9/11 – ten years after: Security improvements in global container shipping during the recent decade

ZAGON CSABA

Abstract: Containerised sea shipping plays a key role in the global trade and traffic, hence its relevance may not be underestimated in the global security. It shows specific vulnerabilities to harmful and illicit intentions to break the trade supply chain or simply attempting to use it as a tool to threaten security. A new era has arrived. Prior to 9/11 port operators and shipping companies handled the risks that threatened the supply chain security from an economic loss point of view while border control issues have traditionally focused on commercial illegality or smuggling of prohibited goods. The events of 9/11 however, highlighted the risk that supply chains might be abused by terrorists to cause enormous physical and economic damage. The event also pointed out many unhandled vulnerabilities that could provide extraordinary opportunities for breaking the lines of defence. In response to that we have witnessed the proliferation of security-focused control regimes worldwide. Following a series of comprehensive analyses, numerous measures have been taken by national and international actors on different levels and points of the global trade supply chain. From all these efforts the clear intention arose that we need to safeguard global supply chains by evaluating advanced cargo scanning and data integration capabilities at overseas ports and inviting them into an operable international security system.

Keywords: container security, non-intrusive inspection, risk analysis, trade supply chain

Introduction

The terrorist attacks - now often referred to as September 11, or briefly 9/11 - has changed the world in many ways and its security, politics, law enforcement and intelligence aspects. Instead of a general overview however, this article is focusing only on the complex security problems of global containerised trade supply chains and aims to explore how they could be improvement. Nevertheless, 9/11 have not caused damages only, but it has triggered wide scale security revision that has revealed the vulnerabilities of U.S. border protection, identified its organisational, institutional and technical roots. The number of security gaps that had been identified proves that this process was worthwhile. These findings supported numerous initiatives and technical development. In a nutshell, the issue of security in general and the developments in the different spheres of security industry gained priority.

Even if the global trade supply chain constitutes just one from the above mentioned fields of security, this area has witnessed the most remarkable improvements in the recent decade.

As we will see later on, the United States has been the main driving force of these developments. Their ideas and developments in the field of security spread all over the world and influenced many other countries that have adapted their own sys-

tems accordingly and participate in security co-operations with their counterparts. This tendency is valid to many aspects of security development and may be considered as an absolutely positive phenomenon.

Shipping profile

It was not my objective to elaborate a comprehensive analysis of world trade and traffic, just to present some general and consciously not very detailed facts and figures that can provide a framework against which containerised traffic and besides sea-born container traffic may properly be evaluated.

Shipping of goods is commonly measured in tonnes while the delivery distance in kilometres. Interestingly enough, recent global shipping figures suggest that somewhat 80 percent of global commodity traffic measured in tonne-kilometres is transported by sea.

Commodity flow might be further categorised according to the character of the cargo such as bulk (liquid, dry), containerised, other combined ones like Ro-Ro, and so on. Surprisingly, if we look at the global trade from this perspective there is again a significant 80 percent share of containerised goods. These numbers indicate the relevance of seaborne container traffic and its links going to, or coming from the inland, the multimodal container terminals, and elsewhere.

Estimates of the European Commission (EC) also underpin the relevance of sea shipping industry. For instance, in their report titled as "Strategic goals and recommendations for the EU's maritime transport policy until 2018" it is mentioned that short-sea shipping carries still 40 percent of intra-European freight where, of course, no distant sea shipping was taken into consideration.[1]

Landlocked countries have somewhat different shipping profile, but surprisingly the share of sea shipping may grow up to 50 percent in their shipping performance measured also in tonne-kilometres. There are several landlocked countries in the European Economic Area (EEA) as well, so they had to work out their priorities and strategies, how they can get access to the global markets via seaports belonging to other countries. Even those countries that have access to the world sea trade through their own seaports have to pay attention how their inland agricultural and industrial products can reach the maritime shipping facilities at the seaports.

The competitiveness of the production of goods and the internal market of countries are highly dependent on the reliability and expenditures of the shipping chain, through which they can access to the relatively cheap deep-sea shipping.

Commercial rail and inland waterway routes gained therefore more and more significance in the past few decades. The so-called Helsinki corridors became main subjects for the transportation development projects in the European Communities. All these ideas are highly motivated by cost-efficiency, reduction of energy needs and emission of greenhouse gases.

There is no doubt that sea transportation has a core importance amongst the commodity transport modes globally, just as sea born container traffic has. This enormously large percentage taken from the global shipping industry alone generates

[1] *Strategic goals and recommendations for the EU's maritime transport policy until 2018*, European Commission, COM(2009) 8 final, Brussels, 21.1.2009, p.2

a continuous need for its characteristics to be analysed in order to be able to handle their risks properly.

Dependency on shipping capabilities

For Europe, shipping has been one of the key pillars to economic growth and prosperity throughout its history. Maritime transport services have always been essential in facilitating the European economy and European companies to compete globally. But Europe is not an exception, many other powers have strong dependency on the shipping capabilities, by which they can reach the world markets. Quality shipping is a key global competitive advantage for those powers, which are in position to enjoy the moderate costs sea commodity shipping allows them.

Trade among countries without a common border takes place mainly across the ocean. In particular, ocean shipping is the principle mode of transport for bulk commodities (such as oil, petroleum products, iron ore, coal and grain, etc). These represent a large share of trade in terms of weight, but a small and decreasing share in terms of value.[2]

In the field of technological innovations, the most important driving forces of globalisation were the ones that improved the speed of transportation and communications and lowered their costs. These included the adoption of containerisation in international shipping.[3]

Three important technological and institutional changes have lowered shipping costs: the development of open registry shipping (i.e. registering ships under flags of convenience to circumvent regulatory burdens and especially manning costs), scale effects from increased trade and containerisation. Standardised containers allow the use of a multi-modal transport system, without unpacking and repacking.[4]

About 40 percent of all incoming trade to the United States arrives by ship, and most of that in sea containers. Other countries, such as the United Kingdom, Japan, and Singapore, are even more dependent on sea container traffic.[5] Containers became essential elements of the global logistic chain and therefore their characteristics have strong impact on the world commodity flow.

Global pattern of container traffic

Containers are undoubtedly the most successful innovation in the freight transport sector in the 20th Century logistics. The global standardisation of shipping containers and container handling equipment triggered a revolutionary breakthrough in the character of the global logistic chain. In our time, container traffic represents a significant proportion within sea-shipping modes and is continuously increasing. Standard merchant containers have been invented in the 1950s and their use in global

---

[2] WTO: World Trade Report 2008, ISBN: 9789287034540, pp.83-84

[3] Ibid. WTO p.20

[4] Ibid. WTO pp.83-84

[5] CSI Fact Sheet, 2007 url: http://www.cbp.gov/linkhandler/cgov/trade/cargo_security/csi/csi_fact_sheet.ctt/csi_fact_sheet.doc downloaded on 02/10/2007

cargo shipping has been spread continuously since the 60s. More than five million freight containers are now in service throughout the world. This became possible principally by the international standardization. Containerised intermodal freight systems have significant advantages against bulk and piece cargo shipping especially in relation to the modal changes. The wide-range use of containers led to the spread of combined, or often referred as intermodal shipping modes and resulted in quicker and cheaper modal changes that happens often three or four times in the distant and intercontinental trade.

Since perceptible international trade is dependent on maritime transport, an increase in trade due to or as a means of globalization would naturally result in a corresponding increase in maritime traffic. Sea-born container traffic increased 10 percent in average in the last decade except the year 2009, when a global economic crisis broke this trend temporarily.[6] Available forecasts may vary, but we can say that the global ocean-borne commerce is expected to grow 3 to 4 percent annually into the foreseeable future.

Higher traffic and commodity exchange volume means higher risks and greater exposure. More intense traffic means more opportunities for criminals, and certainly higher risk for the malfunction of the logistic system. At the planning phase of any trade supply chain security measure, therefore, a very detailed traffic pattern analysis is essential. It is especially true in case of those global trends and dynamics that define the context of the container transportation system.

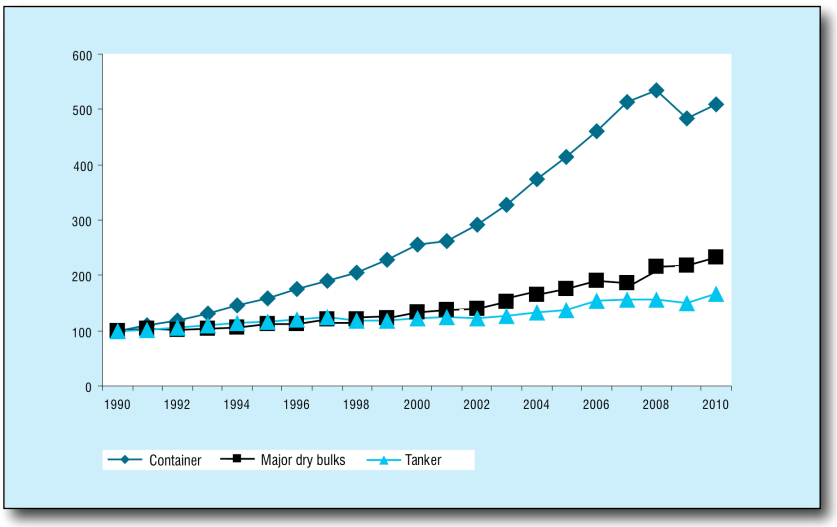


Figure 1 - Global container, liquid and major dry bulks volumes 1990-2010 (1990=100%)

Trade routes with over one million TEU are illustrated in the map below (see Figure 1). This indicates the scale of worldwide container traffic. Not surprisingly the Far Eastern region is the busiest one, by 43,2 per cent of all worldwide container trade that is going to, coming from or operating within there. These statistics were prepared by the UK Department for Transport for their assessment report in 2006, but the primacy of the Far Eastern region is still unquestionable, because almost every second container departs from there, arrives there or even circulates within that region. The second and the third busiest regions were the North American and Western European areas in 2006 by their 14,9 percent each.[7] All these cover 73 per cent of the global container traffic, and in the same time this figure shows the tripartite mainstream in the global flow of containers.

---

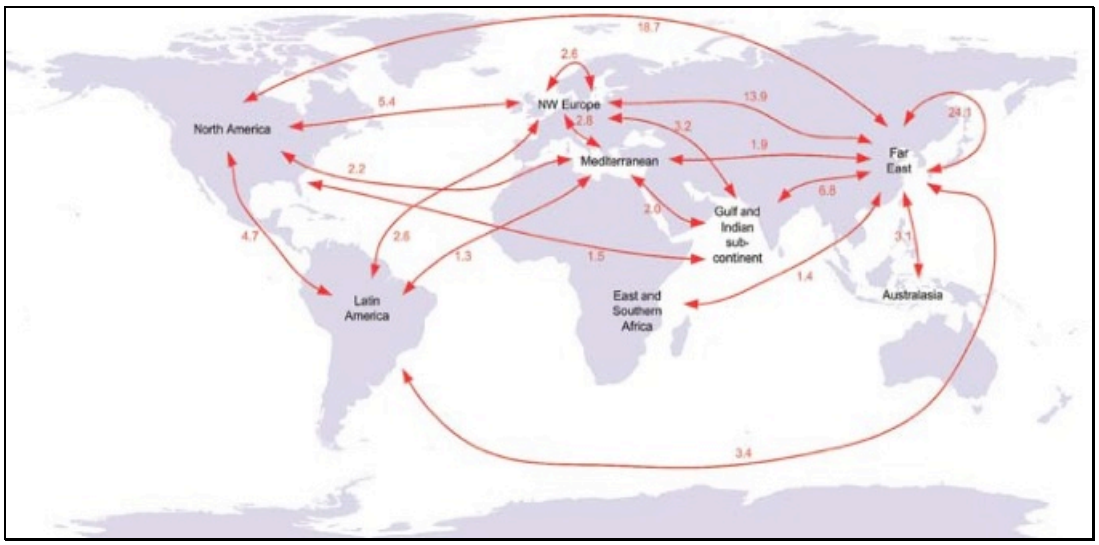
[6] *Review of Maritime Transport 2010*, UNCTAD, ISBN: 9789211128109, p.18

[7] MDS Transmodal, 2006 cited by the UK Department for Transport: The container freight end-to-end journey, 2008 p.13

Since naval strategists like the American Alfred Thayer Mahan, the British Sir Julian Stafford Corbett and others drew the attention to the crucial role of the narrows and straits in the control of the global sea trade (which is certainly one of the core elements of the sea power), these focal points became important scenes of guaranteeing security. Who has power to keep these "bottle necks" under control, has the power to influence the whole system very effectively.

Increased maritime traffic raises concerns about the safety of sea lines, of communication (SLOCs) and the transit through bottle necks — both from the safety of navigation and the environmental protection perspective as well as from a national security point of view. In light of the global terrorist threat, the security of the maritime transit lanes as well as the ports servicing international trade have become very serious concerns —concerns that were deemed almost inconsequential in the immediate post-Cold War years.[8]

Figure 2 - Shipping route container flows greater than 1 million TEU



Other bottlenecks might also be identified in the global system, in places where in a relatively small geographical area, a high intensity of commodities flows across. These points are the seaports. Not seaports in general, but the busiest ones, where the mainstream commodity flow of global trade is handled. Most of these locate at one of the above-mentioned three regions: in the Far East, North America and Western Europe. In the new container security programmes we have to bear in mind these focus regions, and we will see if they have done accordingly.

Characteristics of commodity flow

Professor Zoltan Lakner and Gyula Kasza from the Corvinus University analysed the global flow of foodstuffs. They pointed out in their article that there are focal points, mainstreams, minor flows and dead ends in the global food flow system. The international food supply chain changes time to time, creating new priority streams in the system. The European food map for instance showed the Netherlands and Germany as main centres of the commodity flow in 2008. Between these two entities were the most intensive relation meaning the highest volume of foodstuff exchange. This shape may be proven by the long distance shipping of processed food

[8] TANGREDI, Sam J.: *Globalization and Maritime Power*, Institute for National Strategic Studies, National Defence University, 2002. ISBN: 9781579060602 p.xxviii

products that went across the busy seaports of these countries. Rotterdam in the Netherlands, or Hamburg in Germany were the most frequent entry points for the food traffic all over Europe in that year.[9] Other focal points in Europe are such countries as France, the United Kingdom, Belgium, Italy, Spain –have busy container ports. All of them may be found in the list of the "European top ten" ports. Container transportation system handles not food staff shipping only. That means other containerised cargo may be subjects of similar analyses and, probably our observations will fit for them too.

Threats identified

Piracy

Throughout the history, pirates have always threatened the global sea transportation routes. It has been never happened the risk of piracy could reduce the states throughout their navies all over the world. The risk of piracy shows their specific pattern, and got increased or reduced by factors such as geography, stability of states, capabilities of their navies end so one. However, it is maybe not accidental that some areas at straights and narrows and their proximity are frequent scenes of pirate attacks, while others are not.

The reduction of pirate threat belongs the main responsibilities of the navies as they protect merchant shipping. For instance the Eastern basin of the Mediterranean "Operation Active Endeavour" is going on from 2001 by the NATO navies, that was later extended to the whole Mediterranean,[10] or "Operation Allied Protector" and its follow-up "Operation Ocean Shield" at the Horn of Africa – all are somehow related to 9/11.[11] The tasks of prevent, or deter a pirate attack, or claim back a ship that was fallen in hands of pirates belongs to the navies. However practically no example is known, when a containership was taken and pirates or other unauthorised third party individuals could access to the cargo in containers. When the command of a ship is taken it does immediately mean pirates can access containerised cargo a board. This is because of the loading standards; the proximity between containers is a few millimetres typically. Containers are placed into cells and packed onto one another. The doors may not be opened like that for most of the containers, so there without port machinery pirates are not in the position to pilfer the cargo.

Unauthorised access to the cargo has much higher risk when the container is at a terminal, at the customers' side or even when transported on road or by rail. During sea transportation accidents have still higher risk than cargo became stolen by pirates.

Vulnerabilities

The relevance of containers in the global supply chain is becoming more and more important. It turns us towards the container traffic and urges us to follow its specific security vulnerabilities. One dimension comes from the intensity of the con-

---

[9] LAKNER Zoltan – KASZA Gyula: Az élelmiszerlánc biztonsági kockázatai, Hadtudomány, 2011 electronic issue, ISSN: 1215-4121

[10] FODOR Péter: Katonai szövetségek szerepe az energiahordozók biztosításában, in Hadtudomány 2010. Electronic issue, ISSN: 12154121 www.mhtt.eu/hadtudomany/2010/2010_elektronikus/2010_e_5.pdf (downloaded on: 12/08/2010)

[11] International Institute of Strategic Studies (IISS): *The Military Balance 2010*, Routledge, 2010. ISBN: 9781857435573 p.106

tainer traffic that flows across continents entering busy ports, intermodal hubs, terminals, loading in and out to/from vessels, rail wagons, vehicles and so one all over the supply chain.

While merchant containers are ideal means for transportation of goods, they are just as good for transportation of illegal substances, contraband and even for human beings (stowaways) all over the world. Organised criminals have learnt how containerised logistic chain works and they have developed their facilities to exploit its opportunities well.[12] In most of the contraband smuggling cases the law enforcement faces with many signs of organised crime. This is especially true in cases committed on high value goods like drugs, cigarettes, counterfeit commodities (intellectual property theft), arms smuggling and similar ones, where a single perpetrator is inappropriate to arrange the entire "project" and the supporting logistics alone.

The problems of theft and smuggling demonstrate the relative ease with which criminal elements have capitalized on the use of containers as conveyances. Anonymity of contents, opaque ownership arrangements for vessels, and corruption in foreign ports have all facilitated the efforts of those who are inclined to use container shipping for illegal purposes.[13]

There are undeniable signs that criminal organisations started to act as transnational enterprises. This segment of cross-border crime became international security threat as their capabilities developed, and in the same time, this pattern of organised crime raised the attention of international security analysts as well.

United Nations Office on Drugs and Crime (UNODC) reports on illicit production and trade of drugs on a yearly basis. They indicated for instance, that sea trade plays significant role in the international drug transportation networks. This is especially true in the segments of cocaine and opiates, where containerised shipping is becoming more and more frequent.[14] However, containers may be considered also as frequent delivery means for other types of illicit drugs as seizure statistic figures indicate this in many member countries of the World Customs Organisation (WCO). WCO has also been monitoring and analysing by its Regional Intelligence and Liaison Offices the contraband seizures since the mid 2000. In their international seizure database called Customs Enforcement Network (CEN) more than 250 thousand records were entered until 2009, many of them were drugs. WCO releases on a yearly basis their analyst report on drugs, cigarettes smuggling and goods counterfeiting (intellectual property theft). These reports written on the respective criminal segments are based on the member customs administrations' intelligence shared in the CEN database and also the figures they provided. Therefore the reports became widely known analyst products by the law enforcement and security specialists.

Many WCO member customs administration have developed specific knowledge base for container search, some released handouts, rummage guides, training materials and similar papers even, and included into their training programmes. One of the best-known container search handout was compiled in the Customs 2002 pro-

---

[12] WONG, Anny: Chinese Crime Organizations as Transnational Enterprises in *Transnational Threats - Smuggling and Trafficking in Arms, Drugs, and Human Life*, THACHUK, Kimberley L. (eds.), Praeger Security International, ISBN: 9780275994044 pp.131-142

[13] WILLIS, Henry H. and ORTIZ, David S.: Evaluating the security of the global containerized supply chain, RAND Corporation, 2004, ISBN: 0833037153, p.1

[14] UNODC: World Drug Report 2010, ISBN: 9789211482560, see pages 17, 60, 63, 83, 85, 90

ject of the EC Directorate General for Taxation and Customs Union (DG TAXUD). More over, this training material was put on e-learning basis for better accessibility of the member customs administrations.[15]

Containerised transportation systems show their unique character along both arms of the logistic chain. On one hand containerised commodities flow to their destinations – this is one arm often considered as the only one in the logistic chain. On the other hand, upon delivery at the destination of the cargoes, containers become unloaded and re-transported to container depots and terminals. The cyclic logistic chain starts again when maintenance is done if necessary and the customers (suppliers, manufacturers, wholesalers) are supplied with containers to be loaded with cargoes again. So there empty containers have their own logistic needs and this arm of the logistic chain is just as capable for illegal goods (e.g. contraband) delivery as the other one.

The busiest container ports of the world have ten thousands throughput of containers daily, which is a logistic challenge itself. Port law enforcement agencies should identify the few ones posing threat for the countries or the logistic chain as an infrastructure. Instead of total control, modern border authorities especially Customs use selective control, targeting and profiling on a routine basis to find irregularities in the commodity traffic. The systematic application of such procedures and techniques are all based on intelligence and risk analysis, creating the frames of risk management system.[16] This allows keeping the balance between trade facilitation and security. That means customs can target the high-risk consignments, traders, means of transport etc. deployed their resources effectively, while at the other hand they use simplified means and procedures for trade facilitation purposes, where applicable. So there, the security function of border control does not result unnecessary waste of time and not increases shipping costs for those entities of the trade supply chain, where all regulations met and low risk level perceptioned by the law enforcement.

The capacities of ports, container terminals and in general the border crossing points are limited, just as the law enforcement agencies' resources are. So that it has crucial importance how these resources are deployed and the capacities used in order to get as good result as possible.

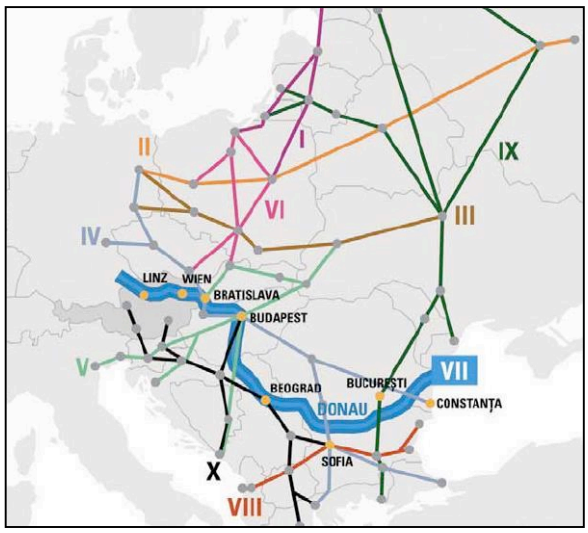


Figure 3 - Helsinki corridors in Cent-

Many people living in landlocked countries do not recognise the role of merchant seaports and the transportation routes landlocked countries can reach these gates of sea shipping (e.g. rail and inland waterways, motorways etc.). We have seen the importance of them at the introduction part this article. However I wonder to raise the attention to the different risk perception and in general, risk management approach how the law enforcement agencies estimate and handle risks for the same

[15] THE EUROPEAN COMMISSION, DG TAXUD: Good Practice Guide for Sea Container Control, Customs 2002 Programme, (may be downloaded from the url: http://ec.europa.eu/taxation_customs/elearning/demo/container/library/library.html)

[16] See details in TRUEL, Catherine: A Short Guide to Customs Risk, GOWER Publishing, 2010, ISBN: 9781409404538, pp.30-32

shipment at the seaports and at the inland territories.

I pointed out that significant portion of sea-born containers play role in the commodity transportation industry of the landlocked countries. Not quite rarely this may reach 50 per cent of the yearly transportation performance. The risk exposure rate of malfunctions or even cut of the supply chain due to an incident is also significant for the landlocked countries. Therefore the security of the containerised transportation systems are just as high priority for them as the countries with sea access. This has still security and economic priorities. For the Hungarian point of view Hamburg, Koper, Rijeka, Constanta or even Thessaloniki are the most frequent seaports where the sea-born container traffic exchange flows across. Please see Figure 3 and follow the Pan-European transportation corridors for the different seaports.

The availability and reliability of the access, its cost efficiency and time needs are not the only factors considered. Security had been promoted among them too, highly because of the lessons learnt from 9/11. If the mentioned seaports use the same security standards providing equal levels of security and access reliability, then time needs and cost efficiency can be considered the most. Time factor, however not so important at most of the containerised cargoes. Or at least the shipping time difference between the different transport modes are not so significant until a container can reach the mentioned seaports from the inland.

To demonstrate the difference I took three transportation examples from the PINE Report – Prospects of Inland Navigation within the Enlarged Europe.[17]

Case I: Containers from Rotterdam to Heidelberg (approx. 520 kms)
Case II: Liquid bulk from Rotterdam to Vienna (approx. 1200 kms)
Case III: Passenger cars from Austria to Romania (approx. 1250 kms)

In these relations rail transportation had from plus 5 percent to minus 15 percent cost efficiency compared to the road transportation, but rail's time needs were also significant 70 percent to 100 percent more than the tucks needs. This resulted for example 4 days instead of 2 and similar.

Inland waterway transportation system, where applicable, had 75 to 30 percent less costs compared to the road transportation, but the door-to-door time needs were 2,2 to 4 times longer than road shipping. That means 3,5 days instead of 1,5 or 8 days instead of 2. This indicates the enormous capabilities of reducing shipping costs by taking inland waterway transportation in case of no tide shipping time. Exact expectations may be created from the data of a certain shipping assignment.

Turning back to the security issues, the risk management systems used at the seaports are sensible for different risk indicators and factors from other inland countries' respective or counterpart agencies' systems. Due to the limited resources port risk management has, they often consider low risk although the many risk indicators identified, because of the shipment's consignee locates inland and the commodities leave the port under the responsibility of a freight forwarder considered as safe. Uneconomically routed container indicated with used, low value cargo for instance flows through the port security system, just because of the forwarding proposal indicates rail transportation service. This is considered as safe due to the rail forwarding company provided guarantee on the customs duties. However container was loaded with contraband cigarettes for example, which did criminals remove during the rail transportation phase. In this case I put here for illustration purposes, customs is unable to keep real cargo under surveillance and is able to claim the freight forwarder's guaran-

[17] PINE Report, viadonau, 2004, pp.404-407 (url: http://ec.europa.eu/transport/inland/studies/doc/2004_pine_report_report_concise.pdf)

tee funds solely, not the ones according to the real cargoes. I would have called many cases for further analysis here according to my own domestic and foreign experiences. Although this given, and some other scenarios may be identified as a real gaps, inland authorities have very little – if not at all - impact on the ports of entries at the same common customs zone to change their risk management system respectively.

Security gaps may vary at the ports, many of them had been identified but not solved prior to 9/11. Peter Chalk browsed them in his article published in Loyd's MIU Handbook. He groups the gaps into categories as follows, however the list is not exhaustive[18]:

1. The sheer volume of commercial freight that is moved by container ships effectively eliminates the possibility of comprehensive checks once the cargo reaches its port of destination. Even in countries with advanced x-ray and gamma scanning technologies, inspection rates remain minimal, usually not more than 10 percent.
2. The highly complex nature of the containerised supply chain creates lots of opportunities for terrorist infiltration. Unlike other cargo vessels that typically handle payloads for a single customer loaded at port, container ships deal with goods and commodities from hundreds of companies and individuals, which in most cases, are received and transported from inland warehouses characterised by varied on-site security. For even a standard consignment, numerous agents and parties would be involved, including the exporter, the importer, the freight forwarder, a customs broker, excise inspectors, commercial trucking firms, railroad, dockworkers, and possibly harbor feeder craft and the ocean carrier itself. Each point of transfer along this spectrum of movement represents a potential source of vulnerability for the overall security and integrity of the cargo, providing terrorists with numerous opportunities to "stuff" or otherwise tamper with the boxed crates.
3. The primitive nature of the locks that are used to seal containers. Existing devices offer little, if any protection, and often consist of nothing more than a plastic tie or bolt that can be quickly cut and then reattached using a combination of superglue and heat. Most commercial shipping companies have been reluctant to develop more resistant mechanisms, given the costs involved. A standard seal can be purchased for a few cents if ordered in bulk, whereas more robust versions might run to several hundreds of dollars. Moves to develop so-called smart boxes equipped with global positioning systems (GPS) transponders and radio frequency identification devices (RFIDs) that emit signals if they are interfered with have run into similar problems and had not, at the time of writing, been embraced with any real degree of enthusiasm by the international maritime industry.
4. The overall vulnerability of crated cargo is further exacerbated by the "Trans International Routier" (TIR) haulage system, which is used to transport such merchandise from warehouse to port. Any container bearing the TIR logo is assumed to have had its contents inspected and sealed at source by relevant authorities—a designation that precludes any additional checks before dockside loading. There are a variety of ways in which terrorists could compromise and exploit this internationally recognized arrangement for their own purposes, ranging from spray painting a false logo on the outside of a generic; preloaded

[18] CHALK, Peter: Maritime Terrorism: Threat to Container Ships, Cruise Liners, and Passenger Ferries in Lloyd's MIU Handbook of Maritime Security, CRC Press, 2009, ISBN: 9781420054804, pp.117-132

crate, to bribing officials to issue a TIR designa tion for a container that had already been tampered with; to stealing and "stuffing" one *en-route* to a port.

5. The effectiveness of point-of-origin inspections for containerized freight is highly questionable. Many resource-constrained states in Asia and Africa fail to routinely check dockworkers, do not require that truck drivers present valid identification before entering an off-loading facility, and frequently overlook the need to ensure that all cargo is accompanied by an accurate manifest. Even richer nations in Western Europe and North America are not devoid of these types of deficiencies. Privacy regulations in the Netherlands, for instance, preclude the option of comprehensive security checks for dockworkers without first gaining their permission. In the words of one Dutch expert, "I would be amazed if harbor employees at Rotterdam, Antwerp, or Amsterdam were required to undergo any form of mandatory background criminal check." In the United States, about 11,000 truck drivers enter and leave the Long Beach terminal in Los Angeles with only a standard driver's license, whereas Singapore, which runs arguably one of the world's most sophisticated commercial maritime terminals, does not require shipping companies to declare goods on their vessels if they are only transiting through the country's port. That means that the government does not know what is being transported on the vast bulk of carriers that tranship through the city-state.
6. The absence of uniform and concerted safeguards is problematic as it is virtually impossible to inspect containers once they are on the high seas, while delaying checks until after they arrive at their destination may be too late to prevent a terrorist event from occurring. The enactment of the International Ship and Port Facility Security (ISPS) Code is designed to offset some of these problems by mandating a minimum set of requirements to govern the integrity of the maritime export-import chain; however, the initiative still suffers from a number of serious gaps.

Even if the customs services of the landlocked countries are not in the position to influence efficiently other member states risk managements and procedures, where containerised cargo throughput crosses the customs borders, they have to raise a discussion at the competent community forums.

Additionally they have to find other choke points at their inland side of the supply chain to provide security. Independently from these, landlocked countries customs, and in general law enforcement agencies should know how seaports are operating, and which kind of selective control they can provide. The "gaps and lacks" must be considered at the development of their own system.

Container shipping as a critical infrastructure

Upon we pointed out countries' dependency on the containerised cargo supply chains another approach has arisen concerning critical infrastructure protection. The idea of critical infrastructure protection within the security industry gained strong priority upon 9/11 and spread across the international security community. Researchers received support from the governments in many countries and its results have been implemented in the risk management systems of the catastrophe responders and the countries' threat reduction and prevention mechanisms.

Respectively, we do not turn here to a detailed analysis of critical infrastructures, just we allocate that there are many approaches and sometimes not even slight

differences in the definition what infrastructure belongs to it.[19] Known researchers of this issue put it that although no common definition and vocabulary have already worked out, there may be some group of joint criteria to be identified.

Containerised shipping and trade supply chain has network pattern or chain structure. There is some interdependency with other sorts of infrastructures due to known links, dependency relations and interactivity. The interdependency should not necessarily be direct or close relationship between these infrastructures. It is not conditional that a country or a group of countries should have located their critical infrastructure within their own territory. Finally the infrastructure has a certain (but difficult to define as a finite) mass, goes beyond a certain limit that in case of cut off leads to a serious harm or damage.

Taking these criteria together, we can identify and determine containerised trade supply chain as a critical infrastructure.

Contradiction in critical infrastructure protection

The interest and responsibility for the critical infrastructure protection belongs to the owners and operators belonging either to the state or the private sectors. This endorses the customers' satisfaction, guarantees the service quality and supports the reliability as part of the company profile. Although no specific legal regulation are available in some cases, many owners and service operators recognised this and they developed their own security system and emergency procedures and voluntarily develops them on their free will. The states and International Organisations task is to give motive and assistance to the service operators by creating clear legal background, handing over information necessary, developing specific financial sources for support programmes – briefly by creating inspiring environment for that.[20] In contrast with these, profit maximisation is that keeps the entrepreneurial sector operational. This phenomenon equally works for the elements of the shipping industry as well.

Port operations and technology are optimized so that ships spend a minimum amount of time at the quay and the maximum time *en-route*. The principal concern of business is to increase the efficiency of the global supply chain, paying comparatively little attention to security. In recent years, ocean carriers have cut crews to an absolute minimum and have continued to order larger and faster ships in an effort to squeeze every cent of profit from the system.[21] Prior to 9/11, supply-chain security focused primarily on reducing shrinkage—the loss of cargo shipments through theft and misrouting. This risk motivated action in the private sector solely.

These led, in short terms, to the neglect of security means and regulations. An accident or a security incident may cut the infrastructure in operation, the accessibility to the service. However, is the clear interest of the profit orientated economic operator to reduce the risks as low as possible of such a service cut or malfunction, because of the very serious economic loss and other consequences such events may probably result.

---

[19] See e.g. POTÓCZKI György: Áttekintés a kritikus infrastruktúra védelem jelen helyzetéről, a továbblépést nehezítő tényezők elemzése útján, in Hadmérnök, 2010, Vol.5. No.2. ISSN: 17881919, pp. 203-218

[20] KIRÁLY László – MEDVECZKY Mihály: Védelemgazdasági ismeretek, ZMNE, 2009, ISBN: 9789637060755, p.95

[21] Ibid. WILLIS-ORTIZ, p.1 cited POLLACK, Richard: The Colombo Bay, Simon and Schuster, New York, 2004. ISBN: 9780743200738

Megaterrorism scenarios

Since the aftermath of 9/11 terrorist attacks on the United States, maritime security threats have been major sources of global anxieties considering the vulnerability of the world's oceans to maritime terrorism. Although historical and empirical evidences have indicated less terrorist attacks on seas before and after 9/11, there is a tremendous fear that maritime vessels and facilities are facing the awesome risks of maritime terrorism. This risk is aggravated by the fact that compared with the land and air, the "sea has always been an anarchic domain" that it is "barely policed, even today." Moreover, the seas have become the medium of various transnational threats that undermine regional and global security.[22]

Security of the system has traditionally focused on reducing shrinkage—the loss of cargo shipments through theft and misrouting. However, heightened awareness of terrorism has redefined supply-chain security—the consequences of an attack on or via a critical global port could be a tremendous loss of life and a crippling of the U.S. economy—and has brought increased attention to the risks containerized shipping presents.[23]

Heightened awareness of terrorism has redefined supply-chain security and increased attention to the risks containerised shipping presents. The west-coast port lockout of 2002 in the USA suggested the magnitude of economic effects a terrorist-related event might cause. Estimates placed the losses for the ten-day lockout between 4.7 billion and 19.4 billion USD.[24] Booz, Allen and Hamilton reported in October 2002 that a 12-day closure required to locate an undetonated terrorist weapon at one U.S. seaport would cost approximately 58 billion USD.[25]

The Hungarian logistics security researcher Attila Horvath raised the attention in his article that such an attack against port infrastructure may cause serious damages along the whole logistic chain, even at their inland arms in landlocked countries.[26] In May 2002, the Brookings Institution estimated that costs associated with U.S. port closures resulting from a detonated WMD could amount to 1 trillion USD, assuming a prolonged economic slump due to an enduring change in our ability to trade.

Currently, the undisputed leader of the maritime terrorism nightmare scenarios is an attack with a weapon of mass destruction voyaging to its target not on the tip of a missile but hidden in a container on board of a large container ship. Number two on the list is the "floating bomb" scenario, that is, a hijacked liquefied petroleum gas (LPG) or liquefied natural gas (LNG) tanker driven into a major port and exploded there, with the intent of disrupting seaborne global trade. The number three position is currently held by the "momentum weapon" scenario, which revolves around a large ship such as an ultra-large crude carrier or a chemical tanker. In such a case, the terrorists would attempt to drive a large vessel into the harbour at high speed to ram either other ships with vulnerable cargoes or oil terminals and the like and then detonate the ship. Such a scenario has been developed, for example, for the port of Singapore, home of South- east Asia's largest oil refineries. All of these maritime megater-

---

[22] Lloyd's MIU Handbook of Maritime Security, CRC Press, 2009, ISBN: 9781420054804, p.253

[23] Ibid. WILLIS-ORTIZ, p.ix

[24] Ibid. WILLIS-ORTIZ, p.2 cited IRITANY, Evelyn, and DICKERSON, Marla, "Calculating Cost of West Coast Dock Strike is a Tough Act," Los Angeles Times, November 26, 2002; and COHEN, Stephen S., Economic Impact of a West Coast Dock Shutdown, Berkeley, Calif.: University of California, 2002.

[25] Container Security Initiative: 2006--2011 Strategic Plan, CBP, Aug. 2006, p.11

[26] HORVÁTH Attila: Characteristics of terror-threats in goods transportation, AARMS, Vol. 8, No. 2 (2009), ISSN: 15888789, pp.345–355

rorism scenarios have one thing in common: they still firmly belong to the realm of fiction.[27]

The threat scenario of a containerised WMD is delivered to US seaports arose in the 90s, or even earlier, however this have properly been analysed as part of the follow-up gap analyses of 9/11. Although such incident, or even attempted assault has never been detected, the threat was considered as possible and real.

The conjunction of three trends—globalization of industry, trade, and transport; proliferation of nuclear weapons technology, and the threatening rise of globally dispersed, WMD-armed, undeterred terrorism—today present an unprecedented threat to the United States, all its trading partners, and the whole civilized world.[28]

One of the latest warnings of a "real and current" threat of terrorist attacks involving WMD smuggled in innocent cargo was issued on 8 November, 2004 by Mohamed El-Baradei, head of the United Nations' International Atomic Energy Agency, at a conference on nuclear proliferation. He stated investigations in suspected weapons programmes had revealed an extensive global black market making radioactive materials accessible to terrorists. His agency counted around 630 confirmed incidents of trafficking in nuclear or other radioactive materials since 1993, leading to what he described as a "race against time" to forestall a terrorist attack. Analyses concluded that Osama bin Laden was seeking to acquire nuclear weapons in order to expand the "attack arsenal" of Al-Qaeda.[29]

Preventive measures

As we have seen maritime containers represent a significant part of the international trade and supply chain, which frames the backbone of the world economy system. Containers transport involves numerous manufacturers, logistic nodes, operators, platforms and checkpoints (in particular container ports). To improve their security there are some requirement needs like an integrated research and development approach, including risk assessment, traceability, secure exchange between nations and across operators, and fast but effective screening.

The sheer volume of international maritime container traffic, the sophisticated and often ingenious concealment methods, along with the diverse routings adopted by organised criminals like illicit drug traffickers and other commodity smugglers, invariably makes the successful interdiction very difficult. Seaports are notoriously difficult and at the same time dangerous places to work and law-enforcement structures are often hampered by a lack of resources, interagency mistrust, complex port processes and systems, and other factors, which are purposefully exploited by criminal and terrorist organisations. This situation poses a very real and serious threat to the security of the international trade supply chain that plays so important role in the sustainable development of the world economy that has high vulnerability on the logistic chains.

---

[27] Ibid. Lloyd p.57

[28] ABT, Clark C.: The Economic Impact of Nuclear Terrorist Attacks on Freight Transport Systems in an Age of Seaport Vulnerability, 2003. url.: http://www.abtassociates.com/reports/ES-Economic_Impact_of_Nuclear_Terrorist_Attacks.pdf

[29] ORSZÁG-LAND, Thomas: Special Report - US expands cargo screening net in Jane's Terrorism & Security monitor, November 01, 2004

Container Security Initiative

Challenges of border formalities in the ports

Although the busiest container ports may be selected quite easily, time and area frames for inspection are very limited, just as the capacities available at the seaports where the enormous number of containerised cargo is delivered either as a final destination or for further shipping. In 2006, more than 11.6 million maritime containers arrived at United States seaports, an average of 32,000 a day.[30]

The paradox of border formalities is that governments usually have separate and unequal processes for managing exports and imports. The high priority given export facilitation often results in reduced controls at departure. With clear revenue and security incentives to control incoming cargo, imports are more rigorously managed. Risk assessment for import cargo release is commonly performed after goods arrive at their port of entry.[31]

Perspectives of cargo movements

Encouraged by the WCO, leading nations are adopting a different perspective. Instead of viewing cargo movement as discrete departure and arrival transactions, they see it as an end-to-end, integrated process from point of manufacture to final delivery destination. Sometimes referred to as an *"elastic border" model*, customs in the arrival country expands its formal control horizon beyond physical borders – back to the shipment's origin and forward to the ultimate delivery location. To facilitate this sort of international and public/private sector integration, the WCO has established standards for mutual recognition, certification and risk management.[32]

Andrew Grainger highlighted the slight interest differences between the business operators and the government agencies in providing security at the ports and along the supply chain. The challenge in reducing transaction costs and meeting regulatory control objectives – like those of increased security – is to consider how best to align the institutional framework with operational requirements. For government agencies, as set out earlier, it is to make efficient use of finite enforcement resources, enhance controls at the border, *extend controls up and down the supply chain*, and to ensure that trade continues. For businesses, the management objective in supply chain management is about reducing costs and increasing value.[33] CSI programme's core part and distinct aim is an extension of the control (involving non-intrusive inspections and physical checks) upwards and downwards of the supply chain by erecting checkpoints at the most frequent ports where from the US-bound cargo is delivered to the American ports of entries. Many examples are known about such border extensions at the land borders where for some reasons at one geographical point the border agencies of both neighbouring countries are present; one of them operating necessarily at the other's soil, but on their own customs territory. However, such an unexampled co-operation has never been arranged in the spheres of sea borders, especially

[30] CSI Fact Sheet, 2007
[31] BARTON et al: Expanded borders, integrated controls - Achieving national prosperity and protection through integrated border management in Border Management in the New Century, IBM, 2007 p.7
[32] Ibid. BARTON, 2007 p.7
[33] GRAINGER, Andrew: Supply chain security: Adding to a complex operational and institutional environment, in World Customs Journal, Vol. 2007, Issue 2. ISSN: 18346715, p.26

not in so many ports in the same time that CSI concerns. American authorities developed this solution that may really be considered as a global one.

CSI has multi purpose objectives like protection of the American people, society and economy by securing the borders and protection of lawful trade, travel and immigration. CSI also promotes of national resilience by strengthening nationwide preparedness and response. It prevents of terrorism at ports of entry by pushing the US's zone of security outward and beyond their physical borders through partnerships on extended border initiatives to deter and combat the threat of terrorism. CSI balances the legitimate trade and travel by promotion of industry and foreign government partnerships by engaging foreign governments, the trade community and others in the supply chain in cooperative relationships.[34]

CSI's structure has four core elements as follows:[35]

1. Identify high-risk containers. CBP uses automated targeting tools to identify containers that pose a potential risk for terrorism, based on advance information and strategic intelligence.
2. Pre-screen and evaluate containers before they are shipped. Containers are screened as early in the supply chain as possible, generally at the port of departure.
3. Use technology to pre-screen high-risk containers to ensure that screening can be done rapidly without slowing down the movement of trade. This technology includes large-scale X-ray and gamma ray machines and radiation detection devices.
4. Use smarter, more secure containers, which will allow CBP officers at United States ports of arrival to identify containers that have been tampered with during transit.

Limited numbers of ports handling the mainstream of the traffic

The more intensive traffic originates from the port, the higher priority for participation in CSI programme. Although the containers arrive from various ports throughout the world, about 49 percent of U.S.-bound containers arrive from the top 10 international ports.[36] Until 2007 the number of CSI ports had been increased to 58 of which covers 86 per cent of the container traffic.[37] In 2002, roughly 7 million containers entered U.S. seaports creating about 87 percent of these ocean containers that entered 10 U.S. seaports only.[38]

The second most frequent partner region for the U.S.-bound container traffic is Europe. The EU-US container traffic was concentrated in a relatively small number of ports, the most noticeable five ports are Rotterdam (NL), Hamburg (DE), Bremen/Bremerhaven (DE), Antwerp (BE), Valencia (ES) covering together more than a half of the total.[39]

---

[34] Ibid. CBP, p.3
[35] CBP: Container Security Initiative 2006–2011 Strategic Plan, p.ii
[36] GAO-03-770 Container Security Report, July 2003, p.5
[37] Ibid. CBP, p.37
[38] Ibid. GAO-03-770, p.5
[39] HESELER, Heiner: Strategic activities of the Free Hanseatic City of Bremen in the field of new technologies for container security, Conference on Maritime Container Security, Bremen 10/09/2009

This figure indicates that if traffic density is taken into consideration as risk indicator (for instance by creating a Pareto chart) strong efficiency can reach at the very beginning of the project. A very few number of ports involvement causes high coverage in the container traffic. This strengthens the strong risk basis CSI programme should be built on.

Security and Trade Facilitation

CBP has to perform this security and border-related work while facilitating the flow of legitimate trade and travel that is so important to the U.S. economy. In other words, Customs has "twin goals"— building more secure and more efficient borders.

The CSI program benefits from the greater exchange of customs-to-customs information resulting from bilateral cooperation and international awareness established to secure global trade. Further, a generally positive perception exists that CSI is a dynamic, flexible program that promises to neutralise large-scale threats and intercept high-risk containers while facilitating the flow of legitimate trade.

Organisational changes in the security system

Because of its core frontline responsibilities for inspection at US border crossing points (BCP), the US Customs Service assumed the lead role in improving ocean container security and reducing the vulnerabilities associated with the overseas supply chain. By January 2002, Customs had initiated the CSI program and also Customs-Trade Partnership Against Terrorism (C-TPAT) to enhance the security of the global supply chain and deter international acts of terrorism, as well as facilitate the smooth passage of commerce across US borders. The purpose of CSI is to enable Customs to screen for high-risk containers in key ports overseas, while the purpose of C-TPAT is to improve global supply chain security in the private sector.[40]

In March 2003, the US Customs Service (USCS) was transferred to the new Department of Homeland Security and other federal law-enforcement agencies have also been reorganised likewise. The border inspection functions of the Customs Service, along with other US government agencies with border protection responsibilities, were arranged into the Bureau of Customs and Border Protection. The scenario that effected among others, this structural reform is known worldwide. We do not focus here on the sequence of events stipulated a new paradigm in security thinking. What we explain here is more about the effect on the trade supply chain and the border security. We also would express here certain efforts willing to reduce the risks of the international transportation systems aiming to serve trade facilitation and security in wider manner in the same time.

To implement CSI, CBP negotiated and entered into bilateral arrangements with foreign governments, specifying the placement of CBP officials at foreign ports and the exchange of information between CBP and foreign customs administrations. CBP first solicited the participation of the 20 foreign ports that shipped the highest volume of ocean containers to the United States. These top 20 ports are located in 14 countries and regions and shipped a total of 66 percent of all containers that arrived in U.S. seaports in 2001. CBP has since expanded CSI to strategic ports step by step up to 58 ports. These new ones, which may ship lesser amounts of cargo, but may also have terrorism or geographical concerns.

[40] GAO-03-770 Container Security Report, July 2003, p.1

To participate in CSI, a host nation must meet several criteria. The host nation must utilise a seaport that has regular, direct and substantial container traffic to ports in the United States. There must be a competent Customs staff with the authority and capability of inspecting cargo originating in or transiting through its country, and there should be installed nonintrusive inspection equipment with gamma- or X-ray capabilities and radiation detection equipment. Additionally, each potential CSI port must indicate a commitment to establishing an automated risk management system, and they have to be ready to share critical data, intelligence, and risk management information with CBP officials. They have to conduct a crosscutting port assessment to ascertain vulnerable links in a port's infrastructure and commit to resolving those vulnerabilities. Host country should also maintain a program to prevent, identify, and combat breaches in employee integrity.

To prepare for implementation of CSI, CBP sends an assessment team to each potential CSI port to collect information about the port's physical and information infrastructure, the host country's customs operations, and the port's strategic significance to the United States. CBP then deploys a CSI team, which generally consists of three types of officials—special agents, targeters, and intelligence analysts. These officials come from either CBP or U.S. Immigration and Customs Enforcement (ICE).[41]

The collaboration between Customs administrations improves their capabilities and increases the overall effectiveness of the targeting process. The mutual goal is to target containerized cargo that poses a potential risk for terrorism and secure maritime trade from acts of terrorism.

Inspections

The large volume of imports and the Customs' limited resources make it impractical to inspect all oceangoing containers without disrupting the flow of commerce. It is unrealistic to expect that all containers warrant such inspection because each container poses a different level of risk based on a number of factors including the exporter, the transportation providers, and the importer. CBP has implemented an approach to container security that attempts to focus resources on particularly risky cargo while allowing other cargo to proceed.

CBP's domestic efforts to target cargo to determine the risk it poses rely on intelligence, historical trends, and data provided by ocean carriers and importers. Pursuant to federal law, CBP requires ocean carriers to electronically transmit cargo manifests to CBP's Automated Manifest System 24 hours before the cargo is loaded on a ship at a foreign port. This information is used in the Automated Targeting System (ATS). ATS is characterized by CBP as a rule-based expert system that serves as a decision support tool to assess the risk of sea cargo. In addition, CBP requires importers to provide entry-level pre-arrival data that is used also by ATS to screen all containers to determine whether they pose a risk of containing WMD.[42]

High tech detectors in service

In general there are two types of inspections that CBP inspectors may employ when examining cargo containers: non-intrusive inspections (NII) and physical exam-

[41] Container Security: A Flexible Staffing Model and Minimum Equipment Requirements Would Improve Overseas Targeting and Inspection Efforts, GAO-05-557, 2005, p.13

[42] Ibid. GAO-05-557, 2005, pp.7-8

inations. The NII involves the use of X-ray or gamma-ray scanning equipment at least. This sort of equipment is supposed to scan a container and generate an image of its contents according to the density pictured. Customs inspectors are to review the image to detect any anomalies, such as if the density of the contents of the container is not consistent with the description of the contents. If an anomaly is apparent in the image of the container, inspectors are to decide whether to conduct a physical examination of the container.[43] Inspectors use additionally radiation detection devices to detect the presence of radioactive or nuclear material as well as explosive detectors.

CBP extended its targeting and inspection activities to overseas seaports by the use of the principle of elastic borders.

Announced in January 2002, CSI was implemented to allow CBP officials to target containers at overseas seaports so that any high-risk containers may be inspected prior to their departure for US destinations.

Sustainability

Security remains a major consideration for shipping. While enhanced security measures in transport and across supply chains are now part of doing business, some developments – especially at the national and regional level – have implications for a globalized industry such as shipping.

One such current issue is cargo scanning, with its related questions of technical feasibility and economic viability, and, more importantly, the questions of trade-friendliness, balance, and the level playing field that should exist, especially for smaller players in developing regions. In this context, the United States' 100-per-cent container-scanning initiative, which requires foreign ports to scan all containers bound for the United States, is of particular concern, especially for trading partners of the United States, for the transport industry and for traders and shippers.

DHS and CBP established the Secure Freight Initiative (SFI) to test the feasibility of scanning 100 percent of U.S.-bound cargo containers, but face challenges expanding the program. In October 2009, GAO reported that CBP has made progress in working with the SFI ports (formerly referred as CSI ports) to scan U.S.-bound cargo containers; but because of challenges implementing scanning operations, such as equipment breakdowns, the feasibility of scanning 100 percent of U.S.- bound cargo containers remains largely unproven.[44]

Trials at a number of foreign ports show that the technology required scanning containers automatically and effectively does not yet exist. The measure is also costly, as illustrated by the figures put forward by the European Commission, which estimate that investment until 2020 would require $280 million, while operational costs would amount to $270 million annually. Recognizing these difficulties, the Department of Homeland Security announced in December 2009 that it would postpone the mandatory application of this requirement until 2014.[45]

The most experts criticises 100 per cent container scanning proposal. The US SAFE Port Act requires 100 per cent scanning of all US-bound container cargo by 2014 using non-intrusive inspection equipment, including imaging equipment (X-rays or gamma scanners) to create images of the containers' contents, and radiation detec-

[43] Ibid. GAO-05-557, 2005, pp.9-10

[44] Maritime Security: DHS Progress and Challenges in Key Areas of Port Security, GAO-10-940T

[45] Ibid. UNCTAD, p.21

tion equipment at foreign ports. A pilot program to test the feasibility of 100 per cent scanning has been conducted at six selected CSI ports. While in theory the physical inspection of the contents of every container provides the best determination of a security risk, it is also one of the most costly and labour-intensive measures to implement. To illustrate the magnitude of the task, of more than 7 million containers that entered the US in 2002, approximately 10 per cent were inspected and scanned (up from 2 per cent prior to 9/11). In Rotterdam the figure is about 5 per cent and in the UK it is between 4 and 7 per cent reported OECD in 2005. Many customs administrations undertake 100 per cent screening of containers in the sense that the associated information is screened, but none physically examine 100 per cent of their container traffic, either through the use of scanning equipment or otherwise. Indeed, this would be impossible with currently available technology and the volumes of containerised trade. The proposal for 100 per cent scanning in the current maritime operating environment represents the antithesis of risk management. On the other hand, screening, which in many cases is now fully automated, forms an integral part of an appropriate risk management regime that assists in identifying those containers, which may pose a security (or other) risk, and are therefore candidates for scanning and inspection. The 24-Hour Rule (pre-arrival data) and similar requirements for advance information contributes to the screening process and the early identification of high-risk cargo. The difficulties of achieving 100 per cent scanning coupled with physical inspection have been highlighted by a number of national and international organisations including the US General Accounting Office (GAO) and the OECD.[46]

100 per cent container-scanning initiative that requires foreign ports to scan all containers bound for the United States, is of particular concern, especially for trading partners of the United States, for the transport industry and for traders and shippers. Trials at a number of foreign ports show that the technology required to scan containers automatically and effectively does not yet exist. The measure is also costly, as illustrated by the figures put forward by the European Commission[47], which estimate that investment until 2020 would require $280 million, while operational costs would amount to $270 million annually. Recognizing these difficulties, the Department of Homeland Security announced in December 2009 that it would postpone the mandatory application of this requirement until 2014.[48]

Container scanning equipment can increase the number of consignments that receive customs attention without causing undue delay, and can identify illicit goods. The equipment requires a large capital outlay, however, and the process of introducing it, from conception through operation, affects the entire control and intelligence sectors and requires changes to the infrastructure and procedures of customs. To justify the outlay, and to ensure maximum return for the investment, it is necessary to

---

[46] WIDDOWSON, David and HOLLOWAY, Stephen: Maritime Transport Security Regulation: Policies, Probabilities and Practicalities, in World Customs Journal, 2009, Vol. 3, No. 2, ISSN: 1834-6715, pp. 17-42

[47] The European Commission, DG TAXUD: Secure Trade and 100% Scanning of Containers, European Commission Staff Working Paper, p. 4-5, (downloaded: http://ec.europa.eu/taxation_customs/resources/documents/common/whats_new/sec_2010_131_en.pdf on 01/06/2011)

[48] Ibid. UNCTAD, p.21

ensure that scanning equipment is used effectively and that it is fully integrated into the risk assessment regime.[49]

Summary

International and domestic incidents over the recent years have emphasized the need for an integrated approach to supply chain security management. Just as a chain is no stronger than its weakest link, a supply chain is only as secure as its weakest link, which includes the suppliers, manufacturers, wholesalers, retailers, carriers, terminals, and governmental organisations that plan, manage, facilitate, and monitor the global movement of goods.

Massive improvements have been done globally in result of the changing security environment after 9/11. One groups of these relates to the known and real security gaps, participants of the international shipping industry were unable (or sometimes simple reluctant) to solve. These gained a strong motive to be reactively solved. Another groups were when theoretical threats were identified, and efforts were proactively taken to prevent such events.

Although the lead was taken by the U.S., the practices, new ideas and technical means spread all over the world. As a result of this, and also because the significantly strengthened security in the U.S.-bound container traffic that is a very large part of the global traffic volume, U.S. security efforts has global impact. This may be considered as an absolutely positive fact.

Despite the Container Security Initiative programme was designed on a risk basis in many aspects, one of the core element of the programme – the 100 per cent scanning – is not in line with that principle. It seems to be, however, that the decision makers recognised it and hanged over to achieve it on a temporary basis. In the time frame available due, other procedures may be worked out instead.

The containerised trade supply chain shows characteristics of a critical infrastructure. It is the researchers responsibility[50] not to cut off their work on the container security issues. They should report all the changes in the security environment and the security gaps newly identified.

---

[49] DE WULF, Luc and MATITYAHU, Omer: The Role of Customs in Cargo Security, in Customs Modernisation Handbook, Luc De Wulf and José B. Sokol (eds.), The World Bank, 2005, ISBN: 0821357514, pp.266-283

[50] HORVÁTH Attila: Hogyan értessük meg a kritikus infrastruktúra komplex értelmezésének fontosságát?, Hadmérnök, Vol.5 No. 1. 2010., ISSN: 17881919, pp. 377-386