AIR CARGO SECURITY POLICY NEWSLETTER

Supply Chain Security and Organised Crime

June 13, 2011

In April 2011, the LOGSEC Consortium[1] published its findings from a year long research project to develop a Strategic Roadmap towards a large scale demonstration project in European Logistics and Supply Chain Security[2].

The LOGSEC project uncovered the gaps in supply chain security and proposed recommendations for future research and demonstration activities, within and beyond the 7th Framework Program (FP7) in the EU.

LOGSEC set out to find answers to the key questions on how to protect supply chains and logistics systems against theft, smuggling, intellectual property violations, cybercrime and a variety of other economic and ideological crimes including crime facilitating acts, and terrorism.

[1] The LOGSEC Consortium included 8 partners; EFP Consulting (UK) Ltd, Cross Border Research Association; Innovative Compliance (Europe) Ltd; European Shippers' Council; CLECAT European Association for Forwarding, Transport, Logistics and Customs Services; ATOS-Origin; Warsaw School of Economics; and, Swiss Federal Customs Administration. (www.logsec.org)

[2] LOGSEC (project number 241676) is co-funded by the European Commission under the FP7 Security Program

The ultimate aim of the project was to come up with recommendations – procedural, technological and so forth – on how to enhance SCS in an efficient manner and to carry out these enhancements without unnecessarily high investments and operational expenses.

The newsletter includes references to two additional reports discussing aspects of supply chain crime that support the LOGSEC project findings:

- in the 2011 Organised Crime Threat Assessment (OCTA), EUROPOL reported that a new criminal landscape is emerging in the EU, marked increasingly by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors. EUROPOL found that "*Internet technology has now emerged as a key facilitator for the vast majority of offline organised crime activity";* and,
- in an article on the theft of cargo in transit (pharmaceutical products sensitive to temperature and humidity), Bloomberg Businessweek reported that a $10 million dollar theft ballooned into a $47 million loss to the company.

Data authentication and cybercrime was identified as an emerging supply chain security gap by almost all of the LOGSEC respondents; and, theft of goods in transit came very high on their list of concerns.

Many of the gaps identified by the LOGSEC respondents could be addressed by physical and electronic "chain-of-custody" monitoring of shipments across supply chains.

.

The LOGSEC project

Through extensive research conducted among manufacturers, retailers and logistics service providers around Europe, the LOGSEC team identified three distinct areas, referred to as 'clusters', in which Supply Chain Security today is compromised.

First and foremost, **Supply Chain Security (SCS) awareness**, knowledge and skills of those involved in supply chain and logistics management seems to be insufficient. This is often combined with poor intelligence and risk management practices, including a lack of awareness of past crime incidents and no or limited access to crime incident statistics and trends analysis.

Secondly, issues related to **authentication**, detection and information sharing to protect the supply chain from false, fake and bogus actors and elements - when it comes to companies, people, licenses, documents, data, raw-materials and finished products - have been largely neglected. In addition, the securing of 'e-trade', supply chain fulfillment and logistics information systems against data theft and tampering requires additional attention.

Thirdly, a major SCS issue relates to **cargo in transit**. In this regard, the gaps identified by the LOGSEC project call for attention to the following: securing of cargo; securing of vehicles; safety and security of drivers; securing parking areas for cargo vehicles; integrity during logistics handovers; and rapid response and investigation by the authorities to crimes and pursuit of criminals.

The LOGSEC roadmap provides leadership in the thinking behind future demonstration projects and proposes a set of recommendations for each of the three clusters ranging from the development of models, process and tools for risk management to tools for the protection of drivers, vehicles, cargo and containers.

Whilst the enhancement of SCS is highly context dependent - the manufacturing sector, transportation mode, geographical location, geopolitics and financial circumstances all play a role in the design and implementation of optimum security responses - the aim of the

LOGSEC recommends demonstration projects that will deliver high impact benefits for business and government with minimal supply chain delays and other costs.

The optimal enhancement to Supply Chain Security is to address all the gaps as a unified package. However, the LOGSEC team has provided a flexible, modular roadmap under genuine business scenarios giving the interested parties an opportunity to prioritise, to start from the most important aspects in order to ensure quick impact and results.

Addressing the recommendations across the three clusters would clearly provide benefits for industry and the Member States. It would provide increased protection to EU citizens from crime, the criminals and the impacts of crime in the supply chain.

The full LOGSEC Roadmap can be accessed at:

http://www.logsec.org/images/upload/file/docs_logsec-roadmap-finalpublic.pdf

Overview of the LOGSEC Findings

Introduction

Global supply chains and logistics systems are threatened. Theft, trade and customs law violations, counterfeit products, organized immigration crime, sabotage, cyber crime, sea piracy, terrorism and other illicit acts generate direct losses, logistics delays, damage to reputation, and other costs for the private sector, particularly for cargo owners and logistics companies. The 2001 terrorist attacks in the USA (“9/11”) triggered an avalanche of governmental programs and regulations to mitigate the risks from terrorism such as those from large scale destruction in the supply chain system itself and/or upon specific targets and locations. Consequently the cost of preventative security for the private sector has increased.

LOGSEC, the 12-month EU FP7 Roadmap project for Supply Chain Security (SCS), set about to find an answer to the key question: “What should be done in the future to enhance SCS in a cost-efficient manner, in the European context?”, and furthermore, “Why and how should these enhancements be carried out, while avoiding unnecessarily high investments and operational expenses?” To start with, LOGSEC takes a broad view on the various crime types and terrorism (defined commonly as “man-made illicit acts for gain”) taking place in supply chains, while appreciating the fact that SCS is highly context dependent (manufacturing sectors, transport modes, geographies etc.).

In the process of seeking the answers to the above questions, the project initially examined current and future supply chain security threats.

Current and future supply chain security threats

Figure 1 illustrates from the data collected in this study the major crimes considered to pose significant threats encountered by supply chain stakeholders, ordered according to the frequency in which they were mentioned.

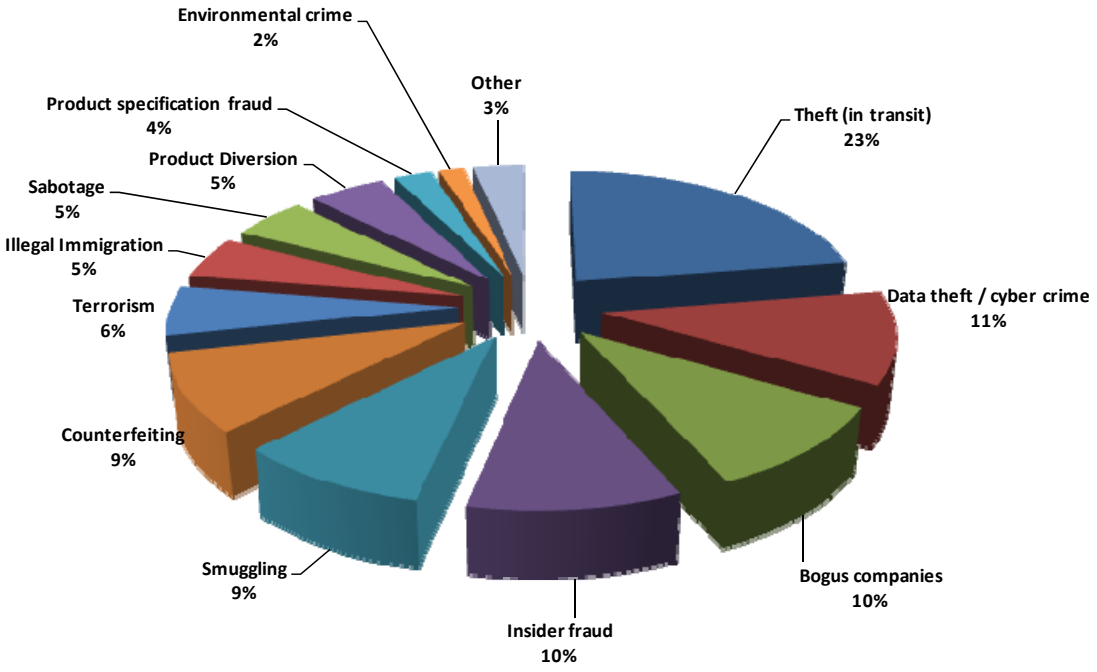

Figure 1 - Present Crime threats (referring to 12 crime types + Other).

The following was indicated: theft in transit (23%), data theft/cybercrime (11%), bogus companies (10%), and insider fraud (10%) formed the top concerns. These were followed by: smuggling (9%), counterfeiting (9%), and terrorism (6%). Other crime threats that were less frequently indicated by the respondents are illegal immigration (5%), sabotage (5%), product diversion (5%), product specification fraud (4%), and environmental crime (2%).

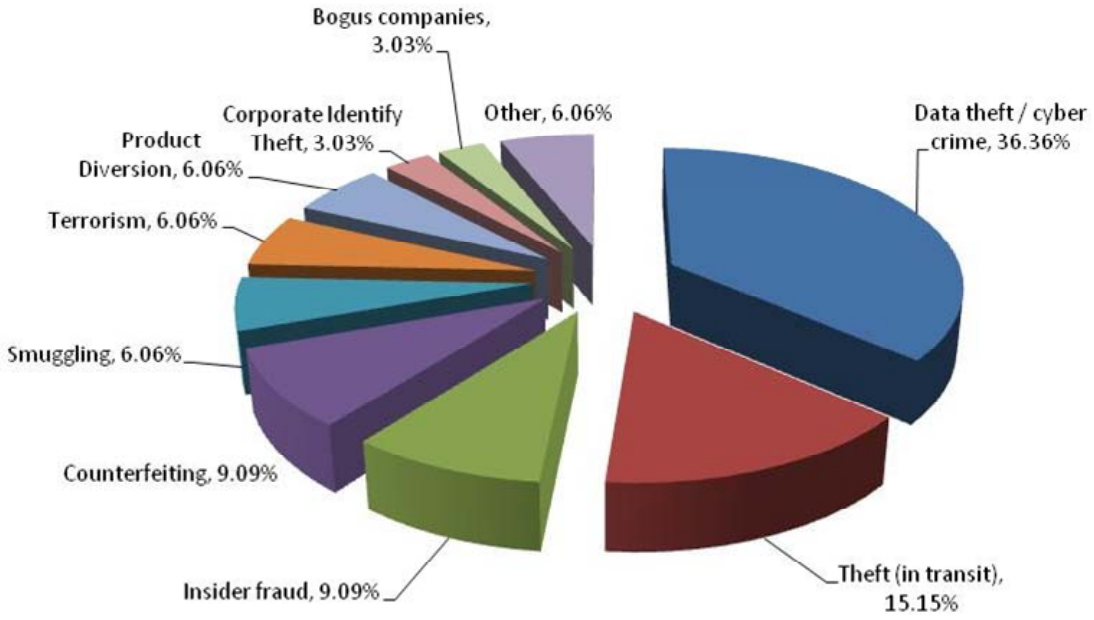

Figure 2 - Concern about crime types in the future

As shown in Figure 2 many threats are still considered relevant in the future, e.g. theft in transit (15.1%), insider fraud (9.1%), counterfeiting (9.1%) etc. However, many respondents seem to agree that data theft/cybercrime will grow to be even more relevant as a threat in the future (36.3%). Finally, threats with increasing relevance in the future, mentioned by the respondents, in supply chains include corporate identity theft (3%) and bogus companies (3%).[3]

Supply chain security gaps

The project concluded that for supply chain actors, there is a lack of security awareness, knowledge and skills, often combined with poor intelligence and risk management practices, among those involved in supply chain and logistics management. In particular there exists a lack of awareness of past crime incidents, statistics, modes of operation by criminals; limited or no access to relevant crime incident data, statistics and trends; a limited pro-active real-time response to disrupt criminal networks and activities; non-compliance with export and import regulations; limited awareness of security and varying – sometimes negative or agnostic, attitudes towards crime threats and security management; limited security knowledge and skills; and limited

[3] The project team deemed corruption and shoplifting to be outside of the main scope of the project , thus they are recorded as "other" in this diagram.

cross recognition of multiple SCS programs,

Closely linked to these issues are those relating to the collection and treatment of data regarding crime risks in the supply chain, intelligence sharing, and integrated risk management processes. In all these areas there are problems which reduce the effectiveness or impede the implementation of effective supply chain security measures.

Being able to filter out false, fake and bogus elements from the supply chain – when it comes to companies, people, licences, documents, data, raw-materials and products is also linked to effective supply chain security, but an area which is often neglected. More specifically, it is important to be able to authenticate genuine, trustworthy business partners and sub-contractors, including logistics, sales channel and reverse-logistics partners; authentication of individuals, licences, and permits; being able to detect forged documents, counterfeit raw-materials and components, and finished products and falsified product test certificates. Another important area includes the securing of 'e-trade', supply chain fulfilment and logistics information systems against data theft and tampering.

A major SCS issue relates to cargo in transit. ´Cargo-in-transit is cargo-at-risk´, especially when cargo is at-rest during the transit operation itself. In this regard, the gaps identified by the LOGSEC project call for attention to the following: securing of cargo; securing of vehicles; safety and security of drivers; securing parking areas for cargo vehicles; integrity during logistics handovers; rapid response and investigation by the authorities to crimes and pursuit of criminals; and tracing of products sent for "final destruction".

both nationally and internationally.

What this in fact implies is that there are three distinct areas, referred to in the LOGSEC report as Clusters, in which supply chain security is today compromised. Every issue or SCS gap (36 in total) that was identified through interviews, workshops and surveys conducted among private sector companies (manufacturers, retailers and logistics service providers) can be directly associated with one or more of the three LOGSEC Clusters.

Within every Cluster exists a set of 'themes', each of which offers the potential to be a subset of the Cluster and a distinct area for a future project, but the sum of these under all of the Clusters will address all the 36 identified gaps. Six themes (potential areas for future projects) were identified for each of the three Clusters.

This analysis will enable one to focus on the most significant gaps in any demonstration project based on one or more of the three clusters.

A roadmap to demonstration projects

The roadmap towards suggested demonstration projects to address SCS gaps is depicted by focussing on each Cluster and taking all or the most significant themes as the basis for individual projects.

Adding important clarity to this roadmap, the LOGSEC report provides for each project area some suggested project objectives and potential deliverables. These are indicative suggestions subject to closer evaluation and assessment of objectives and deliverables when planning for further research/demonstration programmes.

Security Awareness and Risk Management (Cluster A) Project Areas

The areas defined for the security awareness and risk assessment Cluster are described under the following headings:

- Risk management processes and tools;
- Knowledge on past incidents and modes of operation
- Security economic models, metrics and performance measures;
- Security training and awareness building;
- Security compliance management and audit tools; and
- Intelligence on evolving threats.

Table 1 provides further ideas relating to the objectives and deliverables which could be developed within demonstration projects addressing security awareness and risk management.

Table 1 - **Cluster A - Security Awareness and Risk Management sub-project areas**

Sub-project area	Objectives and deliverables
A1. Risk management processes and tools	**Objective**: to develop relevant models, processes and tools to manage risks in the supply chain, both from the private sector as well as the public sector perspective, e.g. to model criminal hazards, to identify and prioritise supply chain vulnerabilities, identify effective and cost efficient countermeasures, monitor effectiveness, etc **Deliverable**: model to enable decision makers to focus their security management resources to the areas of high risks.
A2. Knowledge on past incidents and modes of operation	**Objective**: to develop processes and data sharing platforms for crime incident reporting and statistics. The input is collected both from the private and public sector actors. **Deliverable**: approach for decision makers in both sectors to better perform risk assessment
A3. Security economic models, metrics and performance measures	**Objective**: to develop relevant models and metrics to assess the costs and benefits of security investments, both on individual security measures as well as for different security programmes. Including a methodology that allows for impact assessment of security measures, covering also legislation. **Deliverable**: tools for private and public sector decision makers to better plan security policies, strategies and measures, as well as to monitor the effectiveness of implementation.
A4. Security training and awareness building	**Objective**: to raise the overall level of awareness and knowledge of crime and security threats in supply chains, thus influencing the attitudes of various private and public sector actors towards more secure supply chains. **Deliverable**: content and process architecture for efficient supply chain security awareness building and operational training for management and staff.
A5. Security compliance management and audit tools	**Objective**: to simplify the management of security programs and to facilitate preparation for related audits, storing and providing the information required for external and internal security audits, and to identify the consistent methodology and approach of independent validators.

Sub-project area	Objectives and deliverables
	Deliverable: standardised but flexible approach for effective verification of security measures under various operational environments and circumstances. Independent validation guidelines.
A6. Intelligence on current and evolving threats	**Objective**: to identify, analyze and share intelligence on evolving crime threats in supply chains. Intelligence gathering from public sources will be the core of this sub-project, together with public-private and private-private intelligence sharing schemes. **Deliverable**: upgrade and adapt risk management system to take into account emerging threats.

Authentication, Certification and Data Protection (Cluster B) Project Areas

The six themes defined for the authentication, certification and data protection Cluster are described under the following headings:

- Authentication of companies;
- Integrity of personnel;
- Authentication of documents;
- Protection of supply chain IT systems;
- Authentication of boxes, containers and seals; and
- Authentication of raw-materials and products.

Table 2 provides further ideas relating to the objectives and deliverables which could be developed within demonstration projects addressing authentication, certification and data protection.

Table 2 - **Cluster B - Authentication, Certification and Data Protection sub-project areas**

Sub-project area	Objectives and deliverables
B1. Authentication of companies	**Objective**: help to ensure that manufacturing, trade, logistics, reverse logistics, and other service companies in the supply chain are authentic, and in possession of required licences. The scope of the sub-project includes verification of company data and information against trusted databases etc. **Deliverable**: assistance to effectively validate the security level, standard or qualification of business and supply chain partners
B2. Integrity of personnel	**Objective**: to verify past and present criminal activity among people engaged in the supply chain, through personnel background checks, integrity checking, verification of credentials, etc. **Deliverable**: tools and procedures for enhanced pre-employment background checking and pre- and on-going computer-based evaluation of personnel integrity, in compliance with EU privacy legislation and national employment rules, where applicable.

Sub-project area	Objectives and deliverables
B3. Authentication of documents	**Objective**: to prevent the introduction of false documents in the supply chain including personnel credentials, trade and logistics documents etc.. **Deliverable**: tools and methods to identify forged documents in the supply chain and to take action to minimize their ability to compromise the supply chain
B4. Protection of supply chain IT systems	**Objective**: to reduce successful attempts to steal data, to alter data, and to cause any type of harm in 'e-trade', supply chain management, order fulfilment and to logistics platforms. **Deliverable**: tools and procedures to enhance the identification and authentication of users and electronic systems and where possible, to block unauthorised access to computer systems and databases which might otherwise compromise the security of data and communications in the supply chain.
B5. Authentication of boxes, containers and their contents	**Objective**: to increase the trust of and authenticity of declarations (documentary or otherwise) regarding the content of boxes, containers and seals (i.e. "what's on the box is in the box – and vice versa"), and the integrity of packaging. **Deliverable**: tools and procedures to ensure that the content of shipments reflects the description on the company paperwork.
B6. Authentication of raw-material and products	**Objective**: to identify and filter out counterfeit products and falsified product certificates in the supply chain. **Deliverable**: tools and procedures to aid recognition of various types of counterfeit products and certification forgeries

Physical Transportation Security and Cargo Monitoring (Cluster C) Project Areas

The themes defined for the physical transportation security and cargo monitoring Cluster are described under the following headings:

- Protection of drivers;
- Protection of vehicles;
- Protection of cargo, loads, containers;
- Inspection, scanning and screening of cargo;
- Ensuring integrity during logistics handovers; and
- Protection during stops/parking.

Table 3 provides further ideas relating to the objectives and deliverables which could be developed within demonstration projects addressing physical transportation security and cargo monitoring.

Table 3 - **Cluster C** - **Physical Transportation Security and Cargo Monitoring sub-project areas**

Sub-project area	Objectives and deliverables
C1. Protection of drivers	**Objective**: to provide enhanced protection for truck drivers against all personal threats. **Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools for enhanced driver protection measures - such as anti-burglary solutions, alarms with local and distant functionality, detection sensors, armoured cabins, deterring procedures and equipment, and good/best practice
C2. Protection of vehicles	**Objective**: to provide enhanced protection for trucks and other vehicles against any type of intrusion, while balancing the measures to protect vehicles with the protection of drivers. **Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools for conveyance protection – such as anti-burglary solutions, alarms with local and distant functionalities, detection sensors, engine and brakes blocking devices, satellite controlled trip detectors, geo-location dynamic engine controllers, etc., and good/best practice
C3. Protection of cargo, loads, containers	**Objective**: to provide enhanced protection for cargo, loads and containers against any type of intrusion. **Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools for cargo protection - such as anti-burglary solutions, alarms with local and distant functionalities, detection sensors, tamper proof packaging, tamper evident seals, and tamper detection materials such as inks, powders etc.., and good/best practice.
C4. Inspections, scanning, screening of cargo	**Objective**: to enhance the opportunity for efficient inspection, scanning and screening of cargo. **Deliverable**: Catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools and techniques for inspections, scanning, screening of cargo - such as various non-intrusive high throughput, non disruptive, scanning technologies, etc and good/best practice.
C5. Ensuring integrity during logistics handovers	**Objective**: to enhance the security of freight handovers and prevent discrepancies occurring. **Deliverable**: catalogue of validated equipment and procedures through the implementation and evaluation of new and existing tools and approaches to freight handovers - such as theft protection measures, checking of product labels and quantities; documentation; seals etc.
C6. Protection during stops / parking	**Objective**: to provide enhanced protection for trucks, cargo and drivers during stops against any type of intrusion. **Deliverable**: catalogue of validated solutions and procedures through the implementation and evaluation of new and existing technologies, processes and best/good practice to guard parking areas, drivers, vehicles, and their cargo during mandatory and voluntary truck stops, including the evaluation of alternative approaches to ´traditional concept of secure parking´.

Figure 3 provides a visual overview of the three LOGSEC Clusters and the total of 18 sub-project areas

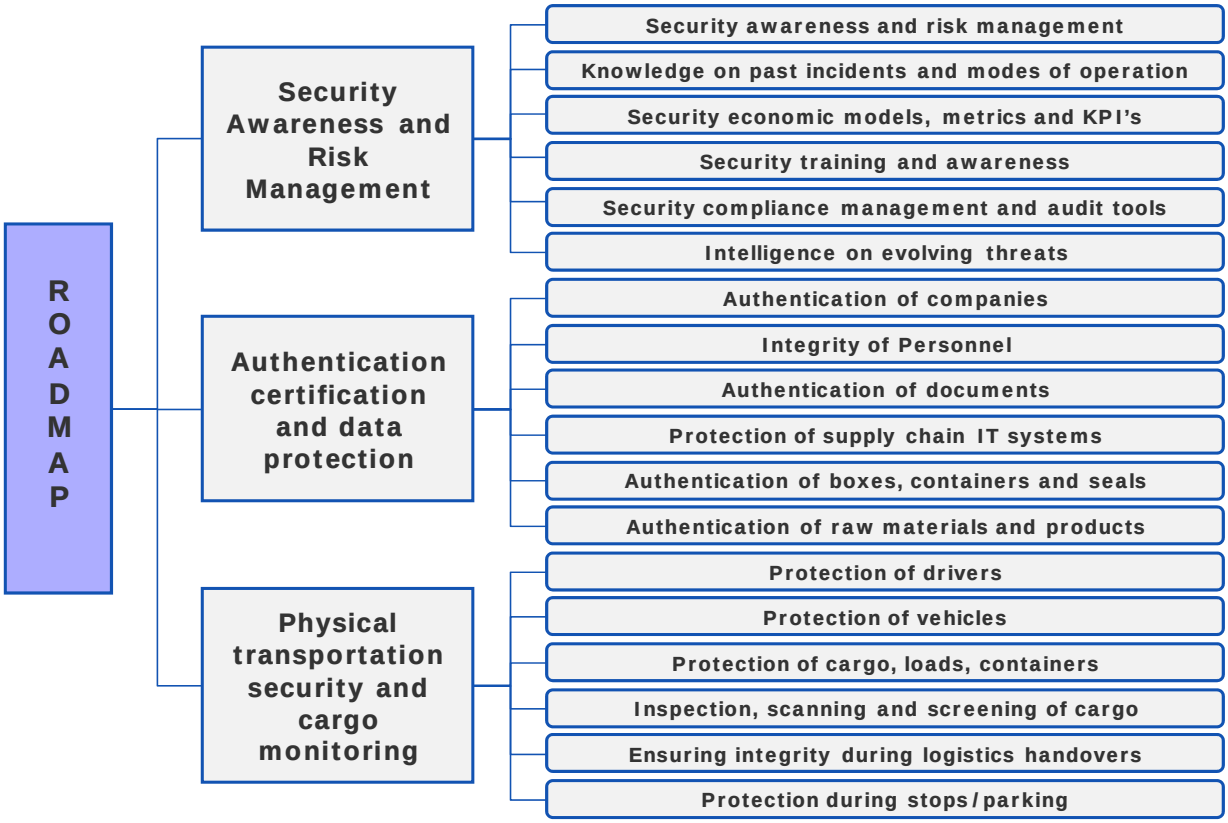

Figure 3 – Overview of LOGSEC Clusters and demonstration sub-project areas

The remaining articles in this newsletter are provided in support of the conclusions and recommendations of the LOGSEC project.

The INTERPOL 2011 OCTA report stressed that organised crime is changing and becoming increasingly diverse in its methods, group structures, and impact on society; and that internet technology has emerged as a key facilitator for organize crime.

The Businessweek article on the theft of cargo in transit, while reporting on events in the US, identified the average stolen truckload of drugs being worth $3.8 million (2.6 M EURO); and that the number of pharmaceutical cargo thefts has multiplied more than four times in the last five years

INTERPOL O**rganised** C**rime** T**hreat** A**ssessment** (OCTA),

Europol's 2011 Organised Crime Threat Assessment (OCTA), published recently, indicated that organised crime is changing and becoming increasingly diverse in its methods, group structures, and impact on society,

The 2011 issue of this bi–annual report, assesses current and expected trends in organised crime affecting the European Union, It describes, *in accordance with the LOGSEC findings*, a new criminal landscape is emerging, marked increasingly by highly mobile and flexible groups operating in multiple jurisdictions and criminal sectors. The report states that "*Internet technology has now emerged as a key facilitator for the vast majority of offline organised crime activity*"; and this was the future supply chain security gap that most worried the LOGSEC respondents.

The following overview appears on the EUROPOL web site presenting the report:

> *"Organised crime is a multi–billion euro business in Europe and it is growing in scale. The further expansion of Internet and mobile technologies, the proliferation of illicit trafficking routes and methods as well as opportunities offered by the global economic crisis, have all contributed to the development of a more potent threat from organised crime," says Rob Wainwright, Director of Europol.*
>
> *"The report highlights the fact that criminal groups are increasingly multi–commodity and poly–criminal in their activities, gathering diverse portfolios of criminal business interests, improving their resilience at a time of economic austerity and strengthening their capability to identify and exploit new illicit markets. Activities such as carbon credit fraud, payment card fraud and commodity counterfeiting attract increasing interest due to a lower level of perceived risk."*
>
> *"The OCTA estimates for the first time that organised crime groups derived more than 1.5 billion euro from payment card fraud in the EU. While the introduction of the EMV chip standard provides a very high level of protection for payment card transactions within the EU, lack of wholesale implementation in other regions has compelled EU card issuers to retain magnetic strips. As a result, half the fraudulent withdrawals made with cloned EU payment cards are currently made outside the EU."*
>
> *"Strong levels of cooperation exist between different organised crime groups, more than ever before, transcending national, ethnic, and business differences. An increasingly collaborative atmosphere has also intensified the practice of barter, in which illicit commodities are exchanged rather than purchased with cash. This has made organised crime activities less visible to authorities targeting criminal assets."*
>
> *"Internet technology has now emerged as a key facilitator for the vast majority of offline organised crime activity. In addition to the high–tech crimes of cybercrime, payment card fraud, the distribution of child abuse material, and audio visual piracy, extensive use of the internet now underpins illicit drug synthesis, extraction and distribution, the recruitment and marketing of victims of trafficking in human beings, the facilitation of illegal immigration, the supply of counterfeit commodities, trafficking in endangered species, and many other criminal activities. It is also widely used as*

a secure communication and money laundering tool by criminal groups."

"In geographical terms the most prominent organised crime activities in the EU are underpinned by a logistical architecture located around five key hubs.

*The **North West** hub retains its role as the principal coordination centre for drug distribution, due to its proximity to highly profitable destination markets, its well developed commercial and transport infrastructure, and its production capacity. The **North East** hub remains a focus for transit of illicit commodities to and from the Former Soviet Union and a base for violent poly–criminal groups with international reach. The rapid expansion in Europe, in the last two years, of the activities of Lithuanian organised crime groups is a notable feature. The leading role of the **South West** hub in cocaine and cannabis resin transit and distribution persists despite eastward shifts in some trafficking routes, and it currently serves also as a transit zone for victims of THB for sexual exploitation. The **Southern** hub continues to be prominent in criminal entrepreneurship, as a centre for counterfeit currency and commodities, a transit zone for victims of THB and illegal immigrants, and a base for some of the best resourced criminal groups in Europe.*

*Of all the hubs the **South East** has seen the greatest expansion in recent years, as a result of increased trafficking via the Black Sea, proliferation of numerous Balkan routes for illicit commodities to and from the EU, and a significant increase in illegal immigration via Greece. These developments in the region have contributed to the formation of a **Balkan axis** for trafficking to the EU, consisting of the Western Balkans and South East Europe. New transit hubs are in the process of being formed in countries such as Hungary, where several Balkan and Black Sea routes converge. Albanian speaking, Turkish and Former Soviet Union criminal groups are seeking to expand their interests in the EU, and may exploit opportunities in the possible accession of Bulgaria and Romania to the Schengen Zone, and recent and prospective EU visa exemptions for Western Balkan states, the Ukraine and Moldova."*

"Europol's OCTA is the definitive EU assessment of organised crime activity. Ministers, police chiefs, and policy makers will use it to set priorities and establish effective response measures. Europol looks forward to continuing to play a significant role in the fight against organised crime," says the Europol Director, Rob Wainwright.

The full EUROPOL 2011 OCTA report can be accessed at:

http://www.europol.europa.eu/publications/European_Organised_Crime_Threat_Assessment_(OCTA)/OCTA_2011.pdf

Cargo Theft: The New Highway Robbery

As in the OCTA study, the issues of cargo in transit, and potential for counterfeiting, also identified in LOGSEC, have been reported in a recent article on Cargo Theft published in Bloomberg Businessweek,

The headline of this article, authored by Daniel Grushkin in the May30 – June5 edition of the journal reads " *Boosting trucks laden with pharmaceuticals is a low-tech, low-risk road to riches for organized criminals*"

The introduction to the article reads as follows:

> *"Thus began a chain reaction that threatened the nation's drug supply. The drugs were owned by the U.S. division of Tokyo-based Astellas Pharma. It was Astellas's first experience with a stolen truck, and a shock to the company's directors. On the advice of the Food & Drug Administration, they started calling everyone in the supply chain that night, from wholesalers to hospitals, to warn them that the stolen drugs might surface in their facilities. The lost truck had contained 18 pallets with 21 different medicines. They were concerned about the release of all the medicines, but an immunosuppressant called Prograf was especially troubling. The drug prevents patients from rejecting transplanted organs such as hearts, livers, and kidneys. The pills are sensitive to temperature and humidity, and if left in an uncooled trailer or warehouse, can fail and result in major complications for a transplant recipient.*
>
> *Within a week, Astellas withdrew all the drugs on the marketplace from the same lots as those on the stolen load. Pills—even legitimate ones—in drugstores and hospitals nationwide had to be destroyed. The $10 million theft ballooned into a $47 million loss. It wiped out 10 percent of the company's North American sales for the quarter—a sudden, multimillion-dollar setback that's becoming increasingly common for companies who rely on America's highways.*
>
> *FreightWatch International, an Austin-based cargo security firm, collected reports of $425 million in stolen cargo in the U.S. last year. Conversations with numerous FBI employees suggest thieves could be making off with far more, with estimates ranging from $10 billion to $30 billion a year.*
>
> *"You name it, they're taking it," says Susan Chandler, executive director of the American Trucking Assn.'s Supply Chain Security and Loss Prevention Council. "Do I think there's a surge? Absolutely"*

The full cargo theft article can be accessed at:

http://www.businessweek.com/print/magazine/content/11_23/b4231072707549.htm