Sixteenth OSCE Economic and Environmental Forum - Part 1: "Maritime and inland waterways co-operation in the OSCE area: Increasing security and protecting the environment"
Vienna, 28- 29 January 2008
Session I - Security aspects related to maritime co-operation

EEF.NGO/1/08
23 January 2008

ENGLISH only

Towards a Resilient European Supply Chain

Ola Dahlman [1]

Content

Executive Summary
Global flows: key to economy and security
European Supply chain
Threats to the European Supply Chain
Increasing security of the Supply Chain
    International Initiatives
    New technologies
    A Layered Defense
Resilience: a concept to address complex socio – economical systems
Resilience: a tool to address the European Supply Chain?
How create a Resilient Supply Chain
Acknowledgements
Annex 1: Resilience analysis process

[1] This report is written when the author has a senior Fellowship at the Institute for the Protection and Security of the Citizen, EU Joint Research Centre ISPRA, Italy. The views expressed are those of the author and do not necessarily reflect those of the European Commission, the Joint Research Centre or the Institute for Protection and Security of the Citizen.

Now with OD Science Application
Fredrikshovsgatan 8 11523 Stockholm
ola.dahlman@gmail.com

Executive Summary

The new global security agenda contains a number of transnational non-military elements. We are increasingly dependent on events and resources globally and on international flows of goods, people, money and information. The European supply chain is one of those important and vulnerable global flows. In addition to being a key provider of goods and services that keep European economies and societies functioning it is an important part of the European economy in it own right and accounts for over 10% of EU gross domestic product or 1000 billion Euros yearly.

The European supply chain is exposed to a number of threats: some created by the system itself, others like large scale natural or man made disasters are coming from the outside. Terrorism has a special psychological and political dimension and the indirect effects of a terror event dwarf the direct effects.

A number of international initiatives have been taken to improve transport and supply chain security. Most of those have been initiated by the USA with the prime purpose to protect the US homeland. The interesting concept of cooperative programs between Customs and Businesses are introduced in the World Customs Organization Framework of Standards, the US C-TPAT and in the Swedish Stairsec program.

New technologies are being implemented into the supply chain in two ways. The main transport companies are developing their own technical infrastructure to meet regulations and agreements and to maintain and improve their market position. Authorities in the US have established screening equipment at border crossing to detect in particular nuclear material. Other countries might follow the US example.

To increase the security of the European supply chain requires a mixture of actions with different time and space perspectives. Such a balanced or layered defense could include actions against the general terror threat, which has a long time scale and a global dimension. Increased international cooperation and a new "mind-set" when it comes to intelligence could help interrupt specific terror operations. The vulnerability of the supply chain can be decreased by protecting the infrastructure and increasing the preparedness to handle events should they happen. Of key importance is the ability to recover without inflicting unnecessary indirect effects..

Resilience, a notion borrowed from material sciences describing the ability of a material or a system to recover after a deformation, has proven to be an interesting concept in analyzing non-linear systems with strong human interaction. Such analysis has been applied successfully to ecological systems to help understand the key factors influencing the stability of such systems. The European supply chain is a distributed socio – economical – political system with strong human interaction

by many actors able to adapt to changing conditions. It has also a number of other characteristics making it conducive to resilience analysis.

Governments certainly have the responsibility to do their outmost to prevent devastating nuclear explosions and pandemic bio-attacks, terror events that by themselves have devastating long-term global consequences. When it comes to other terror attacks, having more limited direct effects, we know that despite our very best efforts we will not prevent such events from happening. The security measures against such events have to be balanced against other priorities in our societies and against the need to maintain a cost -efficient supply chain. We must not create situations where our reaction to a terror event or the very threat of such events multiplies the effect and becomes the main difficulty. We rather have to create a resilient supply chain that may not prevent all possible events from happening but which is able to bounce back by providing reasonable options for the decision-makers on how to proceed after a terror event.

The Custom – Business partnership programs such as C-TPAT and StairSec might prove to be a most essential resilience building element. A prerequisite is that these programs are or could be made safe enough to make it most unlikely that a terror event would happen within those programs. If also political decision makers would consider those programs to provide secure and low risk transports they would be provided an appealing option of retaining or rapidly reestablish transports after an event.

Resilience is likely to come at cost also for the supply chain. More requirements on the trading partners, giving higher confidence to the authorities, might in return give additional advantages to industry. Being able to provide a resilient supply service also if and when a terror event happen is most likely to give a competitive advantage that may off set possible additional costs. Considerable resources are today devoted to protect the infrastructure of the supply chain. One might consider if some of those resources would not be better spent increasing the resilience.

Also with high ambitions to bring trade within the frames of Custom – Trade agreements there will always be a fair amount that will remain outside. In parallel with a gradual development of the Custom – Trade partnership programs it is thus essential to consider how to deal with transports outside those frames.

Issues related to the creation of a resilient European supply chain should be addressed in dialogue among the European supply chain stakeholders and decision makers

Global flows: key to economy and security

Globalization has created a mutual interdependence among all of us. We can no longer seek security or economical development through isolation but through mutual dependence. We are moving from a time focused on States, their resources and what happened locally to a time when we are dependent on events and resources globally and on international flows of goods, people, money and information. We have moved from a land to a flow based economy where a number of international non-state actors, such as large scale financial and business institutions, play important roles.

Our security used to be easily identified as a military security to be guarded by military defense and distinguished from the rest of our society. Although the ability to create and sustain a military defense has always been linked in a general way to the economic resources available to a State, the new global security agenda[2] [3] [4] contains a number of non-military elements. Most of those are transnational, presenting us with common threats; large-scale environmental degradation, proliferation of weapons of mass destruction, national terror or crime or economic and social unrest. We are mutually dependent in responding to those threats. The response is no longer a purely and easily identified military one, it is a response that integrates and depends on a number of crucial functions in our civilian society. To defend the global flows is one crucial element of this new security agenda.

What global flows are we talking about? We are crucially dependent on the flow of goods for our economy and our daily lives and this report deals with the security and resilience of the supply chain. Closely connected to the supply chain is the flow of money and numerous examples have shown how important, rapid and sometimes devastating for individual States this flow can be[5]. Other important global flows involve people, information and ideas. These flows are based on a number of networks; supply chains to provide goods, passenger transport networks to move people and international banking systems to move money. Internet and other communications systems provide rapid distribution of information and global positioning systems provide accurate location information globally. We also have a number of connected flows that are unwanted and negative: drugs, trafficking, illegal money transactions smuggling, international terror and criminality. The

[2] European Union 2003: *A Secure Europe in a Better World. European Security Strategy.* Brussels 12 December 2003.
[3] European Council 2004:*Action Plan for Civilian Aspects of European Security and Defense policy.* Brussels June 18 2004.
[4] Tomas Ries 2003: *The New Global Security Agenda.* Unpublished report Swedish Institute of International affairs, Stockholm
[5] Joseph Stiglitz 2002: *Globalization and its discontents.* Penguin Books, London

negative and positive flows may use the same networks; illegal money transfer and smuggling may use the same network infrastructure as legitimate trade and global financial transactions. Movement of people and ideas are key to global development; the purposes could also be crime and terror. The same is true for the rapid flow of information around the world. Our challenge is to maintain the security, resilience and sustainability of the positive flows and counteract the negative.

European supply chain

There is a clear historical development of the ways and means used to transport goods and people in Europe. In the early days transport was basically carried out on sea and inland waterways. The societies were adapting their infrastructure accordingly by establishing main cities by the sea or other navigable waterways. The stream engine and railways dramatically changed the means of land transport and the traffic pattern changed. The development of cars and trucks brought yet another dramatic and rapid change to the ground transport system. Air transport has dramatically improved our ability to travel rapidly over global distances. The transport system has thus over time changed most dramatically.

The transport sector is today crucial for European economy and the sector itself accounts for over 10% of the EU gross domestic product, or 1000 billion Euros, and employs some 10 million people. Within Europe 44% of the goods and 78% of the passenger traffic in 2000 were on roads.[6] The same year a similar amount of goods, or 45%, were transported by short sea line shipping and on inland waterways. Only 8 % of the goods are transported on rail and the amount transported by air is negligible. Thirty years ago, 1970, the corresponding numbers were: road 34%, shipping 41% and rail 20%. There is thus a significant increase in road transports and a corresponding decrease in transports by rail. This must not necessarily be the case as in the US the railways carry 40 % of the goods and a large European transport customer, IKEA, transports 18% of its goods by trains and is planning to increase to 40% by 2006. When discussing the European supply chain we must not only consider goods transfer within Europe but also between Europe and the rest of the world. 70% of that trade in and out of Europe is carried by ship.

Development of the transport system depends on a number of factors. It is market driven, a market that is complex with a large number of actors and customers with different demands and priorities. Industries and businesses expect a flexible, safe and speedy supply chain and have adjusted their way of doing business – “just in

[6] Towards an integrated European railway area. European Commission 2003. ISBN 92-894-4285-9

time" – to fully benefit from such a system. Efficient and quite often tailor-made supply chains have provided many companies decisive competitive advantages[7] [8].

Transport companies, which are an integral part of the supply chain, cover a broad spectrum of actors: small and large, international or national and using one or more modes of transportation. They operate independently within the frames set by available infrastructure, existing rules and regulations and market opportunities. They are competing and cooperating and they represent a multitude of priorities.

Politicians and governments have over centuries influenced the long-term development of the transport system. In the old days their navies protected the sea lines, later they built and maintain infrastructure from harbors, railways to roads and airports. We saw above that transports on roads have increased and those on rail have decrease significantly over the last decades. We see a similar trend in the development of the transport infrastructure in Europe, new motorways are being built and railways are being closed. Each year, over the last 30 years, 1200 km motorways were built and 600 km of railways have been closed[9].

With the increased global integration not least in Europe, international coordination and cooperation become more and more important. This is particularly important in increasing the security, resilience and sustainability of the supply chain at a time when the threat to our societies and our most crucial systems is increasing. In its Transport Policy paper 2010 (ref 9) the Commission notes that "a modern transport system must be sustainable from an economic and social as well as environmental viewpoint". To be sustainable it has to have a high degree of security and resilience. An expressed goal in Commission policy paper is to revitalize the railways and increase their part of the transport work. The way investments in infrastructure are made could significantly influence the security and the resilience of the European transport chain.

A global or European supply chain can be described in three layers: a logistic, a transaction and an oversight layer[10]. The logistic layer concerns the physical movement of goods or containers. This is essentially in the hands of a large number of shipping companies and involves authorities only at occasional inspections at border crossings. The transaction layer concerns the business part of the supply chain and involves transfer of orders and transport, customs and payment

[7] Ting Shen 2005:*Linking Supply Chain Practices to Operational and Financial Performances.* Supply chain 2020 Project Working Paper. MIT Center for Transportation and Logistics August 2005.
[8] Larry Lapide 2005:*The Four Habits of Highly Effective Supply Chains.* Harvard Business review Supply chain strategy. Newsletter from Harvard Business School Publishing and the MIT Center for Transportation & logistics. Article reprint No. P0505A, 2005
[9] White paper, European transport policy for 2010:time to decide. European Commission 2001. ISBN -92-894-0341-1
[10] Henry H. Willis and David S. Ortiz 2004: *Evaluating the Security of the Global Containerized Supply Chain* RAND Corporation. Technical Report ISBN o-8330-3715-3, 2004

documents. This layer also mainly involves the trading business partners. It is closely related to the physical logistic layer and provides also information to the authorities. The oversight layer is the legal and regulatory structure of the supply chain and involves EU and national authorities and international organizations such as WCO and IMO. This layer sets the frame for the supply chain and monitors the activities carried out.

Threats to the European Supply Chain

The European supply chain is exposed to a number of threats. Some of those are created by the system itself: pollution, high energy consumption, overloaded roads, and high death tolls on the roads, abandoned or low performing railways and severe shipping accidents. Others are coming from the outside. Severe threats to the European transport chain could come from large-scale natural disasters, economical failures, also on a large scale, and from terror events and the political actions taken in the aftermath of such events. Environmental concerns by politicians and the general public are limiting the establishment of new infrastructures for example trough the Alps or transportation through sensitive waterways. The system is also routinely exposed to criminal acts, such as theft and fraud, and is also routinely used as a tool to commit criminal acts: be it smuggling or trafficking. These criminal activities are of concern to transport actors, insurance companies and national and international law enforcement authorities but they are not threatening to destabilize the supply chain as a whole. The supply chain has proven resilient to these kinds of criminal activities.

The focus of this chapter is on events that may be a threat to the overall European supply chain. It will also address the sometimes devastating indirect effects caused by actions taken as a consequence of an event. Events with limited social, economic or political consequences in a European or national perspective will not be addressed. Every day crimes, accidents or economical collapse of individual companies will thus not be further discussed. The supply chain has in general proven to be resilient against such minor or local disturbances even if individuals, companies and even regions might have been hard hit by such events.

Earthquakes and heavy flooding are the kind of natural disasters that could impact in such a large scale that they could seriously affect the European supply chain. Disastrous earthquakes do occur in EU countries such as Greek and Italy. There are a number of examples of extensive and devastating flooding covering large areas in central Europe. Such natural disasters could affect large regions and would have large-scale social and economic impact also on other important functions in the societies. The resilience of the supply chain in relation to natural disasters is thus closely integrated with the resilience of the society as a whole to such events and should be addressed in that context.

The supply chain is closely related to European and world economies. This is a mutual relation: if the supply chain fails the economy will suffer and if the economy is in trouble these difficulties will be shared by the supply chain. This applies throughout the supply chain and the economy from individual companies to the European and global levels. The scale of the disturbances and of the effects relates to the size of the supply chain and the economy involved. The resilience to economic disturbances is likely to differ at different levels of the European supply chain. Limited parts of the chain and related economy could fail but the overall supply chain at European and national levels might still be resilient. A large-scale economic collapse on a European or national level might on the other hand have the most severe consequences for the supply chain. A further discussion of the resilience of the European supply chain in relation to the economy would properly fit into a discussion of the resilience of European economy.

The 9/11 event was a most spectacular terror event using an element of the transport system as a tool. It was turned into a political event as the start of the war on terror with global consequences. Europe has for decades been subject to serious terror events, two recent tragic events were against trains in Madrid and the subway in London. Terror is a serious threat also to the European supply chain, even if no event so far has been targeting the supply chain.

Terrorists can impact the supply chain in different ways. The transport system can be used to forward material, including material and weapons of mass destruction, into Europe from any part of the world. The large number of containers constantly traveling around the world could be a vehicle for such transfer[11]. A container can also in it self be a weapon. A "cruise missile", that can be launched from any point on the globe and be directed to its target with high precision. The container can be loaded with high explosives, in large quantities – tens of tons. Nuclear and highly toxic chemical material might be added to increase not least the psychological effects. A container could also hold a nuclear explosive device. Terrorists might also hijack any of the many transports of dangerous goods that are routinely passing all over Europe, at sea and on road and rail. This could be a gas or fuel tanker or a truck loaded with industrial chemicals such as chlorine. Terrorists could target the supply chain itself by setting of the event in a harbor, on a ship or train or in a transport hub. It could also target other objects of great economic, political or social value in Europe.

A nuclear explosion would, by itself, have devastating large scale and lasting effects on a global scale. The direct impact of a terror attack using conventional explosives may be substantial and locally devastating. The indirect effects of a

[11] Ola Dahlman, Jenifer Mackby, Bernard Sitt, Andre Poucet, Arend Meerburg, Bernard Massinon, Edward Ifft, Masahiko Asada and Ralph Alewine, 2005*: Container Security, A proposal for a Comprehensive Code of conduct.* Center for Technology and National Security Policy, National Defense University, Washington DC, USA. January 2005

terrorist event dwarf the direct effects[12]. A reported estimate by the Center for Homeland Security and Defense shows that a terrorist attack on a major port could result in losses of $1.5 – 2.7 billion per day for the few first days, $5 billion a day for the next two weeks, and could then rise exponentially thereafter[13]. The response and recovery after a terrorist event differ dramatically from that of an accident or a natural hazard. Uncertainty on what happened and what might be a next event will shape the follow up. To the more operational response and recovery operation will be added a political dimension. Political leaders will intervene and the actions will get fairly unpredictable. Would it take one blown- up container to severely harm world trade and economy or would it take five or would one truck with dangerous goods hijacked and blown-up down town a big city do the job? After such events what would be the alternatives for the political decision makers: to stop cargo flow for days, weeks or longer with huge consequences or letting cargo continue to move at the price of further risks?

Increasing security of the supply chain

To increase the security of the European supply chain we must make reasonable efforts to prevent terror event from happening and to protect the infrastructure[14]. How much is "reasonable"? Views certainly may differ among the stakeholders. We know that there is no way to create a cost- efficient supply system that is fully protected from terror attacks. We have to find a balanced mix of actions, nationally and internationally, that provide a level of security acceptable to all at a price the supply chain can bear.

International Initiative

Over the last few years a number of international initiatives have been taken to improve transport security[15]. These initiatives are either regulatory or cooperative between authorities and business. Most of the regulatory initiatives to guard the supply chain against terror attacks have been taken by the USA. The prime purpose has been to protect the US homeland by moving the first line of response across the ocean. A number of measures have been implemented on US initiative related to container transport: The Container Security Initiative (CSI) is a set of bilateral agreements with the US. It provides for a team of US officers to be deployed to

[12] Michael Wolfe, 2004: *Impacts and dynamics of Supply chain security* The Monitor vol10 no 2, Summer 2004

[13] Lord Jopling (special rapporteur) 2005: *Chemical, biological, radiological or nuclear detection: a Technology overview* 167 CDS 05 E NATO Parliamentary Assembly 2005 Annual Session .

[14] European Commission 2004*:Critical Infrastructure Protection in the fight against terrorism.* Communication from the Commission to the Council and the European Parliament COM (2004) 702 final Brussels 20.10.2004

[15] Werner Krudewagen Siemens SBT 2005: *Transportation Security and Supply Chain Integrity:* EAPC/PfP Workshop , Zurich September 2005.

each cooperating foreign port to identify containers that may pose a threat and have them checked before they are shipped to the US. Cooperating States could also have their officers at US ports in a reciprocal manner. As of December 2005 CSI covered 41 ports in 24 countries[16]. The Automated Manifest System requires that US custom receives the shipping manifest information 24 hours before a container is loaded for a harbor in the US. The Megaport Initiative is again a set of bilateral agreements by which the US establish passive radiation detection equipment in selected ports that are part of the CSI. The equipment is manufactured in US and is operated by the host country. Such systems are presently being established worldwide. The Proliferation Security Initiative (PSI) is focused on pre-emptive interdiction that would allow ships, aircrafts or vehicles suspected of carrying WMD related material to be detained and searched.

International Maritime Organization (IMO) has established the ISPS code demanding security certification of ships and ports[17]. The World Customs Organization in June 2005 adopted a Framework of Standards to secure and facilitate Global Trade[18]. This Framework has two pillars, one regulatory, custom-to-custom, and one customs-to-business partnership. This cooperative project with business introduces the notion of Authorized Economic Operators as a certified partner of the supply chain. A similar concept is the basis for the Customs Trade Partnership Against Terrorism (C-TPAT). This is a joint US government – business cooperative initiative to secure the transport chain through "trusted shippers", that are certified to follow agreed security guidelines[19]. More than 8800 businesses have by March 2005 signed up to C-TPAT[20]. According to US Customs commissioner Robert Bonner, C-TPAT now covers 40% by value of the containerized goods imported into the US[21]. Mr. Bonner announced during a January 2005 Customs Trade Symposium in Washington DC that he was ready to take the Customs-Trade Partnership Against Terrorism (C-TPAT) program to the next level, which he called "C-TPAT Plus". C-TPAT Plus would provide "no inspection upon arrival - immediate release" for low-risk shippers using technology that can detect and record whether tampering has occurred with a container seal after being affixed at

[16] US Customs and Border Protection 2005: CSI Fact Sheet, December 2005. www.cbp.gov/xp/cgov/border-security/international-activities/csi

[17] International Maritime Organization (IMO), 2002: *International Ship and Port Facility Security Code (ISPS Code)*, IMO December 2002 http://www.imo.org/home.asp

[18] World Customs Organization 2005: *Framework of Standards to secure and facilitate Global Trade*. www.wcoomd.org

[19] US Customs and Border Protection: *Partnership to Secure the Supply Chain: Customs – Trade Partnership against Terrorism.* http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/

[20] Robert C. Bonner 2005:*Message from the Commissioner Announcing C-TPAT Importer Security Criteria;* US Customs and Border Protection March 25, 2005. http://www.cbp.gov/xp/cgov/import/commercial_enforcement/ctpat/criteria_imprters/co

[21] MIT Center for Transportation & Logistics 2005: *Supply Chain Security Goes Global.* http://ctl.mit.edu/metadot/index.pl?id=4510

the point of origin[22]. Meanwhile the use of smart containers was recommended as C-TPAT best practice.

The Swedish custom has established a similar Custom – Trade cooperation called StairSec build on the accreditation of economic operators[23]. StairSec and C-TPAT are compatible to each other and efforts are underway in Europe to develop a framework for international accreditations. By November 2005 some 150 companies have signed up to StairSec and some 80% of the direct export to the US is under StairSec[24]. It should be noted, however, that only a small part of Swedish export to the US goes directly, most goes through some large continental harbor.

To be part of C-TPAT or StarSec a business partner must fulfill specific criteria for security and traceability of goods and transactions. The company must also in general be well recognized as a serious actor in the supply chain. In return, certified companies enjoy a smooth and speedy handling of custom procedures. We will below discuss such customs – business agreements further as important elements in a resilient supply chain.

New technology to enhance security

New technology is gradually being implemented throughout the supply chain to enhance security[25]. This applies to securing the integrity and the tracking of the container in transit and improving the checking of container at entry/exit points. It also applies to securing the information systems used for supply chain transactions. A lot of the development and implementation of new technology is carried out by commercial companies[26].

A trustworthy seal is a crucial tool to assure the integrity of a container. Most of the seals used so far are quite simple mechanical seals that are easy to forge and applied for liability rather than security. There is at present a rapid development of low cost radio frequency identification devices (RFIDs) that could be embedded into seal to improve security. RFID would also facilitate the traceability of containers. A host of RFID devices for containers, mainly e-seals are already on the

[22] **A**.T. Kearney: *'Smart Box' RFID Technology urged by U.S. Customs for Security also provides Economic Value for Global Shippers* – Savi January 2005. http://www.savi.com/news/2005/2005.01.30.shtml
[23] Swedish Customs 2003:*White Paper on Accreditation of Operators and Supply Chain Security (StarSec)* www.tullverket.se
[24] Christopher Kristensson, security expert, Swedish Customs Personal communication November 2005.
[25] Bahar Barami: 2004: *Embedded Technologies to secure the Supply chain from End-to-End.* Conference paper September 24, 2004,Volpe Center, SOLE 2004 Norfolk VA
[26] IBM and Maersk Logistics 2005: *IBM and Maersk Logistics provide real-time cargo monitoring for global supply chain optimization:*20 September 2005 *http://www.maersklogistics.com/sw37403.asp*

market in the US[27] [28] [29] [30] [31]. JRC has demonstrated the feasibility of using RFIDs to trace livestock in Europe.

In 2004, the Homeland Security Advanced Research Projects Agency (HSARPA) launched a series of projects on Advanced Container Security Devices (ACSD)[32] and specified system functions and minimum requirements for such "smart containers". Meanwhile, different systems including inclusion sensors and/or location and tracking devices have been proposed on the market. Smart containers could also have built in sensors to detect people and specific materials such as explosives, drugs and radioactive material. According to the study made by the Homeland Security Research Corporation, dozens of companies[33] are tempting to market smart container solutions and the market is expected to grow 60 fold over 7 years from $70 million in 2006 to $4 billion by 2012 [34].

Radiation Portal Monitors, RPM, similar to those used in the Megaport Initiative, are also deployed in US ports and border crossings to check incoming containers for nuclear material[35]. In 2006 more than 400 such RPM were deployed in 22 major ports scanning 7 million incoming containers every year (see ref 33). The RPM equipment has two severe limitations: a large number of false alarms as it can not identify the exact origin of the radiation and no ability to detect shielded material or material with low level of radiation such as uranium -235. Research is going on to develop detectors that can identify the sources from neutron and gamma ray observations. Work is also going on to develop active neutron interrogation systems to detect also shielded and low radiation nuclear material. US has also developed and deployed active large-scale imaging systems using X-rays or gamma rays. 166 such systems are currently deployed, each costing about $1 million.

In which way will this rapid technological development be implemented into the supply chain? The big transport companies, none of them American, will most likely take the lead in implementing new technology. The large shipping companies are likely to develop their own standards and procedures, consistent with US and other national and international requirements including WCO and IMO standards. The standards, procedures and technical equipment will be coordinated with those of the major port terminals, which in many cases are operated by the same company. Smaller transport companies must most likely adjust to the standards set by the larger companies to be interoperable. Larger shipping companies will

[27] http://www.alientechnology.com/markets/transportation.php
[28] http://www.securtrack.com/
[29] http://www.higtek.com/
[30] http://www.savi.com/index.shtml
[31] http://www.transcore.com/
[32] http://www.hsarpabaa.com/Solicitations/CSD-RFI-ver-8.pdf
[33] http://www.gesecurity.com/portal/beans/mdme_presentation/jsp/Download.jsp?ID=1879&DID=15808
[34] http://www.hsrc.biz/uploads/HSRC%20Newsletter%203s.pdf
[35] http://www.saic.com/products/security/gr-500

develop their own technical infrastructure and cooperate with IT- and security industries to get equipment and services. The resent agreement between IBM and Maersk Logistics (ref 26) is an example of such a co-operation.

The speed with which new technology will be implemented will depend on a number of factors. One is international or national regulations and standards. An even more important factor will be the further development of the Customs – business agreements towards greater security and corresponding advantages for the trading part. Enhancing security by additional technology is likely to give a competitive edge as long as it can be done at a cost the market is prepared to pay.

When it comes to actions by governments and national authorities, the US has so far focused on increasing its own security and may well proceed down that path. There might also be a more general concern to secure the supply chain globally, realizing that any serious event anywhere will have global consequences. Governments and authorities in Europe and elsewhere might follow the US example to guard against the transfer of nuclear material by installing nuclear monitoring portals and active neutron interrogation systems at ports and other strategic locations. They might also increase container screening at those locations using x-rays or gamma-rays systems similar to those already deployed in US harbors. Europe has a particular security problem with the extensive European land and inland water way transports. Further development of information and tracking systems might contribute to address that problem.

A Layered Defense

To reduce the risk that terror attacks might cripple the transport system we have to think and act in a number of scales both in time and space. Such a layered defense approach is often used in assessing the defense of military objects and has also been used to address the nuclear threat[36]. A layered defense can be described by a number of elements. The challenge is to balance these actions with different time and space perspectives against each other to obtain a cost-effective combination of actions. We have to look at the whole time span from long term prevention and preparedness to the handling of a specific terror event and the recovery from such an event.

The terrorist threat against the supply chain is part of the more general terror threat. To understand the generics of this threat is a basis for any defense or protection activities. This includes understanding the possible actors, their motives and driving forces and their most likely targets. It further includes the identification of possible breeding grounds for terror. Those could be social, ethnic, political or

[36] Matthew Bunn 2005: *Designing a Multi-layered Defense Against Nuclear Terror*. Presentation for Homeland Security Advisory Council Task Force on Weapons of Mass Effect June 13, 2005 John F. Kennedy School of Government. Harvard University. www.managingtheatom.org

religious. They could also be essentially criminal. We have learned that those breeding grounds are not only in failed States far away, they are also in our own backyards. To cope with the long term terror threats the world has to develop a strategy to reduce and eventually eliminate these breeding grounds and create social and economic conditions that reduce the likelihood that terrorist activities develop. This most essential element to eventually root out terror has a long time scale and a global dimension.

Another element is to identify specific threats, terror groups and their like targets and the methods of terror to be used to attack the European supply chain. To detect activities related to the planning or conduct of a terror operation is essentially intelligence work. This new challenge for the intelligence community is quite different than their traditional military activities. It requires a new mind-set and a more intense global cooperation[37]. Open-source data and "soft" information on social and ethic issues are important. Threat scenarios are essential tools for directing the intelligence activities both when it comes to issues, geographical areas and mind-set. Successful identification at an early stage of terror groups could lead to the discovery and interruption of an operation before it has been launched. Short term intelligence information can also be used to increase readiness and provide warnings to authorities, transport operators and the public.

To identify the vulnerability of the European supply chain to the perceived threats and explore ways to reduce that vulnerability is an essential precursory measure. Dependent on the severity of the threats you may choose to act in different ways: Some not too serious threats you may not guard against – you absorb them when they happen and continue. Other events you guard against, given that it is cost-effective. Serious events, especially those involving weapons or materials of mass destruction, you want to guard against also at a very high cost.

The vulnerability of the supply chain can be reduced by a wide range of activities taken by several actors in different timeframes and over smaller or larger areas. These actions, which will be discussed further below, include: physical protection of infrastructure, inspection, checks and tracing of transports, in particular dangerous goods and material that might be used for mass destruction. They further include the introduction of new procedures and technologies and security checking of the personnel in the transport system. These actions should be balanced among the stakeholders in a cost – effective way.

Our ability to handle a specific event depends on our level of preparedness and the size and severity of the event. Minor events, not having a political dimension, might be handled by the transport actors, authorities and rescue services at local or regional level. Larger events, especially those including weapons of mass destruction, could by themselves have such large scale consequences that actions might be needed at a national or even international level to bring the emergency

[37] B. Muller-Wille 2003: *Building a European Intelligence Community in Response to Terrorism.* European Security Review No 22 April 2003

situation under control. This might also include actions to prevent social unrest and panic.

Of utmost importance is our ability to recover. Recovery after a terror attack has two dimensions: a technical/ operational and a political. The technical/operational dimension is about taking all the practical steps needed to restore the system. It would include recovery at the site of the event and the use of back-up procedures and facilities. This part is a fairly straightforward operation, very similar to the recovery operation after a natural disaster. The political dimension of the recovery process is more complicated. To reduce the severe indirect effects of a terror event it is crucial to make the supply chain resilient by giving political decisions makers reasonable options to bring the supply chain and the society back to normal conditions.

Resilience: a concept to address complex socio – economical systems

Resilience is a notion borrowed from material sciences and describes the ability of a material to recover its shape after a deformation. Many technical systems behave in a linear way: with a direct relation between the size of a disturbance and the effect on the system. A linear system goes back to its equilibrium when the disturbance is gone. This is not true for a system with complex non-linear relations between its elements. Such systems might be facing discontinuities and uncertainties that make them totally fail if a disturbance exceeds a critical threshold. For such systems it is necessary to abandon the perception of steady state. Instead the system must be analyzed in terms of its ability to adapt to changes and recover from disturbances while providing options for future developments. Resilient building aims at increasing the range of surprises that a system can cope with. It should prevent the system from moving into undesired system configurations in the face of external stresses and disturbances. Building resilience requires understanding of the complex interaction among the different components and actors in a society and over the scales in time and space relevant for the system. Biological, social, commercial and political systems very often behave in this way. They are complex, adaptive and generally dynamic. They are also nonlinear and capable to self organize to sustain their existence but also unpredictable and may survive unexpected events but also fail completely.

The resilience concept has over the last few decades been introduced to describe complex systems, especially systems where human interaction has a significant influence. It was introduced into the analysis of ecological systems by *Holling* in 1973[38] and a number of interesting studies of such systems have since then been

[38] C.S. Holling 1973: *Resilience and stability of ecological systems.* Annu. Rev. Ecol. Syst. 4; 1 – 23

reported. A few references are given here[39][40] [41] [42] [43] and in the text that follows. A number of studies have also recently been published that address resilience in socio – economical systems including the supply chain[44] [45] [46] [47] [48] [49] and in the socio – political environments. [50]

Resilience has been described in terms of a number of defining characteristics[51]:

- The amount of change a system can undergo and still be in the same configuration - retain the same controls on functions and structure. A more resilient system can absorb larger shocks without changing in a fundamental way.
- The degree to which the system is capable of self-organization
- The degree to which the system expresses capacity for learning and adaptation.

---

[39] C Folke, S. Carpenter, T. Elmqvist, L.Gunderson, C.S. Holling, B. Walker, J.Bengtsson, F.Berkes, j. Colding, K. Danell, M. Falkenmark, F. Moberg, L. Gordon, R. Kaspersson, N. Kautsky, A. Kinzig, S.A. Levin, k.-g Maler, L. Ohlsson, P. Ohlsson, E. Ostrom, W. Reid J.Rockstrom, H. Savenije and U. Svedin 2002: *Resilience and Sustainable Development: Building Adaptive Capacity in a World of Transformations.* ICSU Series on Science for Sustainable Development No 3. The Swedish Environmental Advisory Council 2002:1 Ministry of the Environment, Stockholm.

[40] B.Walker, C.S. Holling, S.R. Carpenter and A. Kinzig 2004: *Resilience, Adaptability and Transformability in Social-ecological Systems.*Ecology and Society 9(2): 5 http://www.ecologyandsociety.org/vol9/iss2/art5/

[41] C Folke, S.Carpenter, B. Walker, M. Scheffer, T.Elmqvist, L. Gunderson and C.S.Holling 2004: *Regime Shifts, Resilience , and Biodiversity in Ecosystem Management.* Annu.rev. Evol Syst 2004 35: 557 - 81

[42] S.Carpenter, W. Brock and P. Hanson 1999: *Ecological and social dynamics in simple models of ecosystem management* Conservation Ecology 3(2): 4 http://www.consecol.org/vol3/iss2/art4/ .

[43] B. Walker and J.A.Meyers 2004: *Thresholds in Ecological and Social-Ecological Systems: a Developing Database.*Ecology and Society 9(2):3 http://www.ecologyandsociety.org/vol9/iss2/art3/

[44] James B. Rice, Jr., Frederico Caniato: *Building a Secure and Resilient Supply Network,* Supply Management review /2003/09/01.

[45] Yossi Sheffi: *The Resilient Enterprise,* MIT Press , October 1, 2005

[46] Yossi Sheffi: *Building a resilient Supply Chain,*Harward Business review Volume 1 Number 8, October 2005.

[47] Jan-Peter Voss, 2004 *The Governance of transformation in Utility Systems: Challenge and Practice.* In Jacob, Binder and Wiezorek (ed): Governance for Industry Transformation. Proceedings of the Berlin Conference on the Human Dimension of Global Environmental Change

[48] Joseph Fiksel, 2005: *In Search of the Resilient Enterprise.* Center for Resilience at the Ohio State University. Presentation October 14,2005

[49] J.M. Anderies, M.A. Janssen and E.Ostrom 2004: *A Framework to Analyze the Robustness of Social-ecological Systems from an Institutional Perspective.*Ecology and Society 9(1): 18 http://www.ecologyandsociety.org/vol9/iss1/art18

[50] C.S. Holling 2004: *From Complex Regions to Complex Worlds.* Ecology and Society . http://www.ecologyandsociety.org/vol9/iss1/art11

[51] B. Walker, S.Carpenter, J. Anderies, N. Abel, G.Cumming, M.Janssen, L.lebel, J. Norberg, G.D. Peterson and R. Pritchard 2002: *Resilience Management in Social – ecological Systems: a Working Hypotehesis for a Participatory Approach..*Conservation Ecology 6(1):14 http://www.consecol.org/vol6/iss1/art14

Resilience must be considered in a specific context: "what to what"[52]. This means that we have to define what functions or elements of a system are resilient to what changes. If a system is composed of elements forming different system levels, it can be resilient at some of the levels but not necessarily at others. Interesting questions discussed by Croxton [53] are; How can an enterprise be resilient without having a resilient supply chain? If each enterprise is resilient – is the supply chain resilient? A large scale system, such as the European supply chain, could be overall resilient even if a number of transport companies fail. The European supply chain could, on the other hand, fail due to a large scale political or economical crisis even if the individual transport actors are intact.

How would we then increase the resilience of a system? Diversity plays a significant role in sustaining the resilience of ecosystems. Loss of functional groups will severely affect the capacity of an ecosystem to recover after a disturbance. Flexible social networks and organizations that proceed through learning by doing are better adapted for long-term survival than rigid social systems that have prescriptions for resource use.

Fiksel[54] identified a number of system characteristics contributing to resilience:

- Diversity and flexibility: where a number of forms and behaviors exist and the system can move easily between them.
- Efficiency: in the sense that the system operates with moderate consumption of resources.
- Adaptability: giving the system the ability to change in response to new pressures.
- Cohesion: providing unifying forces or linkages between the elements of the system.

Resilience is also dependent on the initial security of the system and its ability to resist disturbances. It is even more dependent on the ability of the system to renew and reorganize itself following a large-scale disturbance and provide options for future actions after the disturbance. Robustness will thus be achieved through resilience rather than resistance. Systems that use rigid and centralized control mechanisms are generally less resilient than decentralized systems that are flexible and open to learning. When building resilience it is important to attend to slowly-changing, fundamental parameters of a system, such as the infrastructure of the European transport system. Properly chosen such parameters could create diversity and capability for future development.

---

[52] Steve Carpenter, Brian Walker, J.Marty Anderies and Nick Abel2001: *From Metaphor to Measurement: Resilience of What to What?* Ecosystems (2001) 4:765 – 781 Springer Verlag.
[53] Keely L.Croxton, The Resilient Supply Chain, Fisher College of Business, The Ohio State University.
[54] Joseph Fiksel: Designing Resilient, Sustainable Systems. Environmental Science &. Technology vol 37 No 23 2003, pp 5330 - 5339

Human interventions are crucial in a social – economical- political system, such as the supply chain. Such interventions are far from coherent as there are many stakeholders holding different agenda. The human behavior in and after a crisis situation are also unpredictable. To create resilience it is therefore essential to design a system in a way that facilitates human action conducive to bringing back the system to operation after a major disturbance. An important element is to present decision makers reasonable options for future actions. A resilient system should also, as far as possible, be able to cope with irrational actions by individual stakeholders.

How would we know if a system is resilient, can resilience of complex systems like the supply chain be measured or modeled? As the human influence in socio-economic – political systems are most significant it is not possible to measure or model the resilience of such a system in a conventional way. Instead of predictive modeling we have to use exploratory scenario building among the stakeholders to try to understand ways and means to influence resilience of a particular system to specific disturbances. Experience from the environmental area has shown that it is difficult to accurately predict a priori if a system is resilient to a given disturbance. Efforts have to be concentrated on understanding and improving on the different factors that enhance resilience. Annex 1 shows a process that has been developed to address resilience through a structured dialogue among stakeholders.

Resilience has a cost[55]. To increase resilience is different from improving the performance of a system in times of growth. Just as there are costs and benefits involved in diversifying an investment portfolio there are trade-offs and synergies between production and resilience in any socio – economical system. Resilience building is focused on the behavior of a system rather than just the output. If we can identify the consequences and likelihood of a particular system change, we may determine how much is worth investing in resilience against that disturbance. Tang[56] gives a number of examples of companies losing substantial amount of money and markets due to disruption of the supply chain. A famous example is when Ericsson lost 400 million Euros due to fire in a supplier's semiconductor plant whereas Nokia managed to adjust to the same disruption speedily and gained a competitive advantage. As nobody gets credit for fixing problems that never happened, businesses do not generally pay enough attention to improve resilience of their systems, including their supply chains[57]. It may be even harder to justify investments in general resilience. What about the next unexpected and novel shock? How can we assess the appropriate levels of investments in resilience in such a broad system as the European supply chain?

[55] Brian Walker 2005: *A Resilience Approach to Sustainable Development* (Unpublished report) CSIRO, Canberra Australia

[56] Christopher S. Tang. Robust Strategies for Mitigating Supply Chain Disruptions, August 29,2005, UCLA Anderson School, Los Angeles, CA 90095 USA

[57] N.P. Repenning and J.D. Sterman 2001: *Nobody Ever Gets Credit for Fixing Problems that never Happened. Creating and Sustaining Process Improvements.* California Management Review vol 43 No 4 Summer 2001.

Resilience is, however, not necessarily desirable. As we discussed earlier some global flows and supply systems are not desirable. These might include illegal networks for smuggling drugs, people and weapons. Our law enforcement authorities may today find those supply networks too resilient and want to explore ways to reduce their resilience.

Resilience a tool to address the European Supply chain?

What are the basic characteristics of the European supply chain that makes it fit the resilience analysis concept? The European and the global supply chains are most complex, where different subsystems and stakeholders act and interact in a fairly decentralized way, guided by some general rules and regulations. The supply chain uses different modes of transportation, rail, road, sea and air. In each mode there is a mixture of different technical and operational concepts and actors. The system has a number of diving forces: the transport actors and their customers, the politicians and the citizen of our societies and the technological development. The different actors have different agenda and priorities. The system has a built in ability to self-organize and has proven able to adapt to greatly changing conditions and demands.

The historical development has also clearly shown that the system has changed over time. It has moved from one stable system configuration to another – from sea to sea plus rail and now essentially sea and road. The system has remained in a particular state for a fairly long time and the shifts from one state to another have been gradual although at times quite rapid. The system has managed these shifts maintaining its functionality. This is most likely due to the multitude of actors and market forces that have created flexibility and adaptation. The shifts have not been the same in all parts of the world as illustrated by the differences in rail transport between Europe and the USA.

The European supply chain has a long term component in its infrastructure – roads, railways, harbors and airports. These are elements of the system that can be changed only slowly and at great cost. The way we utilize that infrastructure can be changed more rapidly and at lower cost. There could be new cars, trucks, trains or command and control systems to improve the throughput, the security or the safety. Actors may change their pattern of using the system or part thereof with short notice and without any coordination. The European supply chain thus contains components that can be varied only slowly and at great cost and others that can be changed more rapidly and at lower cost and is in this regard similar to social-environmental systems and most other social – economic – political systems. The transport system thus shows a number of characteristics indicating that it is a system that can be addressed in terms of resilience.

How to create also a resilient supply chain.

Large efforts are under way, particularly in the US but also increasingly in Europe and elsewhere, to increase security to prevent a terror event. Governments certainly have the responsibility to do their outmost to prevent devastating nuclear explosions and pandemic bio-attacks, terror events that by themselves have devastating long term global consequences. When it comes to other terror attacks, having more limited direct effects, we know that despite our very best efforts we will not prevent such events from happening. The security measures against such events have to be balanced against other priorities in our societies. They also have to be balanced against the need to maintain a cost -efficient supply chain. We must not aim at increasing security in such a way that these measures by themselves create key obstacles for world trade, economy and prosperity. There are also legal, social and ethical dimensions: we must fight terror with the means available to democratic societies and firmly established within our legal systems but not, in the defense of our societies, give up the fundamental values on which those societies are built and which we try so hard to protect.

While never accepting terror, we have to balance our actions to cope with the threat and the consequences in ways similar to how we handle other threats to our societies. We must not create situations where our reaction to a terror event or the very threat of such events multiplies the effect of an event and becomes the main difficulty. We rather have to create a resilient supply chain that may not prevent all possible events from happening but which is able to bounce back and recover in a speedy and smooth way. Europe, the US and the rest of the world have a common challenge to create a resilient global supply chain, as a terror attack in any part of the world will have global effects. A chain that on the one hand reduces the risk of a terror attack and on the other, and more importantly, limits the consequences of an attack and facilitates the speedy recovery of the supply chain operation. To restore the supply chain after an event is not only a question of bringing the technical and operational components back to work but also to re-establish confidence in the global trade system. This involves difficult political decisions and a key element of a resilient supply chain is to present reasonable options for the decision-makers on how to proceed after a terror event. This is crucial not only for transport actors and industry dependent on an efficient supply chain but also for States and societies in general.

Let us see what might happen after a major terror attack against the supply chain. This could be an explosion of a container in a harbor or a coordinated attack on several harbors or transport hubs. It could be a purely conventional explosion or it could have nuclear or toxic substances added to increase the psychological effect. The effects of such an attack will be global and affect not only transport actors but also businesses, economy and the public in general. In addition to handling the local effects of an attack, governments all over the world and the EU have to handle the political, social and economical effects. Political decision makers would feel the pressure to stop or severely limit the flow of goods in the supply chain until the event and the circumstances have been fully clarified. To fully understand the

situation will be a prerequisite for taking the necessary decisions to re-establish transport and trade. A key question here is traceability. This relates to the containers that were part of the attack. It also relates to containers that with high probability can be considered as secure. If politicians are not provided reasonable options they are likely to overreact. The consequences of such political reactions would be more far reaching than the direct effect of the event itself. If stopped or severely restricted, it might take long time to reach agreement to allow the supply chain to resume. Many European industries are critically dependent on “just in time” delivery for their production. Disturbances in the supply chain will have severe economic and market consequences for most production companies. There will also be social consequences as also shorter breaks in the supply chain might force companies to close production and send people home. Some companies might be more resilient than others but a major disturbance in the global supply chain is likely to affect many companies severely. Following a terror event it is also likely that more strict security regulations will be implemented that could slow down global trade for a long period and lead to a lasting global recession.

One of the most significant characteristics of a resilient system is to provide options on how to bounce back and recover after an event. A resilient supply chain must contain elements that give decision makers options for actions after an event that do not magnify but rather limit and mitigate the negative effects. Such elements must be identified and built into the supply chain prior to the events. Such resilience building elements in the supply chain are not necessarily identical to those giving increased protection to the supply chain infrastructure. As many crucial decisions on actions after a terror event are political or have a political dimension they contain a strong element of intangibles: fear, trust and confidence. The supply chain actors and the decision makers, including the political level, thus have to engage in a dialogue to identify the resilience building elements that will make it possible to retain at least the most essential parts of a supply chain in the face of a terror attack or a threat of such an attack.

How can we build resilience into the supply chain? Can we identify some elements to be considered by the stakeholders and the decision makers? The Custom – Business partnership programs such as C-TPAT and StairSec might prove to become a most essential resilience-building element. A prerequisite is that these programs are or could be made safe enough to make it most unlikely that a terror event would happen within those programs. If also political decision makers would consider those programs to provide secure and low risk transports, they would provide an appealing option of retaining or rapidly reestablish such transports after an event without additional restrictions.

C-TPAT and StarSec were not established with this specific purpose in mind. A key question is: are they secure enough to make a terror event most unlikely and are decision makers confident that they are? It has not been tested and it might not even have been seriously analyzed. Let us look at some of the most crucial components. To secure the initial stuffing of a container and to ascertain that the bill of lading is

consistent with the actual content of the container is the most crucial step to prevent a container being a terror weapon. If this part is not secure, no action further down the transport chain, short of an adequate screening or inspection, can re-establish security. Measures to ascertain the security of the environment in which containers are loaded and the security clearance of the people involved are part of the certification procedures of C-TPAT and StairSec. The next crucial step is to preserve the integrity of the information related to the different stages of a transport chain from loading to unloading. Key information relates to the integrity of the container box itself during the transport to prove that the box has remained closed and sealed and that there has been no intrusion into the container. As discussed above, new technology is providing high security smart boxes but few such high security containers are as yet operational. Another piece of information relates to the route the container has taken and here the most vulnerable part is the transfer by trucks or small inland barges. The container could be in the hands of one single person for days passing through large parts of Europe. This may offer ample opportunities for interacting with or exchanging a container. Tracking information might prove essential to ascertain the security of such transports.

An important element of the certification process should be for the authorities to ascertain that an industry within a Custom – Trade program has the necessary procedures in place to obtain and secure the integrity of information needed. The actual monitoring of individual transports should then rest with the actual company and authorities should monitor that the companies are able to fulfill this task. It has been suggested[58] that procedures similar to those used in Nuclear Safeguards[59] could be followed where the nuclear material is by and large monitored by the operators of nuclear plants and the authorities, IAEA and Euroatom, monitor that the operators have the necessary procedures in place.

To explore if Custom – Trade programs such as C-TPAT and StairSec are or could be developed to be an essential resilience building element of the European and the global supply chain a dialogue has to be established among the stakeholders and decision makers. Such a dialogue should establish if the present arrangements provide the necessary confidence to all concerned or if additional measures are needed. If additional measures are considered necessary it should also be identified if the transport industry might be granted additional benefits to offset the additional costs. A dialogue should also increase preparedness by exploring ways to handle possible future terror attacks. The use of scenarios and other elements of the resilience analysis scheme presented in Annex 1 might facilitate such a dialogue.

Although an increasing number of companies participate in C-TPAT and StairSec, only a minor part of global trade is presently conducted under any Custom – Trade agreement. To become a key element of a resilient supply chain it is

[58] A. Poucet 2005; *Personal communication* IPSC, EU Joint Research Center, Ispra Italy
[59] IAEA 2005: *The Safeguards System of the International Atomic Energy Agency*.http://www.iaea.org/programmes/safeguards/

important that such programs be implemented to cover the main global trading partners and States, including Europe and Asia. The aim should be that such programs cover all the goods that are essential to our societies.

Also with high ambitions to bring trade within the frames of Custom – Trade agreements there will always be a fair amount that will remain outside. In parallel with a gradual development of the Custom – Trade partnership programs it is thus essential to consider how to deal with transports outside those frames. How do we handle containers where there is no reliable verification of the loading or of the paths they have taken? Will there be checkpoints where such containers are checked before allowed proceeding into the international transport flow? Will unchecked containers be kept physically separate from the containers in the partnership programs? Will main harbor and transport companies eventually reject containers that are not part of a certified partnership program? These are issues that are of interest and importance not only to those companies that for various reasons operate outside the frames of partnership programs but also to actors within those programs.

As noted earlier, resilience normally comes at a cost, and this is likely to be true also for the supply chain. Where would you find the resources to create resilience against something that may not happen if the consequences when it happens are most severe? Could you turn the table and gain competitive advantages by providing a resilient service? The basic idea behind the Customs – Trade programs is that the additional cost for increased security should be offset during normal operations by a preferred treatment. More requirements on the trading partners, giving higher confidence to the authorities, might in return give additional advantages to industry when it comes to red tape and formalities at border crossings. Being able to provide a resilient supply service also if and when a terror event happens is also most likely to give a competitive advantage that may offset possible additional costs. Considerable resources are today devoted to protecting the infrastructure of the supply chain. One might consider if some of those resources would not be better spent increasing the resilience. These are other issues that should be discussed between the supply chain stakeholders and decision makers.

Acknowledgements

This report is written when during my senior Fellowship at the Institute for the Protection and Security of the Citizen, EU Joint Research Centre, ISPRA Italy. I appreciate the kind support given by the Institute and its director Jean Marie Cadiou. I had the pleasure of working in the Unit of Dr Andre Poucet and I am thankful to him and his staff for their support. I have benefited greatly from

interesting discussions with Dr Poucet and Dr Jean-Pierre Nordvik and from their valuable advice. Dr Brian Walker CSIRO, Canberra, Australia has greatly assisted me in understanding the concept of resilience by providing interesting reports and valuable suggestions.

Annex 1

Resilience analysis process

Systems, such as the European Supply Chain, containing a substantial social element, are strongly related to values and perceptions, which can vary significantly among and within the groups of actors involved. Resilience is such systems can not be measured but has to be addressed in an orderly process among stakeholders. A process carried out. A structured dialogue supported by scenario analysis has proved successful in integrating knowledge in a multidisciplinary manner cutting across existing boundaries discipline and connecting different stakeholders.

One such process has been developed within the Resilience Alliance, a scientific community working mainly on resilience of Socio- Environmental Systems (Walker et al see ref XX). This resilience analysis process takes a representative group of stakeholders through a well structured process in four steps:

The first step is the development of a conceptual model of the actual system. The model is based essentially on the stakeholder inputs and reflects their different perspectives on the system. The stakeholders will thus get a multifaceted picture of the system.

The second step examines the external disturbances and processes to which the system is expected to be resilient. Scenarios are used to help stakeholders formulating responses to unexpected events. The prime purpose of this step is to establish a range of possibilities that reflect the major uncertainties about how the system will respond to disturbances.

The third step is to address the resilience by analyzing how the system will respond to disturbances. This analysis is supported by further modeling, simulations and gaming among the stakeholders.

The final step involves a stakeholder evaluation of the process and of the implications of the emerging understanding of the resilience of the system for policy and management actions.

A framework for the analysis of resilience in social-ecological systems.