RAND

"Seacurity"

Improving the Security of the Global Sea-Container Shipping System

Maarten van de Voort, Kevin A. O'Brien
with Adnan Rahman and Lorenzo Valeri

RAND Europe

ISBN: 0-8330-3440-5

Published 2003 by RAND
1700 Main Street, P.O. Box 2138, Santa Monica, CA 90407-2138
1200 South Hayes Street, Arlington, VA 22202-5050
201 North Craig Street, Suite 202, Pittsburgh, PA 15213-1516
RAND URL: http://www.rand.org/
To order RAND documents or to obtain additional information, contact
Distribution Services: Telephone: (310) 451-7002; Fax: (310) 451-6915;
Email: order@rand.org

RAND *Europe*

Seacurity

Improving The Security Of The Global Sea-Container Shipping System

Maarten van de Voort and Kevin A. O'Brien

with

Adnan Rahman and Lorenzo Valeri

MR-1695-JRC

Contents

Preface

In May 2002, at a workshop organised by the Swedish Minister of Foreign Affairs, with the support of the Joint Research Centre (JRC) of the European Commission, RAND *Europe* gave a presentation on the reliability of technical systems. The safety and security of the maritime system, with a focus on container security, was touched upon in this presentation. It triggered awareness with respect to the vulnerability of the global container shipping system. Based on this awareness, RAND *Europe* has co-operated with the JRC to take the matter to the next level and increase awareness throughout the container supply chain, as well as within the European legislative bodies. This effort resulted in organising *SeaCurity*, a stakeholder consultation – held 28-30 October 2002 – regarding the security of container commerce.

During this three-day event in Ispra (It), presentations were given in two categories: threats and solutions. In the first category – Threats – Jack Riley and Peter Chalk (RAND) presented papers respectively on *"Securing Ocean Commerce: A US Perspective"* and *"Threats to the Maritime Environment: Piracy and Terrorism"*. In the second category – Solutions – Jose Perdigao (EU-JRC) presented a paper on the *Contraffic* system, while Adnan Rahman (RAND Europe) gave the *TRI MEX* presentation. The remainder of the consultation consisted of group discussions fed by the presentations.

The presentations from the workshop can be found on the RAND *Europe* website at www.rand.org/randeurope/fields/transportproj.html.

This report follows the broad outline of the consultation. Beginning with issues that were raised regarding threats to maritime and – more specifically – to container commerce, the workshop then discussed the issues and possible solutions that these raised. The report concludes with a number of recommendations and references.

The purpose of the workshop and this document is to raise awareness concerning the current status of maritime security and its vulnerability to terrorism. The main obstacles in achieving a less vulnerable maritime system are identified mainly through the interaction of the workshop's participants.

The report should be of interest to government officials and policy-makers dealing with the maritime system, international trade or anti-terrorism issues, as well as private companies that have an interest in the (international) maritime system.

RAND Europe is an independent not-for-profit policy research organisation that serves the public interest by improving policy-making and informing the public debate. RAND Europe's work is for European governments, institutions, and private sector entities with a need for rigorous, impartial and multidisciplinary analysis of the hardest problems they face. This report has been peer-reviewed in accordance with RAND's quality assurance standards (see www.rand.org/about/standards/) and therefore may be represented as a RAND Europe product.

On behalf of RAND Europe, we would like to thank the consultation's attendees for their participation and ideas, and hope that the material that was brought up through this initiative will result in a strong take-up from all stakeholders.

For more information about RAND Europe or this document, please contact:

General
RAND Europe
Newtonweg 1
2333 CP Leiden
Phone: +31 71 524 5151
fax: +31 71 524 5192
reinfo@rand.org
www.randeurope.org

SeaCurity
Maarten van de Voort
voort@rand.org

The Problem

Summary

In light of the new terrorism, the security of the global sea-container shipping system needs to be reviewed and systematically analysed. A systematic review of global container commerce with an eye to improving system wide security is required. As part of this larger effort, a first step should be a consultation involving relevant stakeholders to identify the major issues and perspectives, the results of which will be used to increase awareness about security issues among the stakeholders, as well as to formulate a research agenda and a research effort to improve the security of global container commerce.

Background And Problem Definition

Approximately 90% of all cargo moves in containers. Approximately 250 million containers are shipped annually. This massive flow of containers around the world is, in some sense, the lubricant for the world's economy. Thus, the global shipping system is a critical infrastructure for the global economy; it is, however, also very vulnerable. Estimates are that the contents of less than 2% of all containers are checked to verify that what is inside these containers is actually what is said to be inside the containers. In fact, containers are used by criminals to transport all sorts of banned goods, and even people. The problem of the illegal transport of goods and people takes on particularly worrying proportions in light of recent terrorist activities. Terrorists could, for example, use containers to transport dangerous materials, weapons, or use the containers themselves as weapons of mass destruction. The potential threat of terrorists using containers poses a large risk to our economies and to our societies. How large is this risk, and what is the most effective way to reduce these risks to acceptable levels?

Answering these questions requires a system analysis for several reasons. First, there is a clear need for an integrated assessment of global threats, risks, and existing and potential security measures with regard to costs and benefits of such measures. Second, all technical and non-technical factors and their interdependencies may potentially act as weak spots in the entire complex system. Third, implementation strategies should be tested for feasibility with regard to political, legal, economical, cultural and other contextual aspects. Fourth, the development and implementation of additional security measures – if any – that stood the test of the analysis, would still require a major investment of stakeholders -- that have yet to be identified.

Securing the global sea-container shipping system is clearly a major undertaking requiring a system approach. Such a major undertaking has been suggested to the European Commission as an Expression Of Interest[1] to conduct an integrated project in the EU's Sixth Framework Programme,[2] among other initiatives. But the approach should also be careful, with small initial steps to gain support among the various stakeholders in the international community. Also, the current security situation and the threat of terrorism require swift action. Under such circumstances, it is wise to take the initiative to gather a group of experts and think the problem through in a logical and systematic way, identifying the major issues in preparation and anticipation of next steps.

This stakeholder consultation will identify the major issues in securing the global sea-container shipping system, as well as help in building support for addressing the issue of security through suggested strategies for doing so.

---

[1] This Expression of Interest is entitled "Securing the sea-container shipping system" and can be found at http://eoi.cordis.lu/dsp_details.cfm?ID=26447.

[2] For more information on the Framework VI Programme, see www.cordis.lu/fp6/whatisfp6.htm. FP6 is the result of the call by EU governments at the March 2000 EU Summit in Lisbon for a better use of European research efforts through the creation of an internal market for science and technology – a 'European Research Area' (ERA). FP6 is the financial instrument to help make the ERA a reality, through funding research across Europe in a broad range of subjects and disciplines.

The Threat

Terrorists' Actions

Certain patterns can be distinguished in the ways terrorists choose concepts and targets for their attacks. It is generally acknowledged that terrorists will choose the way of least resistance; this is, however, a theoretical situation as it implies that terrorists would need perfect information on all possible targets to be able to select the weakest link, which – of course – is not the case. This is one of the reasons the maritime system and container transport so far have not been targeted by terrorists' actions. Besides perfect or sufficient information, knowledge and experience in and with possible targets also seems to be a driver for terrorists with regard to target selection. Once a target has been identified as a weak spot, it will pose a more likely target for future attacks. This can be illustrated through the air travel sector, which frequently remains a terrorists' target even though security measures have been taken after earlier attacks. A most likely reason for terrorists to keep falling back in their usual patterns is that the results and consequences of these kinds of attacks are known to both the terrorists as well as to the general public. Another specific driver that can be identified for terrorists to choose their targets is media coverage. This coverage is most likely to be provided through attacks resulting in many casualties.

Attacks aimed at disturbing the container supply chain have the potential of creating worldwide chaos in that supply chain, but are less likely to inflict a high number of casualties. This is where a clear distinction can be made in threat analysis. Terrorists can both target the maritime sector itself or (mis)use its open character and effectiveness to import / export terrorism. Both threats are fundamentally different and therefore require fundamentally different solutions. For instance, if the maritime system was not considered as a target itself but only as a means, containers inspection at the port of destination would be possible. If, however, port infrastructures are considered possible terrorist targets, securing these by having containers checked at the port of origin results in a more complex and far more costly system. If a terrorist was to blow up a container at a certain time or at a certain location, he would most probably rely on remote control instead of on a timer or e-tracking since these ways would be far less precise.

Based on these drivers, the September 11 attacks do not diverge from previous patterns. It can, therefore, be argued that the container supply chain does not pose a likely target, since it has not been one in the past. However, some terrorist groups like the LTTE (The Liberation Tigers of Tamil Eelam) have been known to attack maritime targets and make use of

waterborne mines. From their past actions, it would not be a drastic turn to using container transport as a means of distributing terror.

Public Ownership

Since 11 September 2001, the awareness of terrorists' actions has clearly risen. This increase, however, has not been as substantial in all fields as it has been in the air transport sector. As far as the maritime sector is concerned, initiatives have been started, budgets have been raised and a few co-ordinated counter-measures have been put into place. Ultimately, this means that the maritime sector and specifically the container transport sector remain wide-open to the terrorist threat, with the key issue in this being responsibility and ownership of the problem. So far, there has not been one single stakeholder who can clearly be identified as being responsible for implementing counter-measures. For instance, in the United States, approximately nine governmental agencies have some role in national security regarding the maritime sector, but so far none has taken control over the problem. Ever since the creation of the Department of Homeland Security was announced, all initiatives from current security-related agencies have been delayed until the make-up and stance of the new department has been determined. This does, however, mean that maritime security will be far from perfect at least until this department becomes operational.

In Europe, there currently are no plans of setting up a similar co-ordinating body; similarly, no clear ownership of the problem can be identified in Europe. The structure of current European co-operation is such that security remains a national issue. These national interests are therefore protected through bilateral agreements with the United States in the Container Security Initiative (CSI) agreement. Another US initiative which is implemented on a bilateral basis is the new Customs-Trade Partnership Against Terrorism (CTPAT), an initiative in which ports within a complying country obligate themselves to have containers sealed before they arrive in the United States. This, however, does not provide actual security as the container can now be sealed at the port of departure, leaving it unsealed during transport to the port of origin – this while land-based transport is considered to be the most vulnerable phase in the container's transport as containers are known to be left unguarded at parking lots and at shunting yards. Once arrived at a port, a container is usually relatively well protected due to terminal fences, guarded gates and (camera) surveillance. In addition, another weakness in the CTPAT initiative is that there is no standard for applying seals nor for the type of seals. It can, therefore, generally be concluded that the existing US programmes are poorly integrated with European ones.

The European Commission strongly opposes these bilateral agreements since they will scatter European interests creating dissension, increase

competitiveness amongst ports and countries, and thus reduce European co-operation and the European Commission's authority. Thus far, the European Commission has not outlined concrete proposals to oppose the terrorist threat and, therefore, gathering support from its member-states. Since the Commission's initiative in this field is lacking, member-states are now launching their own individual (occasionally collective on a bilateral basis) initiatives and solutions. Besides security there is also the countries' ports' competitive positions at stake here. If the United States is planning on expanding CTPAT into their 'safe ports' initiative, it is likely that complying European ports could greatly benefit from this. Individual countries might be able to adapt a system of checks at their ports which would be – for the time being – satisfactory to the United States without providing a supply-chain-wide security coverage system. US-authorised countries and ports will, however, gain an pseudo-oligarchic position, rendering them with considerable competitive advantages.

The resulting lack of ownership, awareness and co-operation between the United States and Europe, as well as within Europe itself, leaves such initiatives scattered, the research budget marginal and the maritime system wide open to the terrorist threat.

Private Ownership

One of the key challenges presented by the overwhelming private ownership of the majority of the container supply chain is that a container changes hands several times on its way from its origin to its destination, causing multiple parties to be responsible and liable for the container's contents. A way around this, in order to achieve involvement by less parties in the transport of a container, would be logistics-chain integration. By reducing the number of supply-chain participants, the number of handovers and - therefore – seal inspections can similarly be reduced.

The current system is, in fact, problematic from the start: although forwarders, transporters and carriers do accept responsibility and liability for a container, they are dependant on information provided by the shipper while not being allowed to open the container. In some cases, the shipper also demands to facilitate the transport from the container's origin to the terminal, leaving the forwarder or carrier in the dark even on the (actual) origin of the container. They now are fully dependant on the data provided in the Bill of Lading. It therefore does not make sense to place responsibility in the hands of a carrier.

A solution for this problem could be found by making one body responsible for the container's transport. It would be logical that, since this party has to be present at both the point of origin where the container is sealed and the point of destination where the cargo is received, this party is either the shipper or the receiver. If the seal is compromised during transport, the

transporting party at that moment should reseal the container, thus taking responsibility for its load. In the current system, liability is only considered applicable to determine which party should approach its insurance company in order to get stolen property refunded. The party that is liable is the party that is shipping or storing the container at the moment of theft.

To verify whether a seal has been tampered with, its number should be compared (or read) with the number on the Bill of Lading. A problem with seals under the current regime is that they are only 'read' occasionally, since reading them costs money. For example, the seals of containers arriving at the Port of Rotterdam by rail, truck or barge are not checked / read. This means the port takes responsibility for these containers without verifying their status. In most cases where seals are read and do not match the numbers on the documents, the mismatch is caused simply by a lack of enforced discipline in the chain, instead of by illicit activities. If Customs, for example, open a container to inspect its content, they afterwards reseal the container with a different seal and therefore different seal number. If this is not properly documented, mismatches will occur.

The majority of containers are currently sealed through a passive, indicative seal. This is a seal that does not physically prevent entry into a container as a lock would, but merely indicates that the container door at one point has been opened. Active seals can incorporate several options from communicating with close proximity readers on the container's status, to signalling a control centre on the container's status and whereabouts. The active, close proximity seals costs approximately $3 - $5, which is significantly more than the passive seals at $0,50. Besides this, the cost of development of the active seals is also high.

Summarising Threats

The system is perceived to be poorly defended against misuse and terrorism due to its global and open nature. There is no clear set of safety and security criteria from both the United States as well as from the European Commission, leading to individual EU member-states taking their own unco-ordinated initiatives. A way of dealing with this in Europe could be the establishment of a European co-ordinating body. If such a body is not founded, Europe risks an additional delay and continued problematic approaches to this challenge, comparable with ones the United States are now experiencing due to fragmented responsibilities of agencies.

The International Maritime Organisation (IMO)[3] has so far served as a market place for ideas and should continue to do so in the future. At its

[3] www.imo.org

December 2003 Diplomatic Conference on Maritime Security held in London, the IMO adopted a number of amendments to the 1974 Safety of Life at Sea Convention (SOLAS), the most far-reaching of which enshrines the new International Ship and Port Facility Security Code (ISPS Code). The Code contains detailed security-related requirements for Governments, port authorities and shipping companies in a mandatory section (Part A), together with a series of guidelines about how to meet these requirements in a second, non-mandatory section (Part B). The Conference also adopted a series of resolutions designed to add weight to the amendments, encourage the application of the measures to ships and port facilities not covered by the Code and pave the way for future work on the subject. These new measures will enter into force in July 2004 as part of a series of measures to strengthen maritime security and prevent and suppress acts of terrorism against shipping, which will be of crucial significance not only to the international maritime community but the world community as a whole, given the pivotal role shipping plays in the conduct of world trade. The measures represent the culmination of just over a year's intense work by IMO's Maritime Safety Committee and its Intersessional Working Group since the terrorist atrocities in the United States in September 2001.

Both in the United States as well as in Europe there is a distinct lack of awareness of the threat, especially in the private sector; if there is any concern within the private sector, it is for counter-measures taken by governments that will adversely affect container throughput – affecting the commercial imperative. Ultimately, greater enforced discipline of uniform application to container security throughout the supply and transport chain would go a long way to obviating much of the non-malicious threat.

Solutions

Building Blocks

For reducing (not eliminating) the terrorist threat, several methods were identified.

1. Risk analysis
2. Container integrity
3. Container tracking and tracing
4. Container load verification

Risk Analysis

Risk analysis forms a strong tool to detect suspicious cargo in order to be able to intercept it. It is, however, only as strong as the algorithms and information behind it. Risk analysis as is currently performed in many ports frequently does not incorporate sufficient data to be able to detect the bulk of illicit trade. An expansion of criteria, enhancement of algorithms, more information exchange within the logistics chain as well as between ports, and more extensive use of computerised search tools would increase the effectiveness of risk analysis.

The European Commission's Joint Research Centre has, in co-operation with the European Anti-fraud Office OLAF, developed a software tool named Contraffic, which is able to perform a risk analysis on the likeliness that a container is transporting illicit material. In the Contraffic system, this is done by keeping track of the ports-of-call of both the container *and* the ship used in the container's transport. In most of the current risk analyses, only the last port-of-call is registered whereas Contraffic registers the actual origin of the container and all ports-of-call on its way to its final destination. Based on the results of a pilot that was performed with Contraffic, it can be concluded that this way of conducting risk analysis forms a valuable extension to the current aspects. The algorithms incorporated in Contraffic focus on the detection of the evasion of anti-dumping taxes; other algorithms focussing on other aspects can be developed using the same principle of origin – destination analyses.

Currently, a large portion (approximately 50%-70%) of the containers that are inspected in both the United States as well as in Europe are inspected randomly, thus without any risk profiling. Random checks severely disturb the logistics chain at the ports and, therefore, need to be minimised. These

kinds of random checks are, however, necessary as they provide a benchmark to assess the effectiveness of risk profiling. Furthermore, they are able to point out weak points in the risk analyses and new or other types of contraband trafficking. For these purposes, a 10% part of total checks should be sufficient.

Risk analysis is a relatively cost-effective way to retrieve illegal cargo, especially financially-motivated contraband trafficking. Unfortunately, it is by no means full proof and is by definition vulnerable to terrorists' contraband, as it relies on patterns which can be assessed by terrorists in order to ensure that their shipments to not match these patterns. It can even be argued that, if risk analysis algorithms are not complicated enough to avoid pattern-recognition based on the analysis' outcome, they pose a threat instead of a cure regarding terrorists' contraband.

Container Integrity

The integrity of a container during its transport from A to B in the logistics chain cannot be assured. Given sufficient time, opportunity and a remote location, people will be able to open a container and tamper with its contents. The easiest way of gaining access to a container is to break the container's seal and open the doors; however, this can easily be identified after which the container's contents can be examined before it is allowed to be shipped again. To avoid attracting attention to the container, criminals will try to leave the seal intact when opening the container. There are several ways to do this, many of which are even illustrated on the Internet.[4] A problem in sealing containers is posed by the fact that a container is not as standardised as it may seem. This lack of standardisation contributes to the lack in sealing standards. Furthermore, the way many seals are attached is susceptible to unnoticed container tampering; for example, it is believed that an experienced thief is able to take cargo from a sealed container without noticeably tampering with it within 20 minutes. A more effective way of sealing a container would be to attach a string / seal around both locking bars or to apply a seal on the inside of a container. The quality of the seal does not have anything to do with the possibilities of working around it; the bottom line of sealing a container is maximising the time that is needed to circumvent it. Indeed, if criminals are given sufficient time and opportunity they can also cut through the side or the hinges of the container giving them access. In order not to attract suspicion, these parts would afterwards have to be repainted, which can result in differences in colour that stand out.

[4] See, for example, "Break Into A Container In Under 2 Minutes!" and "Hide The Evidence Of A Break-In In Under 1 Minute!" at www.sealock.com/problem/problem.htm and www.sealock.com/problem/problem2.htm; see also "09/06/1997 Reference Number: 1997-77" under www.maritimesecurity.org/asa1997.htm and "02/03/2001 Reference Number: 2001-75" at www.maritimesecurity.org/asa2001.htm.

The container's integrity can also be assessed through electronic systems that are installed inside the container. Since these systems are in general quite costly, only containers carrying high value loads are equipped and protected this way currently. These systems are able to detect movement within the container, including the opening of the door. They can be set in such a way that they will send out a signal to a control centre on opening or send out this signal if opened at another position than its predetermined destination. These options incorporate GPS (Global Positioning System) and GSM (Global System for Mobiles) technologies, and are ascending the container integrity function towards container tracking. Many of these systems dispose of integrity assurance as well as tracking and tracing abilities.

Clearly not all possibilities for sealing containers have been carefully studied since it has not received top priority due to the costs this would introduce to the chain.

Container Tracking And Tracing

As mentioned before, there are systems which (although quite costly) are able to give the position of a container. A distinction can be made between systems giving a time-to-time or a continuous update on the container's position, and systems that signal status-changes, like the opening of the door or movement within the container. Currently, these systems do not yet provide global coverage. This is not, however, because of technical feasibility but a result of the moderate number of current system's users.

If the control centre is notified of a non-planned incident, such as deviation from the planned route or opening of the container's door prior to reaching its destination, it will in turn notify local authorities. Experiences with these systems so far indicate that theft is practically non-existent after the system's application and local authorities quickly respond to a control-centre's notification. If these systems would be less costly, for instance because of advantages of scale in producing them in larger numbers, they would definitely improve the security of the container supply chain.

Container Load Verification

There currently are two ways of physical verification of a container's load. The term 'physical verification' used to apply on the actual opening of a container and manually verifying its content with the Bill of Lading. This process of unpacking takes, depending on the number of (Customs) officials who are performing this task, approximately 8 hours. This, of course, results in significant delays for containers and introduces uncertainties in the logistics chain. It also does not offer a structural solution to the problem, as it is due to manpower, container terminal space and the

resulting container handling backlog – therefore, it is impossible to open every container for load verification.

A form of container load verification that has come into use in recent years is by means of an X-ray scanner. These scanners are capable of giving a fairly accurate image of the container's content. Scanners have been known to generate such an amount of taxes in contraband that they can be regarded as a profitable investment instead of a costly expenditure. For X-ray scanners to work properly within a terminal's handling process and to reach a high utilisation, terminal space needs to be reserved for their placement. This is one of the reasons why a number of European terminals do not yet dispose of an X-ray scanner.

Although organic substances are fairly easy to identify in a container scan, there are ways to keep these substances from showing out. Scanners are, for instance, unable to penetrate cans and lead within a container, causing materials inside boxes or tins to remain unverified. In addition, Customs officials interpreting the X-ray image have to be trained in what they should look for; it is suggested, for example, that if a weapon of mass destruction (WMD) would be taken apart and transported in parts in a container, Customs officials would probably not be able to identify these parts as parts of a WMD or to distinguish them form auto-parts. Research is being done to improve scanning abilities and to scan for different types of cargo, such as nuclear, biological and radioactive cargo. In the United States, the container scanning process is focussing on radioactive material. This again illustrates that there will always be a focus on some type of illicit good since a radiation scanner will not be able to detect drugs: one machine cannot scan for everything and it is not feasible to put a container through ten different kinds of scanners.

In the UK, 4-7 percent of imported containers are checked based on a risk analysis, which is well above the European and US average of 2 percent. If a scan does not result in a clear and satisfactory image as 1 in every 150 does, the container is unpacked.

For contraband, it is virtually impossible to forecast which percentage of contraband remains undetected. If such a forecast could be made, it should be made per illicit good, since there are large differences in the ways goods are smuggled in and the degree of success this smuggling has. It is anticipated, for example, that for drugs approximately 10% is intercepted.

Integration

Since all of the measures mentioned above form parts of solutions, clearly an integration of measures is required. An integrated solution that is often referred to is the 'intelligent container'. As such, a container should be perceived to have the ability to scan its own contents and detect certain

illicit and dangerous cargo. The container should then be able to contact and warn authorities. Although there already is sufficient technology available to oppose numerous threats, and technical implementation of such these measures in a container is feasible, financially we still have a long way to go.

Ownership

Although most of the solutions that were thought up so far serve more than one security / legal aspect, they usually do focus on either theft prevention, smuggling prevention or on security enhancement. It is clear that if the problem's ownership is to be shifted to the private sector and a private company such as a forwarder is to invest in one of these fields, theft prevention will be his most likely choice since there is at least some form of benefit to be gained. If theft is not a major problem to the company, there will be little financial incentive for further research.

The initiative to take container security to the next level is currently with companies manufacturing security related products such as seals. Since there are globally thought to be over 15 million containers in circulation which provide for approximately 250 million moves per year, the container securing business has the potential of being a very high value and therefore lucrative one. If these manufacturers would come up with a system that would have a positive return on investments within a reasonable period of time, there would be a potential market of 15 million containers to apply this solution to. A possible outcome to the security and its solution funding problem, could be the introduction of a security tax, as is already in place at airports. Here an amount of $20 is charged per passenger to finance security measures.

Although the public and some governmental bodies are willing to pay (a certain amount) for security improvements, the majority of security measures places costs with the shippers and carriers. Of course this is not insurmountable, but does again raise a new barrier for improvements.

Conclusions From The Consultation

1. There was a wide range of views on the magnitude of the threat posed by terrorists to container shipping. Despite this, however, there was agreement that the magnitude and nature of this threat are not well understood. The participants also agreed on the need to study and understand the nature and magnitude of the threats posed by terrorists, and the potential consequences of terrorist actions.

2. There was a consensus that the flow of containers is vulnerable to terrorist action. The transport chain for containers is quite fragmented and involves many different organisations. This makes the chain quite "leaky" and easy to penetrate. Conversely, it makes it difficult to secure the transport chain.

3. The transport of containers is not sufficiently transparent, i.e., the information about what is being transported, by whom, and from where is not easy to check. The flow of information accompanying the flow of containers is not good. Even when the information is available, there is little customs can do, short of physically opening and inspecting the container, to check its validity. Only 1-2% of all containers are physically opened and inspected.

4. Physically opening and inspecting containers, while possible, is considered to be too expensive to do on a routine basis. Most inspections are based on intelligence gained about the contents of containers.

5. An alternative to physically opening and inspecting containers is to X-ray the container. However, the available X-ray devices are not fool-proof by a long shot. Assuming that X-ray machines are able to detect suspicious loads, the issue of what to do next remains.

6. Ports are reluctant to unilaterally undertake security measures that slow down the processing of arriving containers. In part this reluctance is fostered by the low margins with which the industry operates. This makes ports very reluctant to unilaterally do anything that would raise their costs and hence prices as they see this as hurting their competitive position vis-à-vis other ports.

7. It is difficult to track the journey of a container. There are several ways in which, if one wants, the real origin of a container can be hidden from officials at the destination. This is usually made possible with the help of corrupt officials at intermediate ports who are willing to change or falsify the necessary documents.

8. The issue of who is liable for the contents of a container is potentially a very important issue. As of now, the person (organisation) whose cargo is being shipped is (are) liable. However, it is quite easy for someone to falsify the information needed for transporting a shipment in a container. Given that all the liability rests with shippers, ports and ship owners, there is little incentive for ports, shipping companies, and ship owners to verify the information they are provided with. The risks of damage caused to the assets of port operators, or ship owners are covered by insurance.

9. There seems to be some issue about who controls the ports: most ports are not owned and operated by national governments. This makes it difficult for the national governments to force the ports to do something that the national governments want, but the port itself does not want to do. The lack of policy instruments for exerting any leverage in the area of port security was also noted as hindering efforts to improve port security.

10. Ports are extremely worried about the competitive position vis-à-vis other ports. In short, they are extremely price sensitive and are willing to gloss over security concerns when these are in conflict with their commercial interests. This observation seems to hold for the entire freight transportation sector.

11. National governments of EU member-states are concerned about potential actions being taken by the US government, actions which would adversely affect the position of ports in their countries. The EU is concerned that member-states may negotiate bi-lateral agreements with individual member-states. These concerns are a potential cause of friction between the European Commission and the governments of member-states.

12. Solutions should cover the complete logistics chain, should incorporate some form of risk analysis and should make use of the latest available technology (such as electronic seals, positioning technology, sensors, etc…).

13. Awareness – in both governmental offices and private companies – about the need to improve security against potential threats was perceived as low; it was suggested that actions should be undertaken to raise the level of awareness about these issues

14. The importance of having timely and reliable information was mentioned many times. The available information about containers and their contents needs to be addressed. Several reasons cause the lack of timely and reliable information. Steps to standardise and

digitise information provision would go a long way in remedying this state of affairs.

15. A clear definition of the possible threats and the likeliness of their occurrence should be defined. Many threats and their solutions are in some way interrelated, causing solutions to emerge that are not tackling the threats that they are supposed to.

16. There should be a single European body that deals with port and maritime security. This body should:

    - Co-ordinate European efforts to improve maritime security

    - Ensure post-attack measures are thoughtfully applied; just like halfway measures can bring about more attacks; the 9/11 attacks teach that drastic counter-measures can easily be just as harmful as the attacks themselves.

    - Set security criteria for all European ports to comply with; these criteria should include risk boundaries assessing which containers to scan – in all likelihood, this will cause the number of checks to increase.

    - Check the degree to which the security criteria are complied with.

17. An effort should be made to further standardise containers. Container seals should be applied in a standard way, which should ensure the container's doors cannot be opened without damaging the seal. Efforts should also be made to incorporate advanced electronic container integrity systems in the container transport business.

18. Risk analysis

    - The criteria used in risk analysis should be expanded to be able to target more types of contraband.

    - Container manifests should be pre-announced digitally so risk profiling can also be done digitally.

    - Random checks should be limited to approximately 10%

Appendix 1: List of Attendees

Thomas BARBAS
European Commission-JRC
Via E.Fermi 1
I - 21020 ISPRA
tel. :+390332789512 - fax: +390332789098
e mail: thomas.barbas@jrc.it

Heather CAMERON
OLAF
Rue Joseph II, 30
B - 1000 BRUSSELS
tel. :+32 2 2995936 - fax: +32 2 2998107
e mail: heather.cameron@cec.eu.int

Peter CHALK
RAND
1200 South Hayes St
USA - VA 22202 ARLINGTON
tel. :+70 3 4131100 - fax: +70 3 4138111
e mail: chalk@rand.org

Ola DAHLMAN
OD Science Application AB
Fredrikshovsgatan 8
S - 11523 STOCKHOLM
tel. :+46-8-6628575 - fax: +46-8-6675617
e mail: ola.dahlman@scienceapplication.com

Neil FISHER
QINETIQ
DX 102, Malvern Technology Centre, QinetiQ Ltd, St Andrews Road
UK - WR14 3PS U MALVERN
tel. :+44 77 66134550 - fax: +44 16 84895603
e mail: nfisher@mostyn.globalnet.co.uk

Elisabeth HAMILTON
HM Customs & Excise
Custom House Annexe, Lower Thames Street
UK - EC3R 6EE LONDON
tel. :+44 08707852930 - fax:
e mail: elisabeth.hamilton@hmce.gsi.gov.uk

Naouma KOURTI
European Commission, JRC Ispra
IPSC, TP 750
I - 21020 ISPRA
tel. :+39-0332-786045 - fax: +39-0332-789658
e mail: naouma.kourti@jrc.it

Malcolm MACARTHUR
P&O NedLloyd
Beagle House, Braham Street
UK - E18EP LONDON
tel. :+44 2087002140 - fax: +44 2087002135
e mail: m.j.macarthur@ponl.com

Jenifer MACKBY
Center for Strategic & International Studies
126 rue des Gelinottes
F - 01710 THAIRY
tel. :+33 450 412837 - fax: +33 450 412891
e mail: jmackby@csis.org

Mika MAKELA
EC
200, rue de la Loi
B - 1049 BRUSSELS
tel. :+32 2 2958785 - fax: +32 2 2966996
e mail: mika.makela@cec.eu.int

Andrew MCCARTHY
QinetiQ
DX 103 Malvern Technology Park
St Andrews Rd
UK - WR 14 3PS MALVERN, WORCS
tel. :+44 1684896114 - fax: +44 1684895306
e mail: asmccarthy@QinetiQ.com

Kevin O'BRIEN
RAND Europe
64 Maids Causeway
UK - CB5 8DD CAMBRIDGE
tel. :+44 1223 353329 - fax: +44 1223 358845
e mail: obrien@rand.org

Vibeke Hein OLSEN
Danish Research Agency
Randersgade 60
DK - 2100 KOBENHAVN
tel. :+45 35446361 - fax: +45 35446203
e mail: vho@forsk.dk

Jose PERDIGAO
European Commission-OLAF
Beaulieu 9, 6/196
B - 1049 BRUSSELS
tel. :+32-2-2961237 - fax: +32-2-2960853
e mail: jose.perdigao@jrc.it

Harilaos PSARAFTIS
National Technical University of Athens
Iroon Polytechneiou 9
GR - 15773 ZOGRAFOU
tel. :+30 10 7721403 - fax: +30 10 7721408
e mail: hnpsar@deslab.ntua.gr

Adnan RAHMAN
RAND Europe
Newtonweg 1
NL - 2333 LEIDEN
tel. :+31 71 5245151 - fax: +31 71 5245191
e mail: rahman@rand.org

K. Jack RILEY
RAND
1700 Main Street, PO Box 2138
USA - CA 90407-2 SANTA MONICA
tel. :+31 0 3930411 - fax: +31 0 4516983
e mail: eagle@rand.org

Alois J. SIEBER
European Commission-JRC-IPSC
Via E. Fermi 1
I - 21020 ISPRA
tel. :+390332789089 - fax: +390332785469
e mail: alois.sieber@jrc.it

Ardy THOONSEN
Boer & Croon
Amstelveenseweg 760
NL - 1081 JK AMSTERDAM
tel. :+31 203014751 - fax: +31 203014449
e mail: a.thoonsen@boercroon.nl

Maarten VAN DE VOORT
RAND Europe
Newtonweg
NL - 2333 LEIDEN
tel. :+31 71 5245151 - fax: +31 71 5245191
e mail: voort@rand.org

Hans VAN LEUVEN
Ministry of Transport
Nieuwe Ultleg 1
NL - 2514 BP THE HAGUE
tel. :+31 70 3516171 - fax: +31 70 3511692
e mail: Hans.vLeuven@dgg.minvenw.nl

P.C.H.J.M VAN MECHELEN
Boer & Croon
Amstelveenseweg 760
NL - 1081 JK AMSTERDAM
tel. :+31 20 3014751 - fax: +31 20 3014449
e mail: p.van.mechelen@boercroon.nl

Willem VENKEN
EC-OLAF
200, rue de la Loi
B - 1049 BRUSSELS
tel. :+32 2 2993036 - fax: +32 2 2966996
e mail: willem.venken@cec.eu.int

David WILLIAMS
HM Customs & Excise
26, Belgrave Manor, Brooklyn Road
UK – GU22 7TW Woking, Surrey
tel. :+44 08707852594 - fax: +44 08707853112
e mail: david.williams@hmce.gsi.gov.uk

Appendix 2: Workshop Agenda

Monday 28 October – Opening Dinner

Tuesday 29 October – The Threats

10:00 Welcome address: *Dr. Alois Sieber, Head of Unit: Humanitarian Security Institute for the Protection and Security of the Citizen, Joint Research Centre, European Commission*

10:15 Introduction of participants

11:15 Plenary session: Global Container Security After 9/11 – *Dr. Adnan Rahman, Director, Surface Transport and Aviation Program, RAND Europe*

11:45 The terrorist threat/problem(s) – *Dr. Peter Chalk, Expert on piracy and maritime terrorism, RAND*

14:30 Explanation about the proceedings for the rest of the day

15:00 Parallel Sessions: The threat/problem(s), as seen by:

- Group 1: The Ports
- Group 2: Governments (Customs, Coast Guard, etc.)
- Group 3: Forwarders
- Group 4: Shippers

17:30 Plenary Session

18:30 Conclusion of day's proceedings

Wednesday 30 October – Possible Solutions

10:00 Plenary Session – Introduction to the proceedings of the day

10:30 Technological solutions for tracking and tracing containers and their contents – *Mark Schwarz, Chief Operating Officer, TRI-MEX*

11:00 Safe InterModal Transport Across the Globe (SIMTAG), an EC-sponsored project to address the problem of intermodal transport of hazardous goods susceptible to terrorist interference – *Marion Robery, Thomas Miller & Co. Ltd.*

11:30 Review Of Safety And Security Initiatives Being Considered And Explanation Of Remainder Of Days Proceedings

14:00 Parallel Sessions on Solutions

16:30 Report From The Groups

17:30 Conclusions From Workshop And Thanks To Attendees