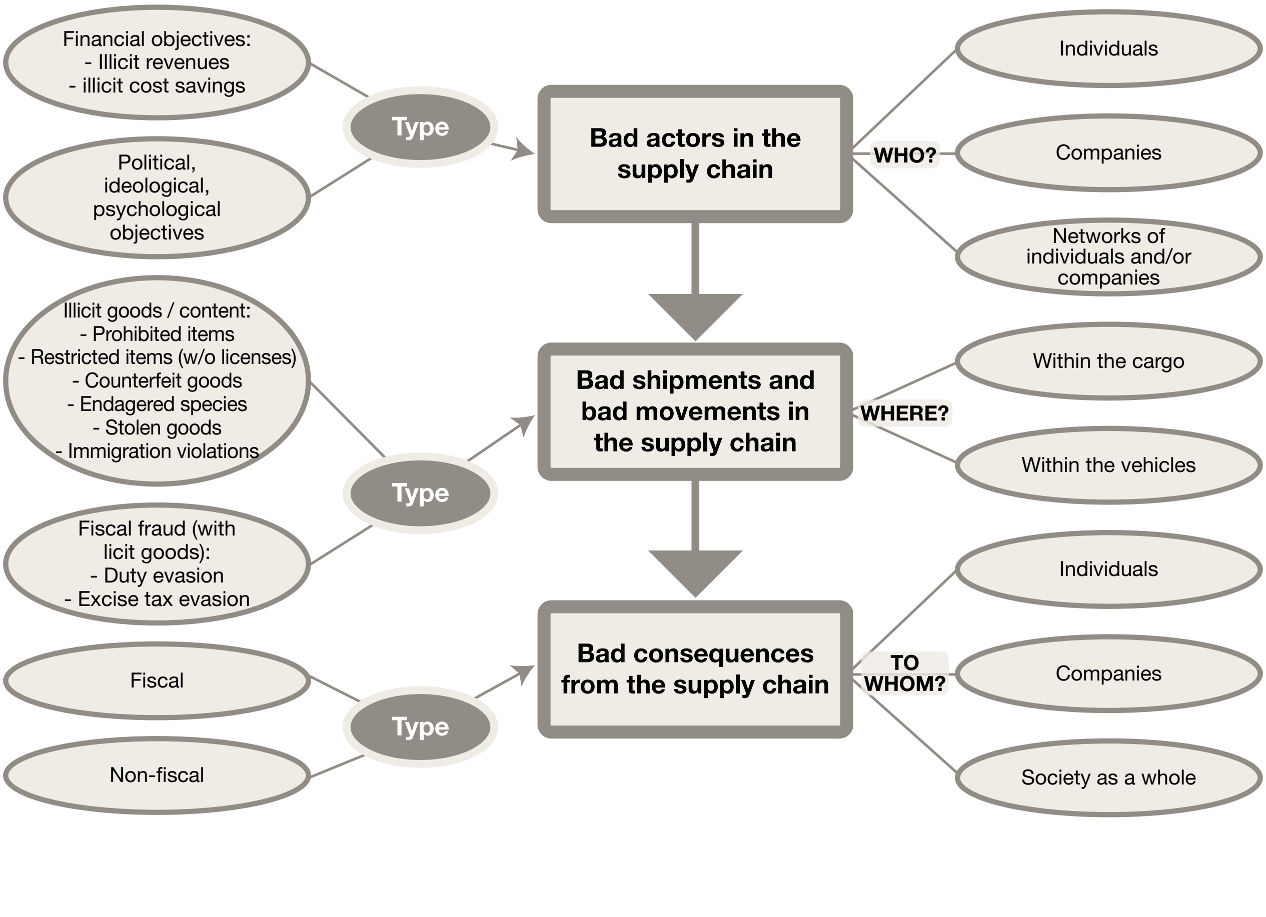
From the illicit actor viewpoint, there is always a risk of seizure when bad shipments and bad movements cross customs frontiers. To minimize the likelihood that customs detect and intercept bad shipments, the bad actors use a range of techniques to conceal their illicit merchandise among legitimate cargo or in the constructs of the vehicle of transportation (e.g. truck or container). For example, in a typical duty fraud case, a dishonest trader masks a shipment of heavily taxed goods with a cover load of less taxed commodities. At a customs frontier, the fraudster submits a false import declaration reflecting the contents of the cover load. In the end of a successful deception, the fraudster ends up paying less in duties and taxes than legally obliged. Smugglers of prohibited and restricted goods have proven to apply creative methods for concealment: cannabis inside hollow concrete blocks, elephant tusks hidden behind a bogus container wall and cultural artifacts concealed among charcoal sacks.

Bad consequences

Bad shipments and movements, if not detected early enough, can cause many kind of harm for companies, governments, citizens and the society as a whole. Articles intended to cause havoc by damaging, destructing and disrupting global supply chains – including chemical weapons and "traditional" explosives – pose an immediate security threat. On the other hand, undesirable consequences of certain bad movements realize only after time: trafficking in military technology could result in (war) crimes against humanity; trade in forbidden chlorofluorocarbons (CFC) compounds deplete the ozone layer; illegal immigration to wide social problems and labor market disputes, and so forth.

Aside a multitude of adverse social, political, environmental and other non-fiscal consequences, bad movements cost dearly for companies and governments fi-

Figure 1



nancially. Smuggling for duty and tax avoidance means lost revenues for governments. Companies face fines when authorities find illegal articles among cargo (i.e. illegal immigrants[19], they might lose their hardly earned authorized trader status (e.g. narcotics found in an "Authorized Economic Operator (AEO) container" and lose sales revenues when contraband sold at black markets decrease demand for legitimate products.

Completing the picture on "the sequence of the three bad

The Figure 1 summarizes how bad actors introduce bad shipments and movements in supply chains that cause undesirable outcomes in case these movements are not intercepted early enough. Next to the top box, three types of bad actors (right side) and what motivates them (left side) are shown. Next to the middle box, the picture illustrates what type of bad shipments there are in the supply chains (left side) and where they are can hidden (right side). The bottom box makes it explicit that the bad shipments can cause both fiscal and non-fiscal harm (left side) for individuals, companies and the society as a whole (right side).

Ultimately, the challenge for customs is to collect information and data from the supply chain, to detect the illicit attempts as early as possible in the chain, both distant-wise – as "far away from own borders as possible" – as well as time-wise–as early as possible.

Violations of customs enforced regulations

Overview

For the purpose of this paper, we define customs related illicit activities as violations of regulations that customs administrations enforce. This definition covers infringements of customs law such as evasion of customs duties or smuggling of prohibited goods but also statuses of other bodies of legislation such as civil law and criminal code.

Detailed taxonomy of customs related illicit activities

According to Cross-border Research Association (CBRA) research, customs related illicit activities can be classified into four general categories. The first category includes events where bad actors smuggle restricted[20] and prohibited[21] goods across borders in order to circumvent prohibitions, license requirements, quotas, and anti-dumping restrictions. The second category concerns shipping of cargo to forbidden destinations. In this category, the bad actors violate regulations regarding embargoed countries, organizations and individuals. The third category encompasses actions where the bad actors evade duties and taxes, which collection should be collected by customs. Tax and duty fraud can be either partial or complete. The fourth category of customs related illicit activities relates to false reimbursement claims for refundable Value Added Tax (VAT), export subsidies, and drawbacks.[22]

The two latter categories, the duty fraud and the false reimbursement claims, are purely profit-driven illicit activities. In comparison, the smuggling of prohibited and restricted goods and the shipping of cargo to forbidden destinations can be motivated by fiscal benefits and sometimes by political and ideological reasons.

CBRA research shows that bad actors use nine *modi operandi* (i.e. methods or techniques) to carry out customs related illicit activities.

The first one consist in the complete avoidance of customs controls. Bad actors can transport their merchandise via clandestine unauthorized smuggling routes. This is an attractive *modus operandi* for traffickers in case legitimate border crossing points are strictly controlled by law enforcement agencies, and when legal importation is problematic or impossible due to product-specific prohibitions, licensing requirements[23], quotas, anti-dumping policies or embargoes. By avoiding customs controls altogether, the traffickers can import/export prohibited and restricted goods and trade with embargoed countries and blacklisted organizations but also evade trade-related duties and taxes completely.

In the remaining eight *modi operandi*, cargo is transported through legitimate trade lanes and customs check points. Here, the modi oprandi always requires giving false information to customs authorities and using appropriate concealment techniques. From time to time, the bad actors facilitate illicit activities also by means of corruption and intimidation.

Over- and under-declaration of value as well as under-declaration of quantity of imported / exported cargo are strongly associated with profit-driven duty fraud and false reimbursement claims. Understating value or quan-

[19] www.ukba.homeoffice.gov.uk/sitecontent/newsarticles/2010/dec/05-illegal-lorry-kiwi-fruit

[20] Allowed for import / export if certain conditions are met.

[21] Absolute prohibition, not allowed to import / export in any circumstances.

[22] A refund of customs or excise duty paid on goods that are being exported or used in the production of manufactured exports.

[23] Referred also sometimes as non-tariff trade barriers that are onerous procedures to acquire licenses or prepare and submit customs declarations.

tity of traded merchandise results in partial evasion of taxes and duties whereas overstating the value of cargo precedes typically fraudulent reimbursement claims.

Under valuation: bad actors submit false customs declarations that understate the actual value of cargo and thus, up pay less duties and taxes than legally obliged.

Over valuation: by exaggerating the value of their cargo, dishonest traders can inflate export records and claim fraudulent VAT refunds, export subsidies or drawbacks from governments. Over valuation allows a disregard for price floors that are part of most anti-dumping policies.

Underdeclaration of quantity: enables the traffickers to partially avoid quantity-based taxes and duties but also to circumvent country- and end-user-related quotas.

Misrepresentation of commodity-specific tariff code (i.e. HS code[24] makes a diverse set of customs related illicit activities. With false tariff code, the bad actors can evade taxes and duties, supply embargoed clientele and smuggle basically every commodity under the sun, whether inherently illegal or not.

Misrepresentation of tariff code deceives customs officers into believe that the content of a shipment is something other than the reality. A false tariff code enables the bad actors to smuggle prohibited goods; disregard licensing, quota and anti-dumping regulations; transport cargo to forbidden destinations disguised as humanitarian aid; evade duties either completely or partially; and skew export records.

Most countries control trade flows in and out of their territories with licenses, permits and certificates. Government bodies grant these credentials for business actors that meet or exceed certain set of requirements, typically considering quality, security, safety, and environmental friendliness of operation of the applicant. Criminals sometimes falsify and misuse these authorizing documents in order to get an access to regulated or/and restricted markets.

Misuse of authorizing documentation: fraudulent use of official documents helps in evasion of basically all international trade related rules. Moreover, the bad actors can deceive authorities into granting tax and duty exemptions as well as quota and anti-dumping restrictions. False licenses also facilitate trading with embargoed countries as well as blacklisted organizations and individuals.

False declarations about country of origin, country of destination or consignee moderates the flow of cargo through transit countries but also allows the bad actors to circumvent country-and end-user-specific restrictions and get preferential tax and duty rates for their merchandise.

False declaring a country of origin: False statements about the origin of cargo enable bad actors to evade licensing requirements, quotas and anti-dumping policies that restrict exports from certain countries. The method can also cover up the origin of source-sensitive com-

[24] The Harmonized Commodity Description and Coding System (HS) is a standardized international nomenclature to classify traded commodities. The system is developed and maintained by the World Customs Organization (WCO).

Type of customs realted illicit activity	Smuggling of restricted and prohibited goods				Shipping cargo to forbidden destinations		Tax and duty fraud		False reimbursement claims
Evasion of Modus operandi	Absolute prohibition	Licensing requirements	Quota	Anti-dumping policies	Country embargo	Denied & restricted party controls	Taxes & duties completely	Taxes & duties partially	-
1. Complete avaidance of customs controls	x	x	x	x	x	x	x		
2. Undervaluation							x		
3. Overvalution				x					x
4. Underdeclaration of quantity			x			x		x	
5. Misrepresentation of tariff code	x	x	x	x	x	x	x	x	x
6. Misuse of authorizing documentation	x	x	x	x	x	x	x	x	
7. False declaration of country of origin		x	x	x	x		x	x	
8. False declaration of country of destination		x			x				
9. False declaration of consignee		x		x	x				

modities like diamonds and timber. Moreover, by misrepresenting the country of origin, the traffickers can benefit from favorable tariff rates offered for products originating from certain countries (e.g. zero tariff for cargo originating from a third world country or trade union member states).

Declaring a false country of destination allows traffickers to avoid country-specific embargoes and related licensing requirements.

Declaring false consignee allows the trade with blacklisted parties and embargoed countries.

Illustrative case A: Smuggling for duty and tax evasion

Duty and tax evasion is a purely profit-driven customs offence that is probably the most recurrent customs related crime type. The effects of harmful crime of a duty and tax evasion depend on the scale of evasion. Full-scale trafficking enterprises break tax laws on a continuous basis, some whereas otherwise legitimate supply chain operators may commit duty and tax fraud occasionally.

Because no duties and taxes are levied on prohibited goods, duty fraud concerns only trade in legitimate, trade articles. Evading duties and taxes in cross-border trade can be complete or partial. Smugglers can evade taxes and duties altogether when they transport their merchandise into a country using clandestine smuggling routes. For the total and partial evasion, smugglers can defraud customs officers by sending fraudulent import declaration that claims that goods are something else than they really are. For example, duties and excise taxes are significantly lower for chemicals used for agriculture than for oil and gasoline in many customs unions. Underevaluation and underdeclaration of quantity partially avoid taxes and duties. Smugglers also send erroneous data about country of origin and profit from the preferential duty rates that customs unions grant their members or developing countries as development aid. Most attractive commodities for duty fraud include high taxed commodities which have a strong and stable demand on the market. These commodities include mineral oils, tobacco and alcohol.[25]

In an illustrative duty fraud case, a dishonest trader masks a shipment of heavily taxed goods, let say cigarettes, with a cover load of less taxed commodities. At a customs frontier, the fraudster submits a false import declaration reflecting the contents of the cover load. At the end of a successful deception, the fraudster pays less in duties than legally obliged. A typical duty fraudster is an otherwise legitimate a cargo engaged in cross-border trade. In some cases top managers are tempted to tamper trade documentation in attempt to avoid duties ad hoc or on a continuous basis.

Illustrative case B: Terrorism and smuggling of prohibited goods

Customs administrations play an important role in countering the cross-border terrorist activity. They enforce laws and regulations aimed mitigating the threat of international terrorism: they for example control exports to embargoed countries, and control trade in dual goods among other counter-terrorism responsibilities.

Terrorist organizations may be involved in cross-border cargo flows for many reasons. They can take part in international trade, either legal or illegal, in order to generate profits to fund their politically motivated core activities. The terrorists can also attack directly against supply chain structures by infiltrating destructive objects and materials, for example an explosive device, into the cargo flow.[26] Moreover, terrorist networks exploit international supply chains to transport materials, equipment and people across borders in order to prepare and carry out their malicious operations. Smuggled commodities useful for terrorist activity include among other, CBRNe[27] weapons, components and machinery to construct weapons of mass destruction.

Illicit shipments and movements, regardless whether they contain counterfeits, illegal drugs or weapons of mass destruction are smuggled across customs frontiers using analogous methods. Likewise, terrorism related cargo can be transported via the same trafficking networks and smuggling routes as contraband which is smuggled for profits.

In an exemplary terrorism related smuggling case, two kilos of military grade uranium is stolen from a research institute in Country 1. The uranium is transported via clandestine smuggling routes to Country 2 and further to Country 3 with the aid of corrupt customs officers. In Country 3, which is regarded as the main international hub of illicit trade in nuclear materials, the uranium is sold to a terrorist organization. The terrorists employ professional smugglers that traffic the uranium to the final destination to Country 4 by the aid of false documentation, fraudulent customs declarations, and appropriate concealment techniques. In the final destination, the uranium is stockpiled until the terrorists have collected critical mass of highly enriched radioactive to build a weapon of mass effect.

[25] European Commission – Customs 2002. Good Practice Guide.

[26] Recall the Yemen air freight bomb plot in 2010 where terrorists smuggled an improvised explosive device (IED) onto passenger planes.

[27] Chemical, biological, radiological, nuclear and explosive weapons.

Information sources to detect bad actors, bad shipments and bad movements

Overview

Customs administrations collect and process information and data which can be used to identify bad shipments and movements in the supply chain. Customs prefers naturally to work with reliable, accurate, detailed and timely information when they are looking for signs of ongoing customs related illicit activities – assuming such information and data quality would be available.

Customs administrations collect information and data for risk analysis purposes from three main sources: (i) collaboration with other authorities, both domestic and foreign, in order to get intelligence about bad actors, bad shipments and movements as well as emerging threats in the supply chain; (ii) supply chain actors information about the shipments – this can be before, during and after the physical flow crosses customs borders; and (iii) external sources, i.e. third party sources such as media and individual citizens. The information that customs administrations look for pertains to supply chain actors; characteristics of shipments and movements; and external factors that might have an effect on a shipment and movement risk level. The picture below summarizes different sources and types of information that customs administrations may collect for risk identification purposes, and also provides illustrative examples of the actual information / data objects (inside the matrix cells).

Authorities as a source of information

Much relevant data is gathered from various governmental bodies. In many case, authorities that issue licenses, permits and certificates maintain electronic databases of certified operators (e.g. Authorized Economic Operator and Known Shipper, and Regulated Agent databases in the European Union). Other governmental actors, whether national, foreign or international, may share information on risky shipments, suspicious supply chain actors or ongoing criminal activities that might help customs to identify and intercept risky shipments and movements.

Supply chain actors as a source of information

Supply chain actors, namely exporters and importers, as well as carriers, are obliged by law to submit data to customs administrations about exports, transits and imports, for example as part of advance cargo information schemes as well as actual customs declarations. Customs officers may also ask for verbal clarifications of such information and data.

More specifically, the following applies in the EU context: Import Control System (ICS) is a systems architecture developed by the Community for the lodging and processing of Entry Summary Declarations, and for the exchange of messages between national customs administrations and between them and economic operators and with the European Commission.[28] ICS obliges carriers or their representatives to submit pre-arrival information for all cargo entering EU territory for shipment risk analysis purposes. The advanced information must be provided in the form Entry Summary Declaration (ESD) that includes among other things details about contents of cargo, planned routing and traders involved with the movement of the goods.[29] [30] Time limits for lodging the EDS to a customs system vary between modes of transportation. In the case of containerized maritime

	I. Authority	II. Supply chain actors	III. Third party
A. Data is about supply chain actors	E.g. Authorized Economic Operator and Known Shipper databases	E.g. company name and address	E.g. White-list databases on transport operators
B. Data is about shipments and movement	E.g. intelligence from foreign customs administration regarding a specific shipment	E.g. data from a commercial invoice	E.g. Country of origin certificate (can be issued by local Chamber of commerce)
C. Data is about other relevant supply chain entities	E.g. country risk information databases	E.g. an email by a supply chain partner that cargo integrity might have been compromised	E.g. media/news (can be real-time updates on terrorist activities in a specific region)

[28] http://ec.europa.eu/ecip/help/faq/ens7_en.htm#faqsection.

[29] FAQ's: Import Control System (ICS) – Information for UK Traders. Available at http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=true&_pageLabel=pageImport_ShowContent&id=HMCE_PROD1_030208&propertyType=document.

[30] Annex 30A of Commission Regulation 1875/2006 lists required data elements of the ESD.

cargo, cargo information must be submitted 24 hours before loading at the port of origin[31] whereas in road transportation the ESD must be sent at least one hour prior arriving at the customs checkpoint.[32] Operators failing to comply with the ICS regulation face potentially fines, sanctions and delays at the borders. Export Control System (ECS) introduces EU procedures to computerize and control indirect exports[33] and to implement the EU safety and security regulations[34]. ECS is the first stage of an Automated Export System (AES) aiming to computerize EU export system to common standards.[35]

- Consignor
- Consignee
- EORI number
- Country of consignment
- Country (ies) of transit (routing)
- Country of destination
- HS code
- Notify party
- Container owner
- Transport charges
- Method of payment
- Licence
- Country of Origin
- Procedure code
- Duty override code

Just like with ICS, the responsibility to file the required data within the required time schedule lies with the carrier, or another person with the carrier's knowledge and consent. A complete table of ICS/ECS data requirements is presented in Annex I of this paper.[36]

According to a customs expert in FP7-project CASSANDRA, the following sub-set of ICS/ECS data elements can be particularly relevant for risk identification purposes.[37]

Third parties as a source of information

Third parties, including Chambers of Commerce (e.g. country of origin certificates); companies specializing in risk-related information and data collection, analysis and storage (e.g. trucking company and truck driver whitelists); media companies (through news etc.); and (paid) informants and even vigilant citizens can play an important role in the total picture of information and data collection for the purpose of identifying deliberate violations of customs enforced regulations in global supply chains.

Further illustration on information and data sources

A further illustration of sources of information and data for customs is provided in the diagram below.

I. Authority	II. Supply chain actors		III. Third party
Country embargoes (e.g. UN)	Advance cargo information	Declaration data	Company databases, e.g. D&B
Denied parties (e.g. UN)	Post-clearance audit data	Shipping line databases	Chamber of Commerce databases
Criminal records	Port community systems	Aviation and air cargo databases	Media and news
Intel from other agencies			Tips from informants

(source: FP7-project CASSANDRA public materials)

[31] Referred sometimes as the "EU 24 Hour Rule".

[32] www.ics-import-control-system.net/ICS-reglementation.html.

[33] Where an export leaves the EU from a Member State (MS) other than the MS of export.

[34] Set out in the European Parliament and Council Regulation (EC) No 648/2005 and the Commission Regulation 1875/2006/E.

[35] http://customs.hmrc.gov.uk/channelsPortalWebApp/channelsPortalWebApp.portal?_nfpb=tru.

[36] Source: CEN SCS Good Practice Guidebook (pending final approval).

[37] EORI = Economic Operator Registration and Identification ; HS code = Harmonized System code.

1. „In advance“				
2. „Real-time“				
3. „Afterwards“				
4. „Continuous“				
5. Random				
6. Combinations of 1/2/3/4/5				
	A) Operator files automatically	B) Operator files per customs request	C) Customs accesses operator systems	D) Combinations of A), B) and C)

Other information and data management aspects

In relation to a single shipment or a single movement, information and data can be collected by customs at a variety of point of time, five in total (plus combinations), as indicated in the left (y) – axis of the matrix below. Information and data access can be arranged in three basic ways (plus combinations), as explained in the bottom (x) – axis of this diagram.

One can exploit this matrix, for example, when discussing between customs and supply chain operators about “Systems Based Approaches” (SBA), a hot topic in the world of customs at the moment. The first step suggested by the authors of this paper is to map on this matrix what exactly discussion participants mean with SBA (one can mean for example following scenario: y-axis is a Combination of 1. In advance and 5. Random; and x-axis is C) Customs accesses operator systems).

Other aspects can be considered when aiming to create a full framework of data and information source; type; credibility and similar important aspects, when it comes to detection of deliberate regulatory violations in customs context. Two of them are:

By being able to verify or audit the information management systems, e.g. Enterprise Resource Planning (ERP) systems, of the supply chain operators, customs may gain valuable insights on how trustworthy the system outputs are. One relevant question is: How popular could such a “systems quality audit” scheme become, taking into consideration all related costs?

Some of the risk related information and data might exist only in paper format or in verbal explanations – getting it into an IT system can be slow, expensive, or error-prone, etc. One interesting question is: How quickly are paper-based information and data made available for automated processing?

Illustrative cases on information and data enabled risk identification

Overview

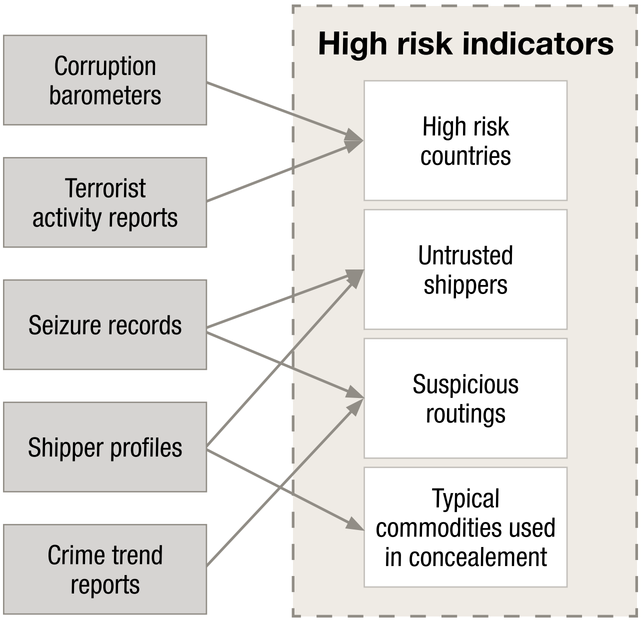
This chapter – the most challenging one in the paper to produce – dives deep into the peculiarities of the actual data elements and related “risk rules”, as “high risk indicators”; as well as into the customs processes dealing with information and data management for risk identification purposes. Also a high-level “risk calculation formula” is illustrated in this chapter. The content of this chapter is based purely on publicly available customs documentation and presentations and other materials.

Illustrative case C: Suspicious information and data values and updating of risk rules

Table below provides 14 illustrative examples on what might be considered as “high risk indicators” by customs administrations, based on the information and data they might have about the shipper; commodity; country of origin; carrier; container; routing and transshipments; and the importer.

The next diagram visualizes how five specific data sources – corruption barometers; terrorist activity reports; seizure records; shipper profiles; and crime trend reports – could feed into updating “high risk indicators”. Again, this is purely for illustrative purposes only.

Supply chain actor / stage	Illustration on what might be considered as "high risk indicators"
Shipper	Shipper has not exported the specific commodity before Shipper information cannot be found from commercial registers or from the Internet
Commodity	Hazardous materials which may be used for terrorist acts: e.g. Sulphur Dioxide and Iridium 192 Common materials which may be used for concealment purposes: e.g. sugar and auto parts
Country of origin	High level of corruption in the country Non-existing (or low) level of export controls: e.g. pre-cursor chemicals, narcotics, and dual use goods.
Carrier	Specific crew associated with organized crime Carrier history of frequent violations of customs enforced regulations
Container	Goods description does not match with the container type or with the total weight of the container. Discrepancies in seal numbers (documents versus actual seal)
Routing and transshipments	Routing of shipment is not cost effective Transshipment cost paid with cash
Importer	The frequency of imports does not support a "sustainable business". A suspect employee is working for the importer.



Illustrative case D: Common risk management framework (CRMF) in the EU

Common risk management framework, CRMF, has its basis laid out in the Internal Security Strategy, (ISS) of the European Union.[38] As part of Objective 4 of the ISS document - Strengthen security through border management – CRMF basics are explained in Action 3: Common risk management for movement of goods across external borders. ISS reference to CRMF is presented in the box below.

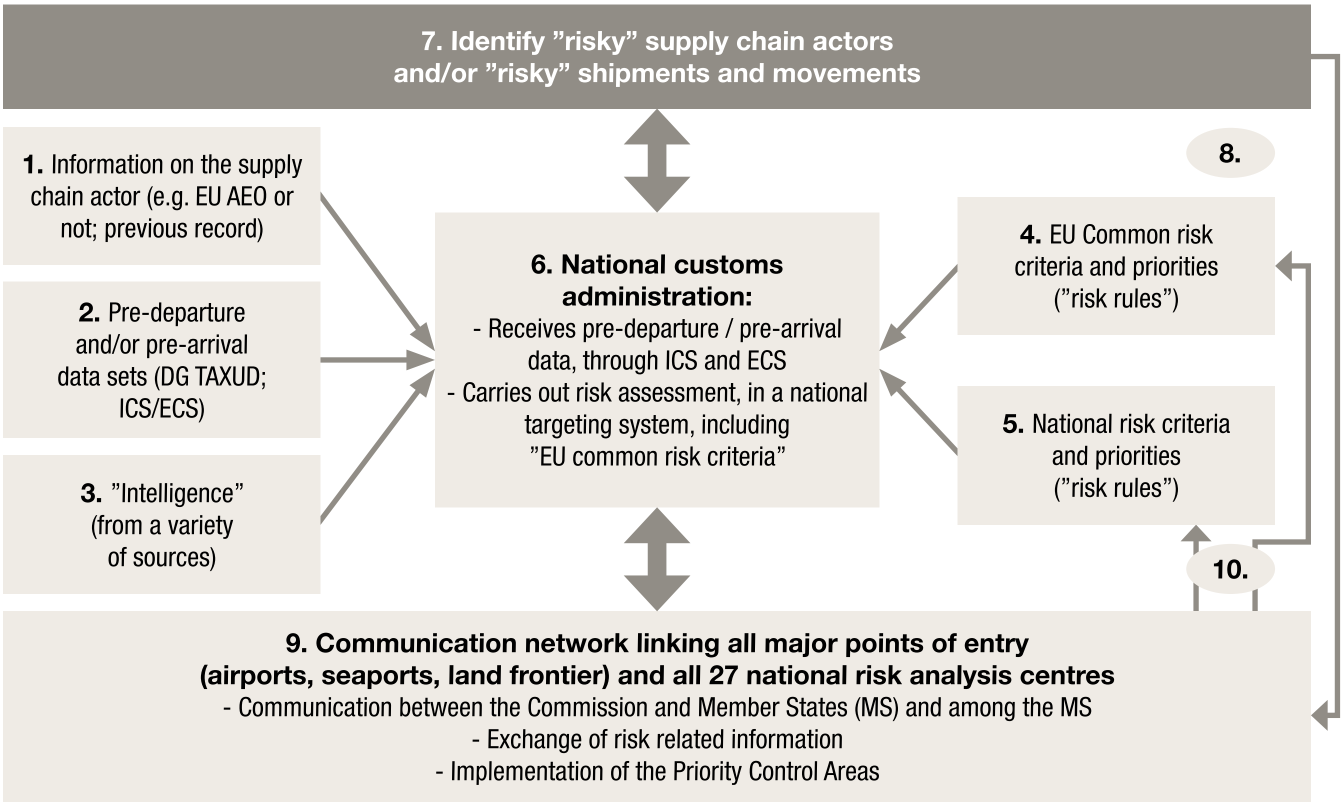
> Significant legal and structural developments have taken place in recent years to improve the security and safety of international supply chains and movement of goods crossing the EU border. The Common Risk Management Framework (CRMF), implemented by customs authorities, entails continuous screening of electronic pre-arrival (and pre-departure) trade data to identify the risk of security and safety threats to the EU and its inhabitants, as well as dealing with these risks appropriately. The CRMF also provides for application of more intensive controls targeting identified priority areas, including trade policy and financial risks. It also requires systematic exchange of risk information at EU level.
>
> A challenge in the coming years is to ensure uniform, high-quality performance of risk management, associated risk analysis, and risk-based controls in all member States. In addition to the annual report on the smuggling of illicit goods referred to above, the Commission will develop EU level customs assessments to address common risks. Pooling information at EU-level should be used to reinforce border security. In order to strengthen customs security to the required level at external borders, the Commission worked in 2011 on options to improve EU level capabilities for risk analysis and targeting and develop proposals as appropriate[41].

A high-level illustration on how CRMF may be meant to function, is explained in the form of a 10-step closed loop process, and visualized right after the numbered list.

1. Customs has data on the supply chain actor (e.g. is the company EU AEO or not; previous record of compliance, etc.);
2. Customs receives pre-departure and/or pre-arrival data sets on the shipment (data set defined in the legislation);

[38] The EU Internal Security Strategy in Action: Five steps towards a more secure Europe. Communication from the Commission to the European parliament and the council. Brussels, 22.11.2010 COM (2010) 673 final.

[39] http://ec.europa.eu/commission_2010-2014/malmstrom/archive/internal_security_strategy_in_action_en.pdf.



7. Identify "risky" supply chain actors and/or "risky" shipments and movements
1. Information on the supply chain actor (e.g. EU AEO or not; previous record)
2. Pre-departure and/or pre-arrival data sets (DG TAXUD; ICS/ECS)
3. "Intelligence" (from a variety of sources)
6. National customs administration:
- Receives pre-departure / pre-arrival data, through ICS and ECS
- Carries out risk assessment, in a national targeting system, including "EU common risk criteria"
8.
4. EU Common risk criteria and priorities ("risk rules")
5. National risk criteria and priorities ("risk rules")
10.
9. Communication network linking all major points of entry (airports, seaports, land frontier) and all 27 national risk analysis centres
- Communication between the Commission and Member States (MS) and among the MS
- Exchange of risk related information
- Implementation of the Priority Control Areas

3. Customs receives intelligence from a variety of sources (other national agencies, foreign customs, informants, etc.);
4. Customs has (in their targeting system) the EU Common risk criteria and priorities ("EU risk rules");
5. Customs has (in their targeting system) the national risk criteria and priorities ("national risk rules");
6. National customs administration Receives predeparture / pre-arrival data, through ICS and ECS; and Carries out risk assessment, in a national targeting system;
7. Customs identifies "risky" supply chain actors and/or "risky" shipments, and takes appropriate actions;
8. Results are passed to the Communication network;
9. Customs shares the results with DG TAXUD and the other member State customs administrations through the secure communication network;
10. EU common risk criteria and priorities and/or national risk criteria and priorities are being updated.

Further aspects on specific risk assessment techniques in the EU

According to European Commission DG TAXUD materials, risk means "the likelihood that something will prevent the application of Community or national measures concerning the customs treatment of goods." Correspondingly risk management is defined as "a technique for the systematic identification and implementation of all the measures necessary to limit the likelihood of risks occurring. International and national strategies can be effectively implemented by collecting data and information, analyzing and assessing risk, prescribing action and monitoring outcomes." According to DG TAXUD, there are three techniques to assess total risk level of an individual shipment:

The first technique utilizes dynamic risk parameters that reflect immediate and typically temporal risks in the customs threat environment (e.g. imports of poultry products from Thailand to the EU during the avian influenza in 2008[40]). Shipments matching the profile that the dynamic risk parameters determine may be flagged as high risk and may be inspected by customs. [41]

[40] www.abs-cbnnews.com/world/11/10/08/thailand-confirms-fresh-bird-flu-outbreak.

[41]The Risk Information Form (RIF) is a possible example of a tool for effective information exchange between member states. The RIF can be used to support targeting and risk analysis in a simple and effective manner at the external frontier.

The second technique of identifying high-risk shipments utilizes fixed risk parameters in the risk analysis. The fixed parameters contain information about historical events such as most frequently used methods of concealment and companies which have committed customs related crimes in the past, thereby allowing the customs to run a statistical analysis.

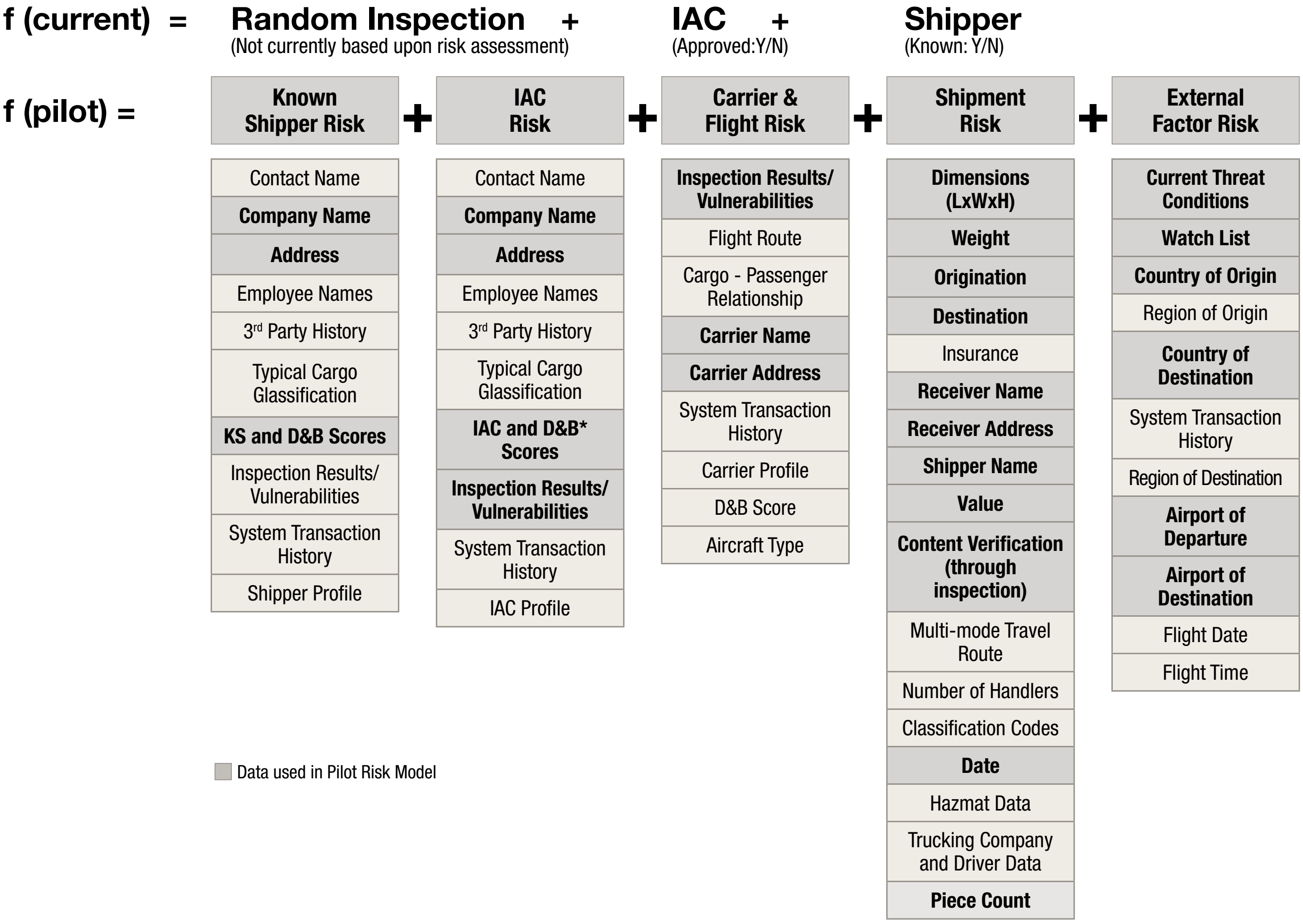
The third method of risk management refers to random selection of shipments to inspection. According the random selection philosophy, every shipment has the same likelihood to be inspected. In practice, the random selection for inspection is done with a computer programme or by manual system based protocols that eliminate subjectivity in the decision-making – still of course not forgetting the importance of customs officer "intuition" as part of the total risk assessment process[42] (both random selection as well as "intuitive" selection are out-of-scope for this paper).

Illustrative case E: TSA's risk model for air cargo targeting

The US Transport Security Administrations, TSA's[43],[44] cargo targeting scheme[45], the Freight Assessment System (FAS), was originally designed to identify "elevated risk" air cargo through pre-screening, focusing on two terrorism-centric security threats[46]:

- Improvised explosive device (IED) exploding on a passenger aircraft;
- Stow-away commandeering an all-cargo aircraft.

The FAS programme was one of the cornerstones of the US Air Cargo Strategic Plan before August 2007, when the "Implementing Recommendations of the 9/11 Commission Act of 2007" came into force. The 9/11 Act legislation mandated the 100 per cent piece-level screening requirement for air cargo carried on passenger aircraft that was in conflict with the FAS's risk-based cargo



f (current) = Random Inspection (Not currently based upon risk assessment) **+ IAC** (Approved:Y/N) **+ Shipper** (Known: Y/N)

f (pilot) =

Known Shipper Risk +	IAC Risk +	Carrier & Flight Risk +	Shipment Risk +	External Factor Risk
Contact Name	Contact Name	**Inspection Results/ Vulnerabilities**	**Dimensions (LxWxH)**	**Current Threat Conditions**
Company Name	**Company Name**	Flight Route	**Weight**	**Watch List**
Address	**Address**	Cargo - Passenger Relationship	**Origination**	**Country of Origin**
Employee Names	Employee Names	**Carrier Name**	**Destination**	Region of Origin
3rd Party History	3rd Party History	**Carrier Address**	Insurance	**Country of Destination**
Typical Cargo Glassification	Typical Cargo Glassification	System Transaction History	**Receiver Name**	System Transaction History
KS and D&B Scores	**IAC and D&B* Scores**	Carrier Profile	**Receiver Address**	Region of Destination
Inspection Results/ Vulnerabilities	**Inspection Results/ Vulnerabilities**	D&B Score	**Shipper Name**	**Airport of Departure**
System Transaction History	System Transaction History	Aircraft Type	**Value**	**Airport of Destination**
Shipper Profile	IAC Profile		**Content Verification (through inspection)**	Flight Date
			Multi-mode Travel Route	Flight Time
			Number of Handlers	
			Classification Codes	
			Date	
			Hazmat Data	
			Trucking Company and Driver Data	
			Piece Count	

▨ Data used in Pilot Risk Model

[42] Documentation confirms that intuition and experience of customs officers continues to be an important selection criteria.

[43] US Transportation Security Administration.

[44] Even though TSA is not a customs administration, it has been intentionally been included in this sub-chapter, for reasons detailed in Chapter 1 disclaimers of this paper.

[45] All information here, as well as in other chapters, is based on publicly available sources. The information presented in this chapter, by purpose, is not fully accurate – thus it can be used only for illustrative purposes.

[46] TSA Air Cargo Programmemes Update, FY2008 Q2.

screening approach and for this reason, the FAS was superseded as the main air cargo screening programme in the US. These days, the FAS serves as the primary targeting system for identifying high-risk cargo requiring secondary screening.[47]

The FAS's Pilot Risk Model, illustrated in the picture on the previous page[48], shows the logic behind the FAS's risk assessment process and the TAS's preceding risk ruling approach that relied heavily on random inspections. The picture presents a set of data elements that FAS designers have considered useful for risk assessment purposes. Data used in field tests in between 2005 and 2006 are indicated with blue color. The Risk Model calculates the total risk level of a shipment as a function of five risk categories: Known Shipper Risk, IAC (Indirect Air Carrier[49]) Risk, Carrier & Flight Risk, Shipment Risk and External Factor Risk.

The Known Shipper Risk[50] evaluates risks associated with the originator of cargo by means of cross-checking reported credentials with Known Shipper databases and company registers, analyzing transaction history of the shipper, assessing shipper related vulnerabilities, etc.

The IAC (Indirect Air Carrier) Risk reflects trustworthiness of air freight forwarders and other relevant intermediates in the USA air cargo supply chains who engage indirectly in air transportation of property.

The carrier and flight Risk covers risk factors such as routing, aircraft type and cargo-passenger ratio. Risk level increases when cargo is transported via low-security level airports, cargo handling terminals and warehouses (e.g. not adequate access control systems in place).

Shipment Risk is calculated on the basis of shipment characteristics considering physical attributes of cargo such as contents, piece count, dimensions and weight; details regarding receiver and destination; transportation conditions for example number of handlers, potential HazMat classification, and secondary mode of transportation. Naturally, any discrepancies with data elements increase risk level (e.g. weight of cargo does not match with reported piece count of contents).

External factor risk reflects the risk of the threat environment where cargo is transported. Risk level of this risk category is determined to a great extent based on intelligence reports on terrorist and criminal activities in certain countries and regions.

Summary and conclusions

The objective of this Discussion Paper has been to shed light on the complicated topic of customs risk management in global supply chains, specifically on the role of information and data in risk identification. The growing public debate on the importance of "risk-based approach" especially in supply chain security policies, regulations and programmes; and on enhanced sharing of "risk related information and data" between supply chain operators and customs administrations, have been a lack of a proper foundation. This paper has intended to provide a robust "discussion platform", while aiming to "show the forest from the trees". The paper started with a simplistic "three-bad logical illustration" on bad actors being involved with bad shipments and bad movements, ultimately causing bad consequences in the society. This was followed by a detailed taxonomy on the variety of violations (criminal and terrorist *modi operandi*) related to customs enforced regulations. Information and data sources, with source categories, data element and timing aspects were discussed next. Finally, several illustrative examples were provided on information and data enabled risk identification in global supply chains.

It is obvious that customs administrations and supply chain operators have both similar but also different interests and priorities – and willingness to pay for - when it comes to mitigating the risk of deliberate violations of customs enforced regulations in global supply chains. In particular, the question on what is the optimum approach to identify terrorism related risks remains to large extent unanswered – but certainly information and data enabled risk identification plays a highly important role in it. The authors of this paper believe that there is a lot of unused potential in two-way sharing of risk related information and data: customs sharing more information for example about criminal and terrorist threats with the supply chain operators; and supply chain operators sharing for example more information and data when it comes to their internal risk management processes and practices. Such two-way communication is likely to lead into more rational usage of "scarce security resources" on the both sides of the fence. Ultimately, one should really see organized crime and terrorism as "the uniting enemy" between customs and supply chain operators – as today it might appear that more time and energy is spent arguing between public and private sector on how the problem should be tackled in the first place. The authors hope that this paper takes the public and private sector actors one step closer to each other.

[47] Homeland Security. IT Programme Assessment: TSA – Freight Assessment System (FAS), 2010.

[48] The picture source is the "TSA Air Cargo Security Programme" presentation hold by Pam Hamilton, Director, Air Cargo, Regulatory Inspections Division, Transportation Security Administration in 30th Annual FAA Aviation Forecast Conference on 18. March 2005.

[49] Indirect Air Carrier is defined by the US legislation as follows: "An indirect cargo air carrier is any U.S. citizen who undertakes to engage indirectly in air transportation of property, and uses for the whole or any part of such transportation the services of an air carrier or a foreign air carrier that directly engages in the operation of aircraft under a certificate, regulation, order, or permit issued by the Department of Transportation . . .or the services of its agent, or of another indirect cargo air carrier".

[50] A known shipper is a shipper that meets TSA's known shipper requirements.

Lastly, the following topics are recommended for future research:

- Assessment of similarities and differences in risk priorities between supply chain operators – separate logistics versus cargo owners – and customs administrations, when it comes to "deliberate violations of customs enforced regulations";
- Evaluation of likelihoods and consequences of "security-sensitive information leaking out " – due to enhanced information sharing between supply chain operators and customs administrations - and/or being used by supply chain insiders to facilitate deliberate violations of customs enforced regulations;
- Feasibility study of joint risk based approaches for multiple governmental agencies with responsibilities in the supply chain – e.g. customs, transport administration, police and phytosanitary – for example within "Coordinated border management" philosophies.

Annex I

The European Commission regulation No 1875/2006 amending Regulation (EEC) No. 2454/93 laying down provisions for the implementation of Council Regulation (EEC) No. 2913/92 establishing the Community Customs Code lays down requirements for entry and exit summary declarations. The annex 30A in the regulation sets the detailed data elements that must be lodged as part of the summary declarations for all goods entering and leaving the customs territory of the EU.

Table below presents required data elements for entry and exit summary declarations for air, sea, inland waterways and other modes of transport or situations. The table excludes following modes of transportation and situations that have their own data requirement:

- Postal and express consignments, ship and aircraft supplies- Entry and exit declaration information;
- Road mode of transport – Entry summary declaration information;
- Rail mode of transport – Entry summary declaration information;
- Authorized economic operators – reduced data requirements for exit and entry summary declarations.

An "X" in the cells of table indicate that the data element is requested at the declaration item of goods level. Correspondingly, an "Y" means that data is required at dec-

Name	Exit summary dedaration (See note 3.1)	Entry summary dedaration (See note 2.1)
Number of items	Y	Y
Unique consignment reference number	X/Y	X/Y
Transport document number	X/Y	X/Y
Consignor	X/Y	X/Y
Person lodging the summary declaration	Y	Y
Consignee	X/Y	X/Y
Carrier		Z
Notify party		X/Y
Identity and nationality of active of transport crossing the border		Z
Conveyance reference number		Z
First place of arrival code		Z
Date and time of arrival at first place of arrival in Customs territory		Z
Country(ies) of routing codes	Y	Y
Customs office of exit	Y	
Location of goods	Y	
Place of loading		X/Y
Place of unloading code		X/Y
Goods description	X	X
Type of packages (code)	X	X
Number of packages	X	X
Shipping marks	X/Y	X/Y
Equipment identification number, if containerised	X/Y	X/Y
Goods item number	X	X
Commodity code	X	X
Gross mass (kg)	X/Y	X/Y
UN Dangerous Goods code	X	X
Seal number	X/Y	X/Y
Transport charges method of payment code	X/Y	X/Y
Declaration date	Y	Y
Signature/Authentication	Y	Y
Other specific circumstance indicator	Y	Y

laration header level and a “Z” that a data element must be submitted on a consignment level.

Comments

Dr. Andrew Grainger
Lecturer in Logistics and Supply Chain Management
Nottingham University Business School
University of Nottingham

Dr. Juha Hintsa and his team have produced an interesting and enlightening discussion paper which looks at the role of information and data in customs risk management. One of this discussion paper’s key aims is to provide clarification about key terms and concepts – or to use a more technical term, it is a first attempt at developing a taxonomy for customs risk management purposes. As such, the authors should be congratulated on their attempt, as indeed, clarity about terms and concepts can inhibit effective policymaking. Feedback to this paper should be encouraged and it is in this vein that I would like to offer some reflective thoughts and comments for discussion.

Taxonomy

The attempt at developing a “customs” taxonomy helps develop clarity about key terms and concepts. In this context, I would like to reflect on when I was part of DG TAXUD’s Trade Contact Group representing EUROPRO. There were a number of meetings relating to the draft and implementation of the “Security Amendment to the Customs Code”. At least initially, such seemingly simple terms like “security” appeared to cause great confusion. For a native English speaker “security” is a relatively unambiguous term. In the Oxford Dictionary it means “the state of being free from danger or threat”. However, in many continental languages, security can have a dual meaning, translating not only into “security” but also into “safety” – which according to the Oxford Dictionary can be defined as “the condition of being protected from or unlikely to cause danger, risk, or injury”. In the context of policymaking this extended understanding of security meant that other regulatory regimes, such as the International Maritime Organization’s (IMO) “Safety of Life at Sea Convention” were brought into play and have, for example, led to the development of the International Ship and Port Facility Security Code (ISPS Code). Indeed, “Safety” has always been a concern – especially in the context of health and safety – and the logistics sector is familiar with a wide range or safety driven rules and regulations ranging from handling specifications (e.g. dangerous goods controls) to product specific specifications (e.g. the CE mark). In the context of export controls – such as for strategic goods (e.g. superfast computers and military equipment) or dual-use goods “security” is more about ensuring that certain types of goods do not fall into the hands of those nations that pose a military risk. Incidentally, in the customs world, the term “security” traditionally refers to financial guarantees (or bonds) against which the administration can draw should the operator be in found in breach with set procedures (e.g. in the context of transit or bonded warehousing). As these examples show, the use of terms like “security” is wrought with confusion, depending on the interests and context within which institutions and their stakeholders use them. Whenever discussing terms such as safety, security, risk and resilience it is essential to be clear about what these terms stand for – hence the need for a taxonomy (language) as is proposed in this paper. Moving beyond this paper, as a next step, it may also be desirable to formally standardize terminology – for example in the context of an official dictionary for customs terms. Inspiration may be drawn from the aviation[51] and maritime sector[52] where organizations like ICAO and IMO seek to standardize key terminology.

What about the “Good actors”?

The research team’s review of “bad actors” is helpful, illustrating in simple layman’s terms what is well known within the wider customs community. Dr. Juha Hintsa and team describe the “bad actors” rather well. However, **I miss a discussion relating to the “good actors”**.

In my view it can be argued that much of customs risk management is about quickly identifying the good actors – those that are responsible for most of the cross-border activity – and distinguishing them from the bad actors, so that scarce customs resources can be optimally deployed. **Good risk management practice is as much as (if not more so) about identifying “good actors” and eliminating them from further investigation, as it is about identifying and perusing “bad actors”.**

This raises the fundamental question of whether the old-fashioned collection of data – be it in paper or electronic means – is the right way to proceed, or whether better mechanisms exist. A view of control that is grounded in the reliance on traders making formal declaration may be somewhat outdated in this context.

[51] See: ICAO resolutions on the “Proficiency in the English language used for radiotelephony”communications.

[52] See: “IMO Standard Marine Communication Phrases (IMO SMCP)(2005 Edition)”.

Do we need to rely on information and data for risk identification?

Dr. Hintsa paper discusses risk and the role of information and data for risk identification in the context of customs, who understand risk in the context of smuggling, duty evasion and certain types of cross-border frauds – a point that Juha Hintsa and his team have well presented! Customs traditionally spends a lot of effort on processing declarations in order to collect duty and revenue and may be predisposed to understanding control in the context of validating and checking the information put to them. However, a point worth making here is that customs over the last few decades (and definitely pre 9/11 and pre AEO) has moved in many areas towards audit based controls – for example in the context of periodic entries (e.g. declaring goods on a monthly basis), duty deferment, and customs warehousing. Control here is more about checking whether traders can be trusted to manage their own affairs in compliance with the set regulatory framework.

Reiterating point 7, **do customs really depend on trade data for risk identification?** Phrased in a different way, can ways be developed that free legitimate (and good) businesses from having to report to the authorities? Certainly such "hands-off" approach to control would free-up valuable customs resource – which in turn could be redeployed to target those "bad actors". Needless to say, such a "hands-off" control approach would also constitute a significant trade facilitation. Rather than declaring data in the form of paper documents and electronic submissions, "good" status may be established by periodic audits, due diligence checks, third party certification, MoUs, linkages between the electronic systems of commercial operators and those of customs (using, for example, pull-type technologies), amongst other methods.

As pointed out by Hintsa et al's paper in Figure 4.1 there are other sources of data that do not come directly from the declarant and his customs declarations. They include, as outlined by Hintsa et al, commercial data captured in the trader's systems (e.g. invoice data), third part sources (e.g. media), and the administration's own intelligence. But there are many more, including MoU agreements and access to businesses' IT systems, whistle-blowing procedures managed by third parties (e.g. NGOs and business associations), tip-offs, as well as the close relationships that may evolve where customs and the private sector work hand-in-hand (e.g. in managing the company's customs authorizations).

Some more technical comments

In the context of violations, it is worth pointing out that the issue of compliance is not quite so black-and-white (compliant or a "bad actor") as made out. I would like to add to Hintsa's discussion, that the range of violations includes "intentional errors" and "unintentional errors". For example, given how complex tariff classification can be, whether a trader has deliberately misdeclared or intentionally is a question of interpretation (and usually at the discretion of the enforcing officer). Moreover, as a former customs consultant, I am all too aware of instances where traders and customs administrations disagree about the correct tariff classifications. Indeed, even within administrations or between the European customs administrations differences in views are frequent – as can be observed when reading national customs tribunal and ECJ cases. In short, whether violations are deliberate or not is seldom clear-cut.

Another issue relating to "violations" is the **integrity of Customs**. The payment of facilitation monies to avoid or circumvent procedures is all too common in many parts of the world. Unnecessarily complex (ie. gold-plated) rules and regulations do not help and provide an incentive for negotiating short-cuts. If we are discussing customs-risk in the context of compliance with set data reporting requirements, than the integrity of the customs administration plays a major consideration. In the UK for example there have been several reports of where HMRC (UK Revenue and Customs) lost large sets of very confidential data.

Even where administrations handle data responsibly, the fear that data could be inadvertently disclosed to commercial competitors can be a real inhibitor to good collaborative practice. For example, many importers are very sensitive about information that show who their suppliers are and at what price they have paid, out of fear that their customers may cut them out of the deal and go directly to the suppliers themselves. Understandably, such businesses are very careful about who has sight of commercial invoices and what information may be attached to the consignment. These are challenges are not easily overcome unless customs can guarantee exceptionally high levels of integrity.

In summary

I do believe that a lot of value can be derived from developing a standardised taxonomy of customs risk terms (e.g. as a WCO recommendation) – and Hintsa's discussion paper certainly provides a good first step.

Juha Hintsa and his team have also made an excellent first attempt at describing the customs environment in terms of risk management and customs data, which is enlightening, especially to the layman.

One of the key questions that remain, at least to my mind, is whether more innovative approaches to establishing good credentials – rather than simply complying with the requests by customs for trade documents and similar data – can be found? Reliance on trade data, be it paper or electronic, appears somewhat old-fashioned.

Further research and case-studies should be strongly encouraged, especially when comparing and contrasting the customs perspective with other stakeholders in the trade environment – e.g. that of businesses, the logistics and transport sector, other government authorities (e.g. those concerned with veterinary and phytosanitary controls, food security, and transport security).

A Trade Facilitation Perspective

Dr. Andrew Grainger | Lecturer in Logistics and Supply Chain Management
Nottingham University Business School | University of Nottingham | Trade Facilitation and Security

Abstract

The topic of trade facilitation is now an established agenda item within mainstream trade and customs policy. Security, especially since 9/11, has lent further impetus into driving trade facilitation up the policy agenda. However, much of the debate appears to be orientated on the draft and implementation of specific trade and customs procedures, such as the Authorized Economic Operator concept, amongst many others. Taking a leaf from Bhagwati, who described the complexity of overlapping preferential trade agreements (Bhagwati 1998), I mischievously described this emerging avalanche of security procedures: "Security Spaghetti" (Grainger 2007). This paper provides an overview of trade facilitation as relevant to security, concluding with the observation that more emphasis on the management of risks – as opposed to procedures – may be called for.

Trade and customs procedures

The topic of trade facilitation is now an established agenda item within mainstream trade and customs policy. This development should not come as a surprise, especially when considering the successes of trade negotiations in the tariff-area and increasing concern for the non-tariff area (Grainger 2011). As such, trade facilitation is closely coupled with: a) the desire to administer trade and customs related controls efficiently and effectively against the backdrop of growing volumes in trade; 2) ongoing negotiations at the World Trade Organization; 3) aid-for-trade considerations; and 4) security – the topical focus of this conference and paper.

Trade facilitation looks at how procedures and controls governing the movement of goods across national borders can be improved to reduce associated cost burdens and maximise efficiency while safeguarding legitimate regulatory objectives (Grainger 2011) – or as Brian Stables adeptly states, trade facilitation is the plumbing of international trade (Staples 2002). As such, the topic is very much concerned about the transaction costs – or friction (to use a mechanical metaphor) – in the relationship between businesses and the many different government agencies tasked with administering trade and customs procedures. While each country is unique, the list of trade and customs procedures to which traders (such as importers, exporters, distributors and brokers), their intermediaries (such as logistics and transport companies) and providers of supporting infrastructure (such as warehouses, ports and airports) are exposed to, can be extensive. Applicable procedures can apply to (Grainger 2011):

- safety and security (e.g. anti-smuggling, the handling of dangerous goods, or the safety of transport vessels);
- revenue collection (e.g. customs duties);
- trade policy (e.g. administration of tariff quotas)
- environment and health concerns (e.g. quarantine controls); and
- consumer protection (labelling, product testing).

Moreover, the number of procedures applicable will increase with the number of countries involved in the trade. Typically this includes the country of export and import, but also any country through which goods transit – especially for landlocked countries (e.g. Figure 1), but

Figure 1 **Illustrative Example: Trade and Customs Procedures for exports from a landlocked country**

Exporting Country

Customs
Expert declaration

Domestic Transit
Additional procedures frequently apply for moving goods from seller's premises to the border

Export Licences (many different line ministries)
Requirements for these can be prolific, especially in developing countries
Application, receipt, fees, queue at government office, attach licence to import declaration

Certificate of Origin
Application, receipt, fees, queue at government office

Sanitary and Phytosanitary
Certain types of goods are subject to sanitary and phytosanitary requirements during transit and in the importing country. The Veterinary Health Certificate, Fumigation Certificate, and similar documents need to be obtained before export

Product specific certificates
Importers in third country are likely to require additional product specific certificates. Examples include: CITES Certificate, Dangerous Goods Declaration, test certificates, quality certificates, product material sheets

Transiting Country

Customs
Unless there is a transit agreement traders will have to make a transit declaration upon entry, arrange for a financial transit security (bond), lodge a transit declaration upon exit and request for the security to be returned
In some countries inspection on entry and exit can be frequent; others may just check transit seals

Sanitary and phytosanitary
Certain types of goods may be subject to sanitary and phytosanitary requirements

Transport Procedures
Vehicle checks (weight, safety), cabotage checks

Immigration Checks
Truck driver, ship's crews
Cargo screening for illegal immigrants

Importing Country

Customs
Import declaration; many countries also require pre-notifications and authorisations

Tariff Quota and Import Licences
Application, receipt, payment of fees, queue at government office, attach licence to import declaration, keep a record of quota amount used

Commercial Procedures
Arrange contract with seller, agree Incoterms, contract with transport and logistics companies, arrange for payment for goods (e.g. letter of credit), insurance

Sanitary and Phytosanitary
Certain types of goods may be subject to sanitary and phytosanitary requirements and need to be declared to the relevant authorities

Immigration Checks
Truck driver, ship's crews
In cargo for illegal immigrants

Domestic Transit
Additional procedures might apply for goods moving from the border to the importers facilities

Source: Grainger 2012

also for those countries that do not benefit from direct shipping services and are dependent on transhipment via terminals located in third countries.

Adding to the trade compliance burden is that the exchange of paper documents and other information is accumulative (Figure 2). For example, a full declaration to customs to pay duty and release goods from customs control is likely to be preceded by summary and advance notifications. In addition, a whole set of supporting commercial documents (e.g. the commercial invoice and transport documentation) and other official documents (e.g. export licences, inspection reports, origin documents, licences, etc.) will usually need to be arranged for. Requirements to register and/or make applications can be similarly burdensome.

Adding to the compliance challenge is that in any international trade operation many different types of organizations are involved, including:

- Traders, such as buyers, sellers, their agents and distributors;
- Transport operators, such as shipping lines, airlines, railway companies, logistics and trucking companies;
- Providers of trade services, such as banking, finance and insurance;
- Operators of transport infrastructure, such as port terminals, airports, stevedores and handling agents, warehouses and electronic information systems; and
- Specialist service providers, such as freight forwarders, shipping agents and logistics service providers (Grainger 2012).

The responsibility and expense for complying with trade and customs procedures will be dependent on the specific commercial arrangements – for example by reference to the Incoterms 2010 (ICC 2010). Compliance cost can be direct, that is the expense of preparing and submitting information to the authorities, and physically presenting the goods where required; or indirect, that is the cost subsequent to direct costs, such as reduced competitiveness or missed business opportunities (e.g. OECD, Peter Walkenhorst et al. 2003).

Figure 2 **Trade compliance interactions between businesses and government**

- **Registrations:** Most authorities will require operators to register before processing any applications, notifications or declarations. Examples might include a company registration, VAT registration or customs computer registration.
- **Applications:** These tend to be a requirement where traders seek special treatment such as preferential duty rates or wish to draw on quantitative quotas.
- **Authorizations:** These are often required so that operators can take advantage of simplified customs procedure or handle goods while under customs control. For example, most ports handling goods for international trade will have a customs authorization allowing them to do so. Authorization may also be required for the handling goods that are normally prohibited or restricted.
- **Advance notifications and pre-notifications:** These tend to be consignment specific and enable authorities to make arrangements prior to the arrival of the goods – for example to inspect goods and ensure that sufficient staff a on standby.
- **Summary or partial declarations and supplementary declarations:** A range of simplified customs procedures allow for goods to be cleared through the port with partial declaration to customs on the understanding that a supplementary declaration, with all missing details, is provided at a later point in time.
- **Full declaration:** Here, all the information necessary to discharge the conditions laid upon the import or export of goods is provided.

Source: Adapted from Grainger 2009; 2007b

Trade facilitation

As outlined, trade facilitation concerns itself with reducing trade compliance cost. To this end, a number of international trade facilitation instruments, recommendations and guidance documents have been developed (e.g. UN/CEFACT and UNCTAD 2002). The organisations involved, include: WTO, WCO, UN/CEFACT, UNCTAD, the World Bank, OECD, amongst others. However, trade facilitation is not just about implementing international instruments in a top-down fashion; trade facilitation is just as much (maybe more so) about identifying and addressing experienced operational frustrations associated with the trade and customs procedures, and finding solutions to these. As reviewed in my earlier work (Grainger 2011), trade facilitation has four interdependent topical focuses: 1) the simplification and harmonization of applicable rules and procedures; 2) the modernization of trade compliance systems; 3) the administration and management; and 4) the institutional mechanisms and tools (Figure 3).

Figure 3 **The Four Interdependent Topics that Define Trade Facilitation**

1. The simplification and harmonization of applicable rules and procedures

i. Harmonization of Procedures
For example: the adoption of international conventions and instruments; and the harmonization of controls applied by the various different government agencie

i. Avoidance of Duplication
For example: regional or bilateral agreements to recognize export controls in lieu of import control; shared inspection facilities, for instance for customs officers, veterinarians, plant health inspectors and health inspectors; and the formal recognition of private sector controls (e.g. in the area of security or quality) in lieu of officially checks.

i. Accommodate business practices
For example: to accept commercial documents (such as the invoice) in lieu of official documents; and to allow goods to be cleared inland, away from the bottlenecks at ports and border-posts.

2. The modernization of trade compliance systems

i. Solutions
For example: use of electronic information systems, the Single Window concepts, electronic customs systems, port community systems, websites, and information portals

i. Standardization
For example: electronic standards for the exchange of information between computers; paper document standards; barcode standards; document referencing conventions; and standards for the description of locations

i. Sharing of experiences
For example: training and awareness building; development of toolkits and implementation guides; collaborative and open source systems developments

3. Administration and Management

i. Service standards
For example: public service level commitments; publish and make available applicable rules and procedures; produce plain language guides; develop online websites; keep the customs tariff up-to-date; provide for efficient appeal mechanisms

i. Management principles
For example: enforcement of controls in proportion to the risk against which they seek to protect; selective (risk based) controls that reward compliant behaviour (e.g. preferential treatment at the border)

4. Intuitional mechanisms and tools

For example: establishing a national trade facilitation body; produce and publish whitepapers setting out reform ambitions and inviting stakeholder comments.

Source: adapted from Grainger (2011); to be published in Grainger and McLinden (forthcoming)

Trade facilitation and security

As outlined, security is a significant trade facilitation policy driver. Since 9/11 a number of new supply chain orientated security initiatives have been launched. Some have been driven unilaterally, such as those of the USA (e.g. CTPAT) and the EU (the Security Amendment to the Customs Code); others have their roots in international institutions, such as the IMO's International Ship and Port Facility Security Code (IPSS Code) or the WCO's SAFE framework of standards. At the risk of over-generalising, they aim to (Grainger 2007):

- Identify security risks before goods move;
- Make efficient use of finite enforcement resources;
- Enhance controls at the border;
- Ensure that wealth-generating trade continues;
- Extending controls up and down the supply chain.

One of the fears, at least for those concerned about regulatory compliance costs, is that where compliance requirements overlap, compliance cost are unnecessary inflated – a phenomena that I mischievously – taking inspiration from Jagdish Bhagwati (1998) – referred to as Security Spaghetti (Figure 5). Noteworthy is that although since 9/11 security plays an ever greater objective in transport and trade procedures, the pre-existing catalogue of safety and security procedures was already vast. To give an example, in the United Kingdom, 37 procedures relevant to safety and security can be counted (SITPRO, Grainger et al. 2008). Broadly, their focus may be orientated across the supply chain ("umbrella"), goods specific, control specific, safety specific, or commercially driven – see Figure 4. Given the potentially wide range of applicable procedures within the safety and security domain, scope for trade facilitation is large. Anyone of the topics as outlined in Figure 3 can be made relevant – be it, for example, by investing into modern IT-systems to collate information, harmonizing procedures (effectively weeding out duplication between countries and cutting down the unwieldy "spaghetti"), or entering partnership agreements with private sector operators and providing them with meaningful incentives to tighten up security internally (Grainger 2010).

Some Observations

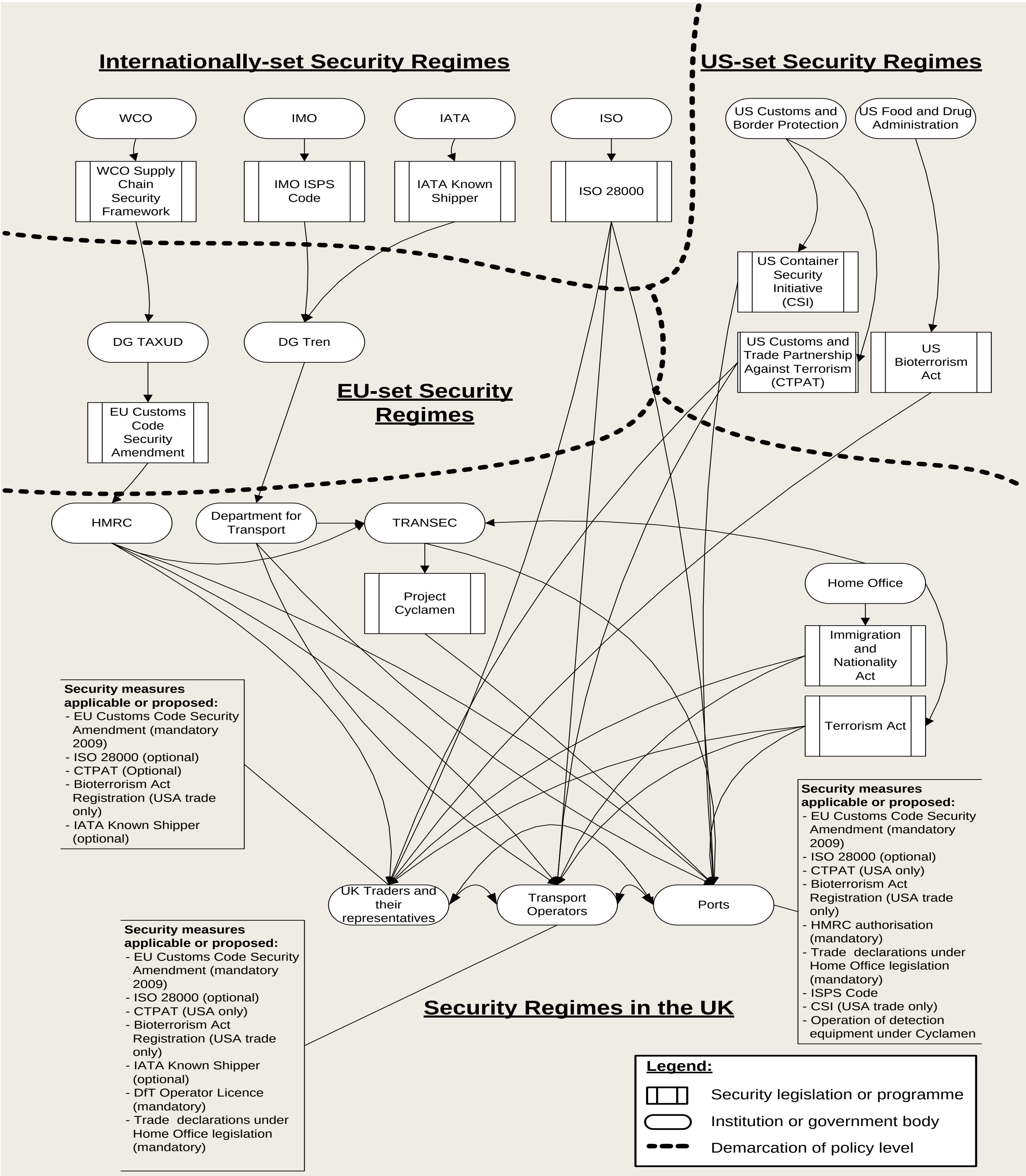
The problem with "security" in the context of trade and customs procedures is that the bigger question of how to protect against risks can quickly go astray. Any cynically minded commentator is likely to point out that it would be very unusual for a terrorist to declare his intentions. Thus, the discussion of security within the context of trade facilitation should be viewed as a means to freeing-up administrative resources, so that it can be put to better use – such as security.

Figure 4 **Security Categories and Objectives**

Category	Objectives
1. Umbrella	**Supply chain security**: Identify risk before goods move **Anti-terrorism**: Ability to build intelligence, identify and respond to threats **Crime:** Build intelligence, prevent, interrupt and stop criminal activities
2. Goods Specific	**Food security:** Ensure food is available and safe for consumption **Bio security:** Prevent harmful diseases and substances from threatening UK life and welfare **Prohibitions and restrictions:** Ensure that sensitive or dangerous goods and technologies are only traded and handled within pre-specified criteria and only by licensed operators, traders and individuals
3. Control Type Specific	**Fiscal Security and anti-smuggling:** Collect revenues; prevent and stop smuggling **Money Laundering:** Identify illegal financial transaction **Immigration Control:** Identify people **Pre-notifications and summary declarations:** Collecting regulatory information in advance of subsequent declarations
4. Safety Specific	**Public safety:** Welfare and safety of the wider public consuming or using goods **Safety of staff:** Welfare and safety of people handling and moving goods **Safety of critical infrastructure:** Ensure that critical infrastructure is protected; ensure that contingency plans are in place should infrastructure and systems fail
5. Commercial	**Business security:** Ensure that risks associated with business and international trade are managed within the firms appetite for risk (e.g. due-diligence, insurance instruments, MoUs)

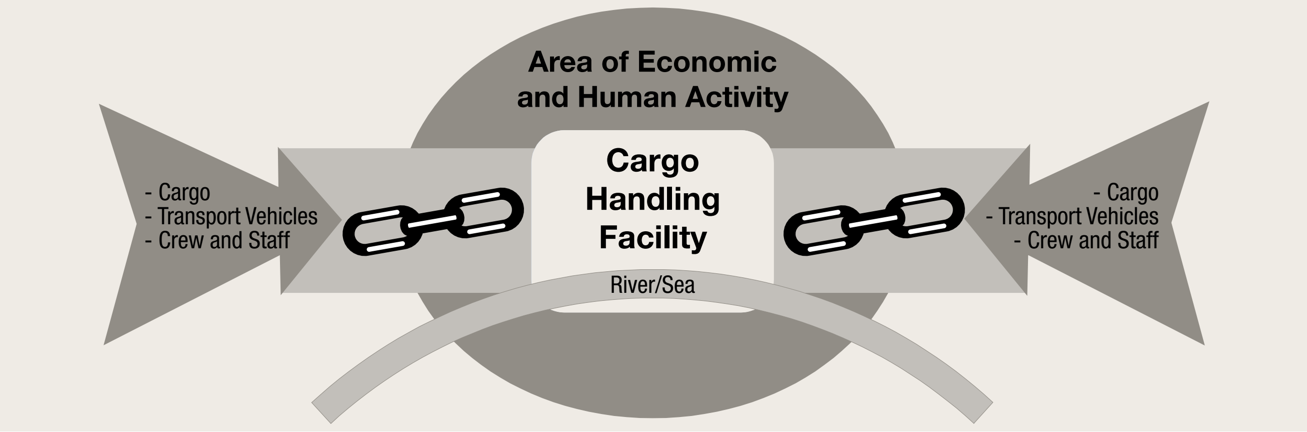
The problem with “supply-chains” is that they are by nature very fluid and flexible systems, shaped by market dynamics and the commercial arrangements amongst its constituents. Moreover, those best placed to manage particular risks may not necessarily be those with the greatest interest in safeguarding against them. Phrased in the reverse, those that have most to fear may not necessarily be best placed to put measures in place to mitigate risks.

Figure 5 **“Security Spaghetti”**


Internationally-set Security Regimes
US-set Security Regimes
WCO
IMO
IATA
ISO
US Customs and Border Protection
US Food and Drug Administration
WCO Supply Chain Security Framework
IMO ISPS Code
IATA Known Shipper
ISO 28000
US Container Security Initiative (CSI)
DG TAXUD
DG Tren
US Customs and Trade Partnership Against Terrorism (CTPAT)
US Bioterrorism Act
EU-set Security Regimes
EU Customs Code Security Amendment
HMRC
Department for Transport
TRANSEC
Project Cyclamen
Home Office
Immigration and Nationality Act
Terrorism Act
Security measures applicable or proposed:
- EU Customs Code Security Amendment (mandatory 2009)
- ISO 28000 (optional)
- CTPAT (Optional)
- Bioterrorism Act Registration (USA trade only)
- IATA Known Shipper (optional)
Security measures applicable or proposed:
- EU Customs Code Security Amendment (mandatory 2009)
- ISO 28000 (optional)
- CTPAT (USA only)
- Bioterrorism Act Registration (USA trade only)
- HMRC authorisation (mandatory)
- Trade declarations under Home Office legislation (mandatory)
- ISPS Code
- CSI (USA trade only)
- Operation of detection equipment under Cyclamen
UK Traders and their representatives
Transport Operators
Ports
Security measures applicable or proposed:
- EU Customs Code Security Amendment (mandatory 2009)
- ISO 28000 (optional)
- CTPAT (USA only)
- Bioterrorism Act Registration (USA trade only)
- IATA Known Shipper (optional)
- DfT Operator Licence (mandatory)
- Trade declarations under Home Office legislation (mandatory)
Security Regimes in the UK
Legend:
Security legislation or programme
Institution or government body
Demarcation of policy level

Source: Grainger 2007

Figure 6 **The port as an interdependent system**



Source: Anand and Grainger 2011.

Take the example of a port. It can be viewed as a handling facility for the safe loading and unloading of ships. It can also be viewed as a node in the supply chain, the choice of ports will be dependent on cost and service. The port can also be viewed as an area of human and economic activity where people work, live and pursue their leisure (Figure 6). Each of these perspectives allows for different risk perceptions. For example, a ship that sinks in the port's access channel may be no more than an insurance case for the shipping line, but for the terminal operator it may translate into a temporary period of severe disruption. For parties further up or down the supply chain this disruption may translate into failures to meet customer expectations and loss of business – for example because delayed critical supplies have meant that production had to be halted. For local residence the sinking of the ship may prove to be a significant inconvenience brought along, for example, by long-term environmental pollution and threat to drinking water. While the vessel's operator is likely to be the person best positioned in preventing the ship from sinking, those located around the port may stand to lose the most.

The task for policymakers is to ensure that those best able to manage risks are suitably incentivised – or coerced – into reducing risks. Given the multitude of interests at work and industry sectors involved in international transport operations, this is no small task. At the risk of over-generalising, risk management in the context of security and international trade is very much focused on individual organizations – such as the Authorized Economic Operators. Even formal security management systems, such as ISO 28000 for Supply Chain Security, or BS 25999 for Business Continuity, take the individual organisation as its primary unit of focus. In contrast, a shift in view towards capturing and addressing inter-organisational (systems-wide) risk dependencies may be desired.

Proposition

The ideas of trade facilitation, as outlined in Figure 3, can significantly help reduce the burden associated with the compliance aspects of trade and customs procedures – including those that have safety and security type objectives.

However, if the aim is to manage security risks – as opposed to mitigating the regulatory compliance burden – than a more systematic understanding of risks and security within international trade operations is desired. Given the complexity of international supply chain operations, few attempts have yet been made at unravelling system wide risks and dependencies. Questions such as who is affected and who is best placed at stopping risks from materialising need to be asked more rigorously.

If risk and its management – as opposed to the administration of procedures – were to be prioritised, then it may be useful to start thinking about appropriate research that helps shape a better system-wide understanding of risks. This effort could be strengthened by developing appropriate tools and institutions, for example: system wide risk registers and impact assessments, models and simulations, and dedicated forums for stakeholders to come together. Moreover, existing private sector initiatives, for example those relating to risk reporting (such as required in annual reports) or business continuity planning, could be aligned with the security interests of policy makers.

Given the complexity of international supply chains and trade operations, much work remains in terms of: a) identifying risks and dependencies; as well as b) the development of suitable policy measure to maximise public welfare.

References

Anand, N. and A. Grainger (2011). The port as a critical piece of national infrastructure. Working Paper, Nottingham University Business School.

Bhagwati, J. (1998). "Trading Preferentially: Theory and Policy." The Economic Journal **108**(July): 1128-1148.

Grainger, A. (2007). "Supply chain security: adding to a complex operational and institutional environment " World Customs Journal **1**(2): pp.17-29.

Grainger, A. (2010). The Role of the Private Sector in Border Management Reform. Border Management Modernization. G. McLinden, E. Fanta, D. Widdowson and T. Doyle. Washington, World Bank**:** 157-174.

Grainger, A. (2011). "Trade Facilitation: a conceptual review." Journal of World Trade 45(1).

Grainger, A. (2012). Trade Facilitation. Ashgate Research Companion to International Trade Policy. Ken Heydon and Stephen Woolcock. Aldershot, Ashgate.

ICC (2010). Incoterms 2010. International Chamber of Commerce. Paris, ICC Publication.

OECD, Peter Walkenhorst, et al. (2003). Quantitative Assessment of the Benefits of Trade Facilitation. Working Party of the Trade Committee. Paris, OECD. **T**D/TC/WP(2003)31/Final.

SITPRO, A. Grainger, et al. (2008). A UK Review of Security Initiatives in International Trade. London, SITPRO.

Staples, B. R. (2002). Chapter 16 - Trade Facilitation: Improving the Invisible Infrastructure. Development, Trade, and the WTO: A Handbook. B. Hoekman, A. Mattoo and P. English. Washington, World Bank**:** 139-148.

UN/CEFACT and UNCTAD (2002). Compendium of Trade Facilitation Recommendations UN/CEFACT, UN. ECE/TRADE/279.

Comments

Prof. Dimitrios A. Tsamboulas

Department of Transportation Planning and Engineering

National Technical University of Athens

Dr. Grainger's contribution is a very well written and highly interesting paper addressing an internationally recognized, timely and important topic of security risk in trade facilitation. With the growing concern surrounding terrorism and other threats, trade security has become increasingly important. In addition, trade facilitation remains one of the key pillars of the global economy, as well as of the individual development of countries, involving a vast variety of stakeholders, products, infrastructure and services while any disruption (due to security issues in this case) to its smooth operation can have severe adverse impacts. To this end, finding the correct balance between trade security measures in a way that these do not impair international trade flows is a key challenge. Within this scope, the paper thoroughly describes current trade and custom procedures, while at the same time developing strong arguments to support the conclusion that more emphasis on risk management is called for, as opposed to procedures.

Given the above, I am of the opinion that there are certain points that need further elaboration/consideration:

Figure 1

This is an informative diagram depicting trade and customs procedures for exports from a landlocked country. It is, however, suggested that it is supplemented with the respective procedures regarding non-landlocked countries, as well as import procedures. This would allow for a direct and interesting comparison between the two types of countries. One should also consider that there is only a limited number of landlocked countries in the world, the majority being countries with sea access.

The interactions between business and government are well described in **Figure 2**. However, it would be worthwhile to further enhance this analysis with the interactions between the government and the groups listed later on in the paper, such as traders and transport operators, since these form key players in the entire supply chain.

It is of particular importance to include transport operators in **Figure 3**, since these form an integral part of trade facilitation and should not be excluded.

Regulatory compliance costs

The discussion about regulatory compliance costs should be further enhanced to explore how such costs affect the final product price. For example, in the case of higher security costs, are insurance costs reduced, and, thus the regulatory compliance costs are set off by such decrease?

Figure 4

is an impressive graphical presentation of security regimes. Nevertheless, it would be of greater research significance to depict the effects of security regimes in the specified sectors, namely the traders and representatives, the transport operators and the ports.

Figure 5

The mention of UK in Category 3 should better be avoided, as it renders the table country specific, whereas it should be of a more general character. Another helpful addition might be to include the list of involved stakeholders for each category, as well as impacts and related costs. Finally, another category should be added corresponding to "Location" specific, identifying critical infrastructure, since a fair amount of work has been carried out in the security sector with regards to identifying and protecting critical infrastructure. According to Executive Order 13010 (12), critical infrastructure is defined as "Infrastructures so vital that their incapacitation or destruction would have a debilitating impact on defence or economic security" (Critical Infrastructure Protection. Executive Order 13010. Federal Register, Vol 61, No 138, July 17, 1996).

Description of port operation

The description of the port operation is indeed an indicative example of the diversity of risk perceptions. It is recommended that the character of the port as a dynamic nodal point in the entire supply chain is further highlighted, and that there is higher security risk related to the interaction of all the different actors involved. The latter would further support the very accurate statement made by the author that a shift towards capturing and addressing inter-organizational risk dependencies may be desired.

It is recommended that the author introduces the concept of "supply chain resilience", that is the ability of a supply chain system to reduce the probabilities of disruptions, reduce the consequences of those disruptions, and reduces the time to recover normal performance. The topic of resilience emerged a few years ago in the supply chain literature, and is nowadays more widely recognized as critical to uninterrupted trade. To this end, the concept of resilience is highly relevant to the content of the paper.

Proposition Section

In the question of who is affected and who is best placed at stopping risks, the author should also add who takes responsibility for security.

It is recommended to elaborate more on the World Bank proposed six indicators for Logistic Performance Index (LPI) which are quite relevant to trade facilitation (J. Arvis, M. Mustra, L. Ojala, B. Shepherd, D. Saslavsky, "Connecting to Compete 2010: Trade Logistics in the Global Economy-The Logistics Performance Index and its indicators", World Bank, 2011). These indicators are:

- Efficiency of the customs;
- Clearance process;
- Quality of trade and transport-related infrastructure;
- Ease of arranging competitively priced shipments;
- Competence and quality of logistics services;
- Ability to track and trace consignments;
- Frequency with which shipments reach the consignee within the scheduled or expected time.

It would beneficial to explore of adding a new indicator: security. This could be further elaborated by the author.

It is recommended that the development of standard operating procedures in case of an incident (incident management) is added to the risk reporting and business continuity planning in the concluding paragraph. Also, IT services should be mentioned in terms of how these can support such operations.

9

Our Passenger is Our Partner – A programme to improve safety in Israeli Railways

Mr. Michael Cale | Clinical and Traffic Psychologist | Cognito, Israel

Traffic accidents happen. They really do.

In spite of our more or less serious attempts as road users to be attentive, law abiding and careful, accidents might, do and will occur. In spite of the authorities excellent planning and design, strict law enforcement and wise education, some accidents do and will happen.

Let's face it. The zero vision is a long way away.

But not only traffic accidents threaten us, natural and man-made disasters happen too. In spite of precautions, serious attempts at prevention and safeguards by authorities and citizens alike, accidents and disasters do happen.

In this connection we face the fact that things can actually get worse. Secondary accidents are no rare occurrence. After collisions, other drivers get curious, look the wrong way, brake suddenly (or don't brake at all), get scared, curious or confused, do not realize there is oil on the road, don't see paramedics or others performing emergency procedures, policemen redirecting traffic or injured passengers on the ground.

And the problem is by no means restricted to traffic accidents. What about a fire in a cinema, store or train? What about mistakes because of shock, panic or disorientation? The damage caused by secondary accidents can potentially be no less terrifying (and maybe even worse) than that from the initial one.

A recent example: in autumn 2010 the head of the safety department of the Israeli railways requested a study from me in my position as a traffic psychologist. The Israeli railways is currently building its first long tunnel (more than sixteen kilometers long) for the new line from Tel Aviv to Jerusalem. The initial questions posed were:

- What behaviour should be expected from the passengers if and when fire breaks out in the train which is then forced to stop within the tunnel?
- Must one expect panic, irrational and/or dangerous behavior, passengers stampeding just to get out?
- Will they be at risk of crossing the trucks and being hit by a train coming in the opposite direction?

If so, are there ways to minimize the potential dangers and damages by influencing passenger behaviour?

Outsiders and professionals alike might consider this project overly academic or even superfluous and a good example of how psychologists manage to push their noses into everyone else's business. Three days after I handed in my report with explicit recommendations, a train on its way from Natanya to Tel Aviv caught fire on the open track. In the investigation report which was published some months later, the fault was assigned to a screw which had been left ten years earlier during routine repairs in the Danish factory.

The good news is that no one was seriously hurt and that there were luckily no fatalities. The bad news is that the word "luckily" was well chosen. When the fire was recognized the passengers reacted with disorientation, helplessness and panic. The train stopped but no one could figure out, how to open the door. Anger at the railways ignited quickly but anger does not open doors. After some minutes a "brave" border guard loaded his rifle and heroically shot and shattered a number of windows permitting many passengers to climb out (and regrettably sustain cuts and bruises while fleeing the burning train). In this situation, fire was undoubtedly serious but the real dangers lay in whatever the passengers did or did not do.

When we wonder to ourselves, what is to be expected in case of a disaster, most of us are likely to imagine panic, cruel battles to survive leading to stampedes. We base these assumptions on memories of the stampede during the haji (pilgrimage) in Mecca, the tragedy which occurred during the finals of the European soccer cup in Belgium, the fire in the London underground, the kids who were killed trying to push their way into a pop concert in Arad, the catastrophe of the Love Parade in Duisburg in 2010 or similar events. These memories are indeed real and they represent the truth but luckily, not the whole truth.

It is also true, as described above, that secondary road accidents are not rare (we may assume that some 10 per cent of the fatalities on the road are related to this type of accident), that people do panic, react wrongly or perform other dangerous behaviours as a reaction to imminent dangers.

Many studies have shown that human beings are not always egocentric, don't always panic and are not always tuned into going over bodies to save their own lives. Many incidents have been recorded in which total strangers helped each other along and saved other people – frequently at the cost of their own lives. Remember the plane which crashed into the Pontiac river, the stories around 9/11 and many, many other incidents. They are less well-known because they are simply less newsworthy.

Disaster or no disaster – that is the question

The question why one disaster situation will end tragically due to inappropriate behaviour of those involved but another will not is indeed very intriguing. To answer this question, I would like to refer to two bodies of research which were published some twenty years apart. The first is a series of experiments performed about thirty years ago by two prominent social psychologists: Darley and Latanee. Beginning their quest from the tragic story of Kitty Genovese who was raped and killed with at least thirty neighbors looking on without intervention, they wrote a number of studies aimed at finding out who and what causes people to help or to refrain from helping others in emergency situations.

To make a very long and fascinating story short, the researchers found that humans function based on a four stage model.

The first step is to perceive the emergency. As shocking as it may be, studies and film footage from many sources show people passing and ignoring others in need of help on the sidewalk or subway as if they were made of thin air. If we do not perceive an emergency, we naturally will not respond to it.

In the second step, we judge to decide if it is indeed an emergency. It might be interpreted as kids playing, a prank, an actor or a harmless occurrence. If we conclude that it is no real emergency, we will consider ourselves free to continue with whatever we were doing.

In the next step, we decide if it is indeed up to us to intervene or help. Studies have documented many incidences (and indeed the Kitty Genovese case was one of them) in which people disperse responsibility and assume someone else will or should help.

In the last step, we must confirm to ourselves that we have the tools needed to intervene, that we know enough about emergency procedures, have a cell phone to call the police or can find the fire extinguisher and put out a fire.

A most fascinating point is, that if we answer to one of the questions above negatively, we tend to go back a step and reconsider the previous answer. For example, if you decide that you are not qualified or able to help you will most likely go a step back and decide that getting involved is not really any of your business. Latanee and Darley (and other researchers too) have shown that people will go back to step zero and claim they never even saw the person lying on the ground, never heard the victims screams, never perceived the smoke filling the room.

In emergency situations (and in fact in many other ones too) we tend to look at others to get hints of how we should behave. If other people react competently, helping others, the outcome can be expected to be favorable. However, if other people disregard the smoke filling the room or do not stop to help someone lying on the sidewalk, it is extremely likely that we will act in the same manner. If we only see and perceive hysterical panic reactions, we will indeed model our behaviour accordingly.

Our tendency to look for cues in other people's behavior is both part of the problem and the solution in one. Accordingly, we may say that in order to prevent dangerous behaviour in emergency situations it is necessary to:

- Create a minimum number of competent and charismatic people who can serve as credible role models;
- Give passengers the knowledge and tools needed to intervene in an emergency situation;
- Prepare as many passengers as possible so that they will be of the opinion, that it is their responsibility to intervene and help others and believe that they are capable of doing so.

The second line of research I would like to refer to is best represented by E. Scott Geller. Dr. Geller frequently refers to the term "empowerment". According to Geller, three requirements are essential to get people to make real changes – especially in the realms of health and safety promotion:

- First of all the person must subjectively believe that whatever is supposed to achieve is a real issue, which must be solved (e.g. saving lives). People will not even consider making an effort to obtain changes for something they do not care about. It can be perceived as important to have a prominent social role, keep yourself fit or simply to get home safely;
- Secondly, the person must believe, that he or she is capable of doing whatever is required to achieve that goal. You cannot expect a normal adolescent to refrain from partying, someone suffering from ADHD to sit quietly in class for an hour or an untrained passenger to help other passengers escape from the burning train;
- The third requirement demands that the person we try to influence believes, that there is an excellent chance that the "real" goal (as described above) will be achieved if he or she does whatever we require. If you use condoms you are not at risk to get AIDS, if you use a designated driver who does not drink you are much more likely to get home safely, if you prevent panic on the train it is much more likely that everyone will get out safely.

To sum this part up, the potential secondary damage to an emergency situation, e.g. fire on a train can be limited if you assure two things:

- Make sure that people feel empowered to intervene. They must realize the importance, feel capable of intervening and be convinced, that their intervention and behaviour will save the day;
- Make sure that there are sufficient positive role models available and that the passengers are and feel they are capable of successfully intervening.

Perception

Many studies and books have been written about the rules of perception, learning and cognition and no attempt will be made here to repeat them. There are even serious publications defining "better practice" in railway environments (see RSSB (2010), RSSB (2006) or Technion (2006)). The important point to be made is that information which we want people to notice, perceive and learn must be presented in such a way that this is possible and extremely likely to be processed correctly. In a later part of this paper, I have listed principles to guide the planning and performance as far as what should be done or provided. Here I would like to list a number of things that should not occur:

- We must prevent stimulus and information overload;
- We must prevent situations in which the critical information is only presented during an emergency;
- We must prevent situations in which passengers cannot perceive, comprehend or use the critical information.

As reported above, the Israeli Rail decided to take preventive action against the possibility, that fire breaks out on a train especially in a tunnel. Given the nature of life in Israel the plan should also include the need to evacuate a train due to terrorist attacks, problems due to extended, unscheduled stops in extremely hot weather conditions, technical problems and emergencies based on accidents (Israel has only 95 level crossings but the barriers are destroyed by vehicles driving through some 400 times a year.

Additional consideration had to be given to the following facts:

- Israel is a multilingual country with people speaking Hebrew, Arabic, English and Russian;
- Train rides are relatively short (no more than two hours);
- The population using Israeli Railways is very heterogeneous including many soldiers (Israel has mandatory draft with soldiers in uniform riding free on trains);
- Israeli Railways has currently a rather negative public image.

Working Assumption

As referred to above, one basic assumption was that the time of an emergency situation is not suitable to teach, train or inform the passengers. During the fire on the train reported above a large number of passengers panicked because, according to their perception, they had no idea how to open the doors (in the end a soldier shot through some of the windows). Some of them were interviewed on the evening news complaining about the fact that no one told them how to open the doors while a large sticker with extensive, verbal explanations were just behind them.

Accordingly, it was decided to create a situation in which passengers can be expected to respond appropriately in the event of an emergency and not to build the solution on the assumption that passengers will read extensive handbooks or stickers while under stress.

Needs and limits

We realized that various groups of passengers use the railway so as a first step, a number of different passenger groups were defined so that we could be sure we cater to the vast majority of passengers.

Average Passenger	Citizen who travels by train on an average between once a week to about once a month	A passenger who is basically familiar with the railway environment. Has spent time waiting and or riding but not on a daily basis.
Experienced Passenger	Uses the train daily or a number of times a week.	Gets around the train and the station without having to think or plan.
Elderly	Passenger aged 60 or above who is physically able and can ride the train without support.	Similar to above but older. In emergency situations might need assistance and might react extremely.
Soldiers	Israel has mandatory conscription and soldiers travel free of charge.	Young, healthy, responsible passengers who can easily be trained.
“Hi-techer”	Professional commuter with a high cognitive level who will grasp situations quickly.	They frequently work on their desktops which make them clumsy and frequently listen to music or lectures on electronic equipment.
Airport	Israel Railway reaches Israel’s only international airport with more people choosing to get there by train each year.	Frequently inexperienced, excited and overtired and carrying much luggage.
Group	Groups of younger or older passengers who will look at each other in emergency situations	Group members might wait for each other and/or relate to hints from close group members rather than members of the general public.

The next issue to be decided is where emergency situations can be expected. The following places were defined:

Between the gates of the station and the platform	Prevent potentially dangerous disturbances in flow of passengers
Waiting on the platform and getting into train	Prevent crowd behavior leading to people being pushed onto the lines
Normal train ride	Ensure general safety behaviour
Ride in a congested train	Make sure that people do not fall on each other, case panics or alike
Emergency or unexpected stop outside of a station	Prevent panics, restlessness, anger and frustration which may lead to dangerous situations
Emergency stop in a tunnel	Ensure safe disembarquement

The resulting programme which is currently being developed had a number of different units which will be presented briefly below.

Welcome message from the attendant

Whoever has flown on a commercial aircraft will be familiar with the welcome speech or clip presented by the flight attendant. During this, you learn over and over again, how to fasten your seatbelt, use oxygen masks or flee the plane if it lands on water. This recorded clip or live welcome serves many purposes including calming the passengers and giving a feeling that there is hope even if the plane is in difficulty, giving real and important information, keeping the passengers quiet and mesmerized while getting the plane ready for takeoff, making the passengers feel that, the team is in control. In our programme, we will use central LED screens to broadcast such a video clip. In the following table you can see the contents of the clip compared to a standard, airline one.

These clips will be shown in Hebrew every 30-45 minutes raising the likelihood that each passenger will see the clip at least once each trip. Each time there will be subtitles in one of the following languages: Arabic, English and Russian.

Most passengers (see the groups) will see the clip numerous times (like frequent flyers do) and passively become acquainted with the safety precautions. Additionally, we expect the procedure to improve the travel experience and raise the confidence of the passengers in the railway services.

Item	Plane	Train
1	General, personal welcome ("captain xyz and his crew would like to welcome you..")	Similar, personal welcome by train driver. Mentions the staff members who are at your disposal at any time
2.	Please put your luggage in the overhead compartments or…	Please put your luggage in the overhead shelves, the storage areas near the doors or…
3.	Please do not leave objects in the aisle or in front of emergency exits	Please do not leave objects in the aisle or in front of exits
4.	Information about closing and opening safety belts	There is no requirement to be belted but for your safety we recommend that you be seated at all times
5.	Where are the emergency exits and how are they used	Where are the emergency brakes. Explanation when and how they may be used
6.	Choose the closest emergency exit	In the extremely unlikely event of an emergency, please leave the train from the closest door. Leave all belongings behind. Do not cross onto the other rails but get out of the train and down the embankment as quickly as possible."Explanation of how to open doors and descend outside of a station
7.	Emergency	Where hammers can be found to break windows
8.	How to open emergency exits	How to open doors (Repeat)
9.	Use of lifebelts	Use of emergency phone number (under what conditions, what to expect, no need for everyone to call)
10	Oxygen masks	
11	Do not use cell phones	Please respect the other passengers and refrain from loud cell phone conversations or loud music
12	Referral to card with additional safety information	Referral to card with additional safety information
13	Non smoking flight	No smoking trip
14	Repeat personal welcome	Repeat personal welcome

Signs outside of the trains

Getting around a railway station, boarding the train and leaving the station after arriving at ones destination is more complex than one might assume. For safety reasons we want the flow of movement to be as smooth as possible without disturbances or dangers. Thus, it is vital to have all important information presented in such a way that nearly all passengers know how to proceed as intuitively and easily as possible.

The situation today is complex with many stations lacking information and others suffocating the customers with information overload. Important information includes but is not limited to:

- Directions of movement, use of mobile stairs;
- Places where it is safe to stand and wait;
- Public toilets;
- Places in which smoking is permitted;
- Forbidden behaviour;
- E.T.A. and departure of the next train(s);
- Fresh water fountains and first aid stations;
- Line(s) you may not cross;
- Shopping and recreational areas;
- Ticket counters and machines.

Signs for these pieces of information will be based on a number of empirically based criteria:

- Extensive use of pictograms;
- Minimal use of verbal messages (remember, they must be in four languages);
- All signs positioned at height of 165 – 175 cm (within the active visual field of most adults);
- Use of colours (green = required or permitted, yellow = pay attention, red = danger, forbidden);
- Bigger pictograms point at closer objects;
- Consistent use of the same signs (including arrows and pictograms) in all trains and all stations;
- In areas which carry information signs, no other information (e.g. advertisement) may be posted.

Signs within the trains

There will be visual signs inside the trains to support and add to the information presented in the video clips (see paragraph 1). It will include:

- Hotline telephone number;
- Where the emergency brake is placed and how to use it;
- Where a fire extinguisher is placed and how to use it;
- Where an emergency hammer is placed and how to use it;
- How to open the doors under normal conditions and in emergencies.

The signs are prepared according to the same principles which appear in paragraph 2 and, as mentioned above, are referred to in the clip (see paragraph 1) and do not contradict principles defined by RSSB (2010).

Auditory information

People react more calmly and in a predictable manner if you let them believe, that they know, what is happening, what they should expect and that they are in control. It is important to prevent rumours from spreading and people from panicking because they misinterpret the situation. Israeli citizens who are trained at being alert tend to react quickly, have been known to lose their patience and become frustrated if there are unexpected delays or changes. The current author experienced one such instance when travelling by train from Haifa to Tel Aviv. The train stopped to let passengers in from an earlier train which had broken down. Within just a few minutes, everyone in the crowded train was talking angrily and very emotionally about the rail company and two lawyers started signing people up who wanted to sue. Such reactions are more than unpleasant and can lead to mutiny and disruptive behaviour.

As part of the programme recordings are made and the following instructions will be transmitted:

- Within 30 seconds of an unexpected stop a standard, automatic, calming message will be broadcasted via the train's loudspeakers;
- A second soothing message will be broadcasted not more than four minutes after the first one;
- After no more than three further minutes, a live announcement is to be delivered including an apology, information about the reason for the delay and an estimation of the extent of the delay.

Safety Partners

In the introduction, I described the empirically proven importance of having positive, reliable and competent role models in emergency situations. To obtain this goal, we will draft and train hundreds of passengers in rail safety issue. The main part of this group will consist of soldiers performing their mandatory service. The soldiers are a group we can enlist easily by cooperating with the military command. They are fit, used to high pressure situations, and dedicated to saving lives. Normal citizens can volunteer and will receive training which lasts about one day. Training for soldiers and civilians alike will be at the expense of and responsibility of the department of community connections of Israel railways. All changes will be evaluated separately and as a total programme employing quantitative and qualitative methods. Due to extensive changes in the management of Israel Railways, the timeframe has been changed. It is the intention of Israel Railways to make all changes and improvements by September 2012 and to start the empirical evaluation parallel to the changes.

References:

Darley, J.M., & Latanee B. (1970). The unresponsive bystander. Why doesn't he help? New York: Appleton Century-Crofts

Geller, E. S. (2001). *The Psychology of Safety Handbook*. Lewis Publishers, New York.

RSSB: A guide to Research in Safety Policy and Risk Management. London (2010)

RSSB: Operations. Research into Signage and Wayfinding at Stations. London (2006)

Comments

Mr. René Van Bever

Director General

Federal Public Service Mobility and Transport, Belgium

One could think this is a wrong presentation in our security Round table, because it is about a safety programme and not a security programme.

As a matter of fact when an emergency occurs, the measures to be taken and the procedures to be followed are similar, regardless of what causes the emergency: an accident, a natural or a man-made disaster. To be prepared for the consequences of an accident, helps to be prepared for a man-made disaster.

However, there are some differences.

Most terrorist attacks on public transports are bomb attacks. The wounds caused by the blast of a bomb attack are different from the wounds caused by a collision for instance. It is important for the medical teams to be informed of the nature of the emergency and to be prepared to it. But the main specificity in case of a man-made disaster is the fact to be confronted with unexpected dangers.

An example from Belgium: in 1985, Belgium was confronted with a wave of bomb attacks from an anarchist group. A series of bombs exploded at night time in isolated places close to symbolic targets, like NATO, pipelines, bank offices, and so on. One day - it was a holiday – they put a car on fire with explosives onboard in the vicinity of the leading employers' organization. They threw papers around the car warning about explosion, but the fire brigade did not pay attention to these papers. For the fire brigade, it was just a burning car. They ran to the car to do their duty and two firemen were killed in the explosion. So, let's translate this story to a larger scale and let's imagine the challenge for the emergency services at 9/11 to adapt their organization when the nature of the disaster became clear.

Everybody probably remembers the attack in the Tokyo underground by means of sarin gas. Emergency services are equipped to combat CBRN incidents and accidents. The problem in case of a CBRN attack is that the toxic product must have been detected and that the emergency services should be informed before to intervene of what kind of product they will be confronted with.

So, a programme to improve railway safety by promoting public awareness and influence public behaviour surely will improve railway security as well. But there are limits. Emergency services are trained to face unknown situations and to avoid panic. The public is not.

Less than two years ago, a collision between two trains killed 19 people in Belgium. A colleague of mine was on board of one of the trains and survived without any injury. His first impression after the disaster, – and this impression was shared by other surviving witnesses – was the feeling to be paralysed by the fact that his brain could not believe and analyse correctly what his eyes were seeing. If you add to this element that in case of a terrorist attack, the disaster would more than probably be caused by an explosion, I believe that panic, doubled by the uncertainty about possible further explosions, cannot be avoided for the passengers.

Now, the programme Mr. Cale presented will be implemented by the Israel authorities. We all know the political situation in Israel, and its repercussion on daily life. A consequence of this is that Israel is a kind of laboratory for security measures that can be copied by other countries if necessary.

In this way, I would like to make a parallel with a recent incident that occurred in Belgium. Apart from the political environment, the situation for the Israel railways and the Belgian railways are very similar: multilingual countries, short train rides and a rather negative public image. One thing however is different: the climate. Last summer, the 27 of June was a very hot day according to Belgian standards and caused traffic disruption on the railways. Catenaries broke down and several trains were stopped for hours. There were so many complaints that the Minister asked for an investigation. The main complaint from the passengers was about the lack of information. Consequently, many recommendations of the report from the investigators concern information improvements.

I do not believe that safety and security information procedures in the aviation world can be used as such for the railways. Welcome messages such as in aircraft, that are flying from point to point, can only be used in long distance trains and that is already the case today. It relaxes the passengers and this is good for safety and security. But it cannot be applied to stopping trains, calling at all stations.

Aircraft passengers are acquainted with safety and security measures in the aviation world. Safety and security messages do not affect the trust of airlines users any more in the reliability of air transport.

Railways authorities are reluctant to send safety and security messages when not absolutely necessary. These messages would be new for the public using railways and could give the impression that there is a hidden threat for railways users. So, it only could be envisaged in a situation where the message would set the passengers' mind at ease rather than worrying them.

But the part of the Israel programme about auditory information is interesting, because it could be very useful for any railway company in case of incident. A calming message for the passengers of a stranded train is of great importance. And a live announcement about the situation at short notice is of paramount importance. Uncertainty is the main reason for unrest and panic.

Surprisingly, in a world of ever growing information and communication technologies, where every citizen is overwhelmed by information, this evolution seems to be very slow in the railways world. Passengers in a stranded train are often better informed of what is happening through their personal links to the media than by the railways personnel on board. Maybe they are even better informed than the personnel onboard! But the only information they really trust and really need is the one coming from the railways authority onboard of the train.

A good communication in crisis situations or in unexpected situations is a crucial part of the crisis management. This requires an evolution of the professional skills of the staffs. I noticed in the London underground that an announcement from the driver usually immediately follows an unplanned stop between two stations. I have read that it took a long process to have this measure applied by all drivers, because some of the drivers did not feel they had the required capacities to make these announcements correctly.

To conclude: yes, the behaviour of the public is important in case of emergency. And yes, it is possible to influence this behaviour by adequate information measures. The programme for the Israeli Railways is very promising in this way and it would be very interesting to hear about the lessons learned from the programme once implemented. So, in the frame of international cooperation, it would be fine to meet back at a Round table in the next years, Mr. Cale, on this subject.

10

Panel discussion: “The Role of Governments in Enhancing Inland Transport Security”

Statements by Dr. Susanne Aigner, Professor Dimitrios A. Tsamboulas, Roeland van Bockel and Dr. Garland Chow

Introduction

Dr. Susanne Aigner
Deputy Director Compliance and Facilitation
World Customs Organization (WCO)

Inland transport (security) has many angles, and is a very complex issue; infrastructure, procurement, investment issues, but certainly also border regulatory and control issues can be evoked when talking about inland transport. From a border agency point of view (and Customs is the preeminent agency in most countries, but there are others including border guards, police, immigration and transport officials) the main areas of interest are the control and security of supply chains involving inland transport (which are in principle all supply chains, given that most consignments need to be transported by road or rail, even if they have been or will be further transported by air or sea).

Inland transport security has not received the international attention it deserves. The main focus is on maritime and now more and more on air cargo security. The security threat does however exist in relation to all modes of transport; already past terrorist attacks affected road and rail (e.g., Madrid, London, Moscow). In addition, inland transport (security) is also impacted by the increasing number of natural disasters.

Different to maritime and air cargo/aviation security, controls on road and rail transport modes are more difficult to carry out without impact on the smooth flow of goods, due to the complexity and openness of the systems. The majority of controls will be carried out at border crossings; however, unless advance cargo information requirements and rigorous transit regimes are properly implemented along with automated risk analysis to be carried out on goods before they arrive at the border, these controls will impact the clearance time and thus often not be carried out, or, if they are carried out, to the detriment of rapid release.

Role for government

The WCO has a range of relevant instruments, of which the SAFE Framework of Standards to facilitate and secure global trade (“SAFE”) is most relevant. It addresses the security and facilitation of all modes of transport, including of intermodal and inland transport. The current discussions on amendments to time limits concern all modes of transport, even if currently priority is being given to air cargo security requirements. SAFE foresees the implementation of advance cargo reporting for road and rail, with a view to allow risk analysis before export/exit from the country of origin and before the goods arrive in the country of destination. Relevant rules were implemented in some countries (EU, US, Canada). A number of countries see the necessity (also due to their geographical situation) to avoid focusing on air and maritime only; given the complexity of current trade patterns, it is necessary that security measures include also requirements for road and rail. However, due to the openness and the sheer volume of trucks and trains involved in road and rail systems, it is much more difficult to ensure that measures are implemented in a coherent and efficient way.

Technology solutions are frequently implemented at border crossings (radiation detection equipment; scanning equipment). The technology is frequently used based on a multi-layered intelligence-driven risk management approach, as promoted in the SAFE.

Surely modern customs procedures as promoted in the Revised Kyoto Convention (eg., transit; transshipment; risk management) are also important in view of securing inland transport.

Partnership approach

Adequate measures should obviously not be implemented in isolation but in partnership and close coordination with all stakeholders. Insofar, concepts like AEO are of value. It is, therefore, very positive to note that implementation of AEO programmes is increasing worldwide. Industry stakeholders should also be duly consulted before any measures that might have an impact on their procedures and processes are introduced; the Private Sector Consultative Group (PSCG) to SAFE has an important advisory role, which is replicated in many WCO Members (COAC, Trade Contact Group). The SAFE Working Group does not only involve PSCG but also many stakeholders, including IRU and, more recently, also COTIF.

Coordinated Border Management (CBM), Risk management (RM) and Globally Networked Customs (GNC)

Partnership and cooperation/coordination go further than C2B partnership but need to involve also cooperation between agencies nationally and internationally.

Coordinated Border Management certainly contributes to a more efficient management of supply chains, and does also positively impact intelligence-driven risk management through cooperation of the agencies involved. A number of projects (e.g. Greater Mekong Region) have shown that the weakest links in the various economic corridors remain the border crossings. Improved infrastructure, coupled with enhanced cross border cooperation usually leads to greater integration and economic development.

CBM, as promoted in the WCO Strategy on Customs in the 21st Century (C21) is based on the concept of virtual borders encompassing the entire transport and supply chain where goods and passengers can be assessed for admissibility and clearance in advance of arriving at the physical border.

Coupled with the availability of advance cargo information at early stages (ideally at beginning of supply chain), trusted trader like AEOs and IT-supported risk analysis (the latter two also being part of building blocks of C21), an important reduction of release times for legitimate shipments can be achieved. These measures allow customs to focus on high risk consignments and more rapidly release consignments of no or low risk. CBM considerably enhances intelligence-driven risk management as intelligence sharing and close cooperation with other agencies (even if no joint risk management/targeting is foreseen) will lead to improved risk management. CBM also promotes coordination among agencies, and thus increases efficiency and intelligent and better use of resources.

The efficiency and effectiveness of CBM depends on close cooperation/coordination and sharing of information/data among border agencies. Therefore, the concepts of Joint Customs Control and Globally Networked Customs (first building block of C21) are important enablers for CBM. The sharing of information across borders, e.g. on control or risk management results will make it possible to focus controls on high risk consignments. Examples are the EU-Switzerland and EU-Norway agreements on mutual recognition of control results. A similar agreement between EU-Andorra has applied as of 1 January 2011.

In such a system, AEOs and other reliable traders shall get benefits and should be considered of low to no risk. The objective is to move goods/means of transport that constitute no risk or limited risk across borders without unnecessary halts, thus facilitating legitimate trade while allowing border agencies sot focus on consignments/ means of transport constituting elevated risk. The holistic and collaborative end-to-end supply chains approach also leads to reduced administrative and compliance costs, as well as increased savings for trade, customers and governments.

The implementation of CBM requires efficient intergovernmental and interagency networking arrangements, which allow the agencies to cooperate effectively with a set of common and agreed standards. WCO has developed Data Model Version 3, which is Single Window compatible, and thus allows cross border exchanges in a single window environment, which is an intrinsic part of properly implemented CBM.

JCC - One stop border posts/juxtaposed offices/Coordinated Inspections

A number of countries have established one stop border posts (OSBP) to improve the cross border movement of goods; usually the setting up of such OSBPs needs to be supported by an enabling legal framework and be based on an implementation strategy that is supported by all stakeholders. The Revised Kyoto Convention (RKC) and SAFE support and promote CBM and OSBPs. Examples for OSBPs: SACU (South African Customs Union), EAC (East African Community), Mercosur; Switzerland-France, Switzerland-Italy, Switzerland-Austria, Switzerland-Germany. One stop border posts Norway/Sweden/Finland, where Customs carries out controls on behalf of another government (including Norway on behalf of EU countries); leading to savings in terms of money, resources and time.

Legal implications (extra-territorial jurisdiction) have to be taken into account; controls to be allowed on the other country's territory (in limited and designated areas); sequence of controls (first exit, than entry), powers of officers, immunities of officers, jurisdiction in case of offence.

Joint Customs-Police Cooperation Centres (CPCC)

As a consequence of Schengen and the gradual removal of border controls, it was necessary to reinforce the police and judicial cooperation among Schengen members. In a number of countries, such Customs Police Cooperation Centres were set up, based on bilateral agreements (eg Switzerland-Italy, Switzerland-France; recent flows of illegal immigrants showed importance of such measures). The CPCC usually covers 4 responsibilities: public security, fight against illicit trafficking, fight against illicit immigration and trans-border crime. The CPCC also coordinate measures for the surveillance of the border area, and contribute thus to secure end-to-end supply chains. The CPCCs have usually a double-headed structure, and decisions are taken on a consensual basis.

Trade facilitation and Security

Prof. Dimitrios A. Tsamboulas
Department of Transportation Planning and Engineering
National Technical University of Athens

Trade security has become an important component of the modern 'trade and development' thinking.

While attacks on trade ("threat to trade") can have adverse impacts on an economy, an even **greater threat** stems from the potential for **trade to be misused** as to facilitate attacks on human life and key infrastructure ("threats from trade").

The importance of trade security as a threat to trade grows as the globalization process continues and economies become increasingly interdependent and trade dependent.

At the same time, large potential gains can be made by facilitating trade procedures and thereby reducing transaction costs for international trade.

Even for the countries that comparatively have the most efficient trade procedures – such as parts of Europe, Asia and North America – there is a great potential for trade facilitation, primarily by harmonizing procedures between countries and taking advantage of IT solutions.

Question 1: One central issue when discussing the formulation of a security initiative is the way in which security measures affect trade flows. It is of interest to ascertain whether the **increase in the number of security initiatives prevents the benefits** of **trade facilitation** from being realized.

Question 2: Another question is the **extent** to which **countries** take a step backwards from trade facilitation they have implemented, by giving the **companies an increasingly complex set of regulations** to comply with and by customs authorities increasing their controls.

Trade and Transport Facilitation provides important benefits:

- Increase trade competitiveness through better logistics, border management, and availability of services for overall improved supply chain performance.
- Result is better cash flow, lower risk, just in time delivery, and more market opportunities (volume and diversification).

The four principles of trade facilitation are harmonisation, simplification, standardisation and transparency.

Making transit work through collaborative border management benefits:

- Quality and Efficiency of service providers;
- Customs brokers;
- Truckers;
- Freight forwarders.

One opinion is that **Security and Trade Facilitation reinforce each other**, since security as a global public good is also closely associated to the expansion and flow of international trade. Hence, better trade facilitation can actually enhance trade security and vice versa.

By simplifying and **facilitating Customs procedures**, chances increase that **fraud** and **criminal activities** will be **discovered**. The simpler and the more transparent the system is, the easier it gets to detect suspicious behaviour. It further counteracts potential corrupt behaviour within the Customs, a cost that governments rarely speak of, but too many companies have felt.

Many of the security initiatives state that they have elements of trade facilitation, but in a review of the security initiatives it is not always obvious that this is the case.

Also, several security initiatives have come into being with a considerable increase in the number of security controls and the certification programmes do not specifically offer a total reduction in these controls, even for those companies that reach the highest level of certification.

In addition, the **costs of transport** resulting from **intensified security** requirements can prove to be **considerable**.

Countries that are greatly dependent on trade and whose transport costs already constitute a large proportion of the value of goods are probably those that are most severely affected by extended transport times, while their access to foreign markets is jeopardised.

Concern has been expressed about the risk that **enhanced security** can **distort competition**, and change **trade patterns**, both among the producers of different goods and between different geographical regions.

The fact that international **trade** shows a **great degree of price sensitivity** with regard to transport costs is evidence of the importance of **minimising the costs of the increases in security** requirements in the supply chain.

Distribution of security-related costs is required together with identifying the parties that are most negatively affected by these costs.

On the other hand, 100 per cent inspection bears the risk that it will not be possible to realise any benefits from trade facilitation.

An economic analysis of the **maritime** and **air transport** sectors indicates that as long as there is overcapacity in these sectors, the companies will have **difficulties** in passing **on security-related costs** to the final customers.

The National Board of Trade concludes that, in order not to jeopardise the benefits of trade facilitation, **the formulation of security initiatives needs to include trade facilitation measures**.

To minimise these costs it is reasonable that the security initiatives should be based, as far as possible, on **risk analyses and risk management**, rather than on an increase in the number of inspections. Most of the security initiatives have a component which requires risk analysis.

The proposed rules for 100 per cent scanning of containers to the USA is the only initiative that completely avoids risk analysis, but, at the same time, has been the subject of criticism from both the EU and the WCO for constituting a barrier to trade.

EU White Paper on Transport for 2011 on 'end-to-end' security

While many tools for protecting cargo security exist in the European Union, there are currently **no rules in place for the European land transport supply chain** in its entirety.

The Commission proposes to build upon the experience gathered with AEOs (Authorized Economic Operator) and 'known consignors' to develop an **'end-to-end' security management system** involving a **harmonised Joint Security Risk Assessment** of operators involved in an entire transport supply chain, independently of the transport mode used.

'**End-to-end**' **security certificates** delivered to compliant operators would entitle them to benefit from security facilitations related to operations at any stage of the supply chain.

The system would be based on risk management and not on the elimination of risk. Procedures for restoring the functioning of the supply chain after a major terrorist attack or any other distortion linked to security would therefore be integrated in the design of European and national Mobility Continuity Plans.

Finally, **international cooperation** must be further **strengthened** in all the aspects of transport security, where joint efforts can bring considerable synergies (such as the exchange of intelligence information on international terrorism) and where national competences are not clearly defined (for instance navigation on international waters).

Example**:**

SERSCIS: Semantically Enhanced Resilient and Secure Critical Infrastructure Services

The aim of SERSCIS is to develop adaptive service-oriented technologies for creating, monitoring and managing secure, resilient and highly available information systems underpinning critical infrastructures.

Controlling infrastructure vulnerabilities caused by:

External events:

- a change in requirements from ICT systems;
- compromising the availability of ICT systems.

ICT system:

- faults or underperformance;
- security breaches making interconnected;
- system components untrustworthy.

Application Areas:

- AIR TRANSPORT in air traffic flow control and airport services process optimization;
- SEA TRANSPORT in intermodal port community operations.

Is there a role for government to provide and/or enhance inland transport security?

Mr. Roeland van Bockel

Convenor

CEN TC 379 supply chain security

Is there a role for government to provide and/or enhance inland transport security?

Government should act based on the answers to the following question:

What assets are you trying to protect?

What are the risks to these assets?

How well does the security solution mitigate those risks?

What other risks does the security solution cause?

What cost and trade-offs does the security solution impose?

The major risks in transport security are:

In public transport: terrorist attacks. The public authorities should assist private parties with clear guidelines on how to prevent and protect and provide sufficient police and other assistance in case of an incident;

In freight transport: crime. The public authorities should provide police assistance to prevent and capture. Companies should put sufficient measures in place.

In inland freight transport security, governments have to play a role. The major role is to secure a level playing field amongst the participants in the market, i.e.:

- preventing inequality amongst the participant in the supply chain, and
- preventing excesses, i.e. based on measures imposed.

When governments request businesses to invest in security measures, they should be allowed some benefits, i.e. trade facilitation.

What are/should be the respective roles of private and public sectors?

Public authorities have to protect their citizens from unlawful damages being done, prevent the citizens from being exposed from risks they cannot prevent themselves against individually. Above all, public authorities relate to the collective goods and allowing people freedom that does not jeopardize the freedom of others.

Private (business) parties have to stay in business, earn money in a sustainable way. Therefore, they have to take risks, to venture and manage the unexpected.

How is/should be inland transport security financed?

Financing is related to the party that is benefitting most. Security is difficult to be given a price tag. It relates to:

- Opinion of the voters (public authorities concern);
- Damages;
- Price of measures been put in place (awareness training, IT and physical measures);
- Enforcement.

Both the public and the private sector can benefit from security investments, thus have to pay for it. However, the value added of security money being spent has not been defined. That should be better reviewed before new decisions can be made on areas to invest in. Security investments do not only benefit security purposes.

Government is ultimately responsible for inland transport security

Dr. Garland Chow

Associate Professor, Sauder School of Business

Director, Bureau of Intelligent Transportation Systems & Freight Security (BITSAFS – Sauder)

Associate, Centre for Transportation Studies

University of British Columbia, Canada

Keep in mind that freight security is used here in the context of detecting and keeping out unwanted cargo, people, drugs and other additions to freight or its conveyance. Transport security, or rather the lack of security (or perhaps we can call this “insecurity”), is an externality produced by firms that impacts the general public and society. The movement of product over space creates the opportunity for a “security” incident or failure that can injure the public, destroy infrastructure, disrupt an economy and degrade the environment. A security incident can result in costs and consequences that are far beyond the bottom line of the firm, or even the supply chain that is involved.

The behaviour of most firms with respect to security is that it is a secondary corporate performance metric, and when the bottom line is impacted, the bottom line “trumps” security. It is fortunate that many freight transport stakeholders pursue business strategies and practices that result in freight security as a collateral benefit, but this is not always enough. A firm has the incentive to invest in trusted personnel, access control and surveillance to prevent goods from being stolen when the cost of product loss is high, but would they make the same investment if product loss were low? Does security investment that effectively prevents loss and pilferage also effectively prevent harmful goods from being added to the shipment? Would the same level of security exist if the firm is not earning a profit? Does the firm include in its calculus, the billions of dollars of physical, economic and unfortunately human loss that may occur if their lack of security contributes to a security incident? Can a firm even estimate that cost? Thus government must be the final arbitrator of what constitutes a reasonable level of security and implement programmes to achieve that because the firm cannot. This is essentially what has happened in the case of safety and congestion externalities traditionally produced in the transportation, and this still evolving with respect to government involvement in sustainability.

The public sector plans and controls freight security environment: the private sector implements freight security

Security management is no different from the management of any value adding process; it involves planning, implementation and control. Government should be largely responsible for planning and control of the security environment, while the private sector should be largely responsible (though not completely) for the implementation of freight security. Planning is the setting of goals and the major policies to achieve a perceived level of security. Ultimately, government has to decide on compromises between security and trade and between security and privacy, for example. Planning is deciding on major strategies and the U.S. and Canada (as discussed in my paper) have pursued a risk management strategy based on trusted partners and pre-screening at its sea and land borders. Implementation is the mobilization of resources to execute a process and is primarily in the realm of the private sector. It is the private sector that chooses to implement best practices in freight security in form of access control, surveillance, obtaining qualified and trusted personnel, choosing trusted suppliers, and the security processes enabled by these resources. The security of the supply chain is the sum total of the security practices of all of the members of the supply chain, including the government. It is at the physical perimeter or virtual border that government is uniquely positioned to both implement and control security plans, through the clearance and potential detection of unwanted cargo. It is at the border where government can determine whether freight seeking entry into a country is secure or not.

Another role of government is to provide the private sector with incentives to develop, invest and adopt best practice in security. This is done now by giving freight movement participants benefits, such as faster access to clearance and reduced clearance requirements at the border. But ideally, the internalization of security cost to the public would be superior, as it would embed the cost of security into the decision making of the freight transport participant. For example, (and the figure is purely an example) a FAST certified shipment crossing the U.S.–Canada border might be charged the minimum if any border clearance fee while a non–Fast certified shipment would be accessed a $10 fee for each vehicle load.

Government freight security implementation and control should be financed through user charges and incentives for improved security provided through rebates of these user charges

Transport security activities of the government can be classified as user specific or general. Most of the public sector’s transport security planning activity is a general cost that is not attributable to a specific carrier or importer moving freight across a border. That cost should be borne from general taxpayer funds. However, every movement across the border generates a direct clearance processing cost, and in fact in many jurisdictions, there is a security processing fee (for example, examine the details of your last airline ticket receipt). While the concept of a user fee is not innovative, the following variation is suggested, since the ultimate goal of border security policy is to reduce and prevent the entry of unwanted, unauthorized freight. It is proposed that transport providers and importers who participate in trusted partner programmes, or in pre-clearance programmes, are provided a rebate or reduced border-processing fee reflecting the reduced effort needed to clear their freight movements. This would provide an additional incentive for carriers and importers to employ and implement best practice security processes and presumably increase the level of security that they produce. Thus, this procedure is consistent with the internalization of security costs discussed earlier, though in this case, this is more properly the internalization of security benefits. We have seen this successfully applied in California where the state government levied an automatic environmental impact charge per container picked up or dropped off at the port terminals, but this charge is eliminated if this container activity is performed at night when the environmental impact is considerably less.

An unwanted, but possible scenario in the future

This discussion has focused on controlling freight security at the borders between countries. This is based on the implicit assumption that within the borders of a country (e.g. the USA) or region (e.g. the EU), the movement of inland freight is secure. We know that this assumption is not 100 per cent true, but it is reasonable to assume that it is more likely that freight movement within a political jurisdiction is more secure than freight movement across political jurisdictions.

We must be prepared to accept the possibility that a freight security incident could occur that would require greater freight security control within the boundaries of an individual country or trading bloc. The “border” may end up being redefined to checkpoints where inland freight crosses. One only has to look at Mexico to see this phenomenon. I would note that developed countries, which have advanced levels of vehicle size and weight and commercial vehicle safety enforcement, already have “inspection” facilities at key nodes in the highway transport network where security-screening functions could be performed and administration costs shared.

ANNEX 1 – Statement by Mr. René Van Bever, Director General, Federal Public Service Mobility and Transport, Belgium

Mr. René Van Bever

Director General
Federal Public Service Mobility and Transport, Belgium

Ladies and gentlemen,

Good morning. Welcome to the Inland Transport Security Discussion Forum, OSCE-UNECE Round Table. Security is a complex issue. It involves a lot of elements that can contribute to reducing the risks, by reducing the threats or reducing vulnerability; through 4 kind of actions – the so-called 4 P's – : Prevent, Pursue, Protect and Prepare. To prevent illegal acts by tackling their underlying causes; to pursue the authors of illegal acts; to protect the public and the infrastructure; and to prepare for the consequences of an illegal act and improve resilience.

This means that security is provided by the joint efforts of a lot of actors: diplomats, social workers, intelligence services, the judicial powers, the police, border control, emergency services, and so on. The transport sector has to act for its own protection, but an efficient transport security policy can only be reached by a global approach to all these security aspects.

Transport is a complex issue also, with specificities for each transport mode, and specific security aspects for each of them. This is true, of course, for the different transport modes defined as inland transport modes as well.

But one thing is definitely common: today, inland transport security is a universal problem. All over the world, freight carriers are confronted on a daily basis with cargo crime, transported dangerous goods can be transformed into lethal weapons, and the threat of bomb attacks on public transport cannot totally be excluded in any place in the world.

The International Transport Forum of the OECD dedicated a session of its annual summit this year to security in transport. A conclusion of this panel is that international cooperation is essential. And I quote one of the panellists from the private sector: "joint development of security measures must be the goal".

Ladies and gentlemen,

The present Inland Transport Security Discussion Forum organized by OSCE and UNECE as a common Round Table, is a perfect illustration of this international cooperation at intergovernmental level.

The item "transport security" has been part of the respective agendas of OSCE and UNECE for several years now, and I had the opportunity to participate in the activities organized by both organizations on this subject. Therefore, I am very pleased that the cooperation between OSCE and UNECE gives me the opportunity to chair the first day of the present Round Table. It's a real honour for me

This event could not have been organized without the support of the staff of the hosting organization – OSCE – and without sponsorship. So let me thank them all, in the name of all participants, with special thanks to the two main sponsors: the Republic of Kazakhstan and Belgium. With this support, both countries reiterate their interest in the topic of transport security, they put forward during their respective Chairmanships of the OSCE in the last few years and they confirm that they consider transport security as an important issue.

So, I warmly thank the Belgian government and the government of Kazakhstan for their financial support. Mr. Usen Suleimenov is Deputy Permanent Representative of the Republic of Kazakhstan to the OSCE and I now give him the floor for the opening session of the Round Table.

Thank you.

ANNEX 2 – Statement by Mr. Usen Suleimenov, Deputy Permanent Representative of the Republic of Kazakhstan to the International Organizations in Vienna

Mr. Usen Suleimenov

Deputy Permanent Representative of the Republic of Kazakhstan
to the International Organizations in Vienna

Mr. Chairperson,

Ladies and Gentlemen,

Distinguished Participants,

It is an honour and a great pleasure for me to take part in the Opening Session of this joint OSCE-UNECE Expert Round Table being held in the framework of the Inland Transport Security Discussion Forum. I join the Chairman in welcoming to this Round Table the representatives from national governments, international organizations, civil society, the private sector and academia. It is a pleasure also to welcome our distinguished speakers, moderators and panellists. We look very much forward to your thoughts and ideas on and your guidance for our discussions.

I congratulate the organizers for having prepared such an interesting agenda, for bringing together such an impressive list of inland transport security experts and national participants, and for all their efforts for a smooth set up of this meeting. A sincere "thank you" goes to Mr. Goran Svilanovic, Co-ordinator of the Economic and Environmental Activities, and his able staff, as well as to Ms. Eva Molnar, Director of the UNECE Transport Division and her team.

This Expert Round Table is a direct follow-up to last year's Economic and Environmental Forum process under the Kazakh OSCE Chairmanship and in my view it clearly meets the current requirements and needs of our region. Particularly at a time in which many countries continue to face economic challenges safeguarding the security of the international transport circuit remains a key issue. **How else can we make sure that our goods and cargo find their way from the producers to the consumers in a safe, timely and predictable manner?** The issue of predictability is a necessary pre-condition for international trade and transport and it can only be guaranteed when transport policies (including those pertaining to security) are co-ordinated and agreed upon among countries and to the extent possible harmonized and streamlined.

Transport development and security remain a high priority for my country which, as most of you are aware, is centrally located offering a land bridge between Asia (where China is the world's largest producer of consumer goods) and Europe (among the largest consuming regions). By means of our geographical location, we play a tangible role in linking the markets in the Far East with those in the West.

Having a strong interest in this topic and having gained experience in this field, we stand ready to share our knowledge with all participating States as well as we are eager to learn from other countries. It is therefore with great pleasure that I can announce that in the course of tomorrow's afternoon session a senior representative of the Kazakh Ministry of Transport and Communications will share with you information on my Government's efforts and policies in creating a more secure transport environment. It is also based on the same rationale that my Government (together with the Belgian Government – as Mr. Rene Van Bever just mentioned) decided to co-fund this Round Table and the subsequent publication of the expert papers and reviews.

In conclusion, in my Delegation's view we would be glad if this two-day Round Table will result in the adoption of a more 'systematic approach' towards inland transport security. We would welcome proposals for initiatives of bringing existing approaches and policies closer to each other. This meeting should enable us also to better define the current strong points but also the deficiencies, if any, and it should offer a fertile ground on the basis of which new more comprehensive inland transport security policies can be developed. Kazakhstan is more than willing to continue contributing to the efforts of the international community in this regard.

Thank you for your attention!

Organization for Security and
Co-operation in Europe (OSCE)

Wallnerstrasse 6
A-1010 Vienna, Austria
Tel.: +43 1 514 360

info@osce.org
www.osce.org

facebook.com/osce.org

@osce

youtube.com/osce

United Nations Economic
Commission for Europe (UNECE)

Palais des Nations
CH-1211 Geneva 10, Switzerland
Tel.:+ 41 22 917 44 44

info.ece@unece.org
www.unece.org

facebook.com/unece.org

@un_ece

youtube.com/unece

2012 Inland Transport Security Discussion Forum **Proceedings**

Organization for Security and
Co-operation in Europe

UNITED NATIONS
ECONOMIC COMMISSION FOR EUROPE