Workshop on Cyber Security Aspects in the Maritime Sector

Meeting of the working group of cyber security challenges in the maritime sector

The agency arranged a Maritime Cyber Security Workshop in Brussels (28/09). The objective of this workshop was to discuss the subject of Cyber Security in the maritime sector on the topics of national and European initiatives, standardisation and regulation initiatives as well as the various challenges that are coming up in this context.

Subject matter expert representations from both public organisations (including CPNI.NL, DG INFSO and DG MOVE) and private companies (e.g. Deloitte, Cassidian) were present during this Maritime cyber security workshop. The participants discussed and exchanged perspectives on the topics introduced during the various workshop presentations, as well as on related subjects presented by ENISA. These discussions resulted in a number of recommendations towards the implementation of cyber security good practices in the maritime sector.

Context

Critical infrastructure in the maritime sector sustains essential services and the movement of vital goods. Maritime activities are so crucial that their unavailability or delays in their supply chain may adversely affect the well-being of any Member State population. The need for adequate cyber security is underpinned by the scale of the maritime domain:

- 22 Member States with maritime border manage more than 1.200 sea ports supporting the maritime sector activity.
- Three major European seaports (i.e. Rotterdam, Hamburg and Antwerp) accounted in 2010 for 8% of overall world traffic volume, representing over 27,52 Million-TEUs (Twenty-foot Equivalent container Units).
- Additionally, these seaports handled more than 50% of the entire European waterborne foreign container trade.
- The main European seaports carried in 2009 17,2% of the international exports and 18% of the imports, the European economy is consequently critically dependent upon the maritime movement of cargo and passengers.
- Around 90% of EU external trade and more than 43% of the internal trade take place via maritime routes. Industries and services belonging to the maritime sector, contribute between 3 and 5 % of EU Gross Domestic Product (GDP), and maritime regions produce more than 40 % of Europe's GDP.
- Securing the critical infrastructure of the maritime sector and the movement of vital goods has become a priority and area of concern for the key European stakeholders, including the European Commission, Member State governments and the main actors from the private sector.

EU Policy on network and information security and CIIP

The workshop started with a presentation by Andrea Servida, Deputy Head of Unit at the European Commission - Unit on Internet, Network and Information Security. Through this presentation, Mr.

Servida introduced the EU Policy on network and information security and CIIP, and gave a clear description of its purposes while also describing the required future efforts. It was explained that current policy is aimed at mitigating IT security risks for Europe, looking at Cyber disruption in a holistically, ranging from national security to law enforcement.

Mr. Servida indicated that adequate policy should:

- Focus on prevention, resilience and preparedness;
- Take into account the civilian and economic stakeholders' role and capability;
- Make security and resilience the frontline of defence;
- Adopt an all-hazards approach;
- Develop a risk management culture in the EU;
- Focus on the role of socio-economic incentives;
- Promote openness, diversity, interoperability, usability and competition.

The presentation by Mr. Servida also highlighted the Communication by the Commission of March 31st, 2011 – "CIIP COM 163 (2011), Achievements and next steps: towards global cyber-security", which takes stock of the results achieved since the 2009 CIIP Action Plan and builds on existing policy initiatives.

SafeSeaNet

Mr. Jukka Savo and Mr. Jean-Bernard Erhardt from DG MOVE introduced the SafeSeaNet initiative, which consists in a centralised European platform for maritime data exchange, aimed at linking together maritime authorities from across Europe. This platform enables European Union Member States, Norway and Iceland to provide and receive information on ships, ship movements, and hazardous freight. This initiative is being implemented under the supervision of EMSA (European Maritime Safety Agency).

The presented initiative puts in practice the Directive 2010/65/EU of the European Parliament on Reporting Formalities, which states that the information on cargo and crew/passengers transmitted when ships arrive to European ports must be communicated using electronic forms (e-messages), and for which the deadline is the 1st of June, 2015.

The SafeSeaNet platform aims at offering data exchange services to clients, but must do so in a secure way as the information it provides can be considered critical. A balance is therefore required between enforcing security and granting access to the application. National single windows are put in place in order to exchange the required data from one country to another, while an interconnection of single windows with e-Customs and SafeSeaNet is also foreseen. The importance of cyber security regarding such systems was clearly stressed by the speakers.

Management of public-private partnerships and information sharing for the protection of critical infrastructures

Mr. Allard Kernkamp from CPNI.NL (Dutch Centre for Protection of the National Infrastructure), provided insights from the Dutch public-private partnerships approach for critical infrastructures. This presentation highlighted the importance of building trust relationships with the private sector in order to have an effective information exchange regarding cyber security incidents, as well as the importance of building awareness towards information and cyber security. It also introduced the newly created Harbour ISAC (Information Sharing and Analysis Centre) and its chairman, Mr. Ruud Jongejan.

The conclusions of this presentation brought a certain number of recommendations:

- **Create a sense of urgency** for management regarding cyber security;
- **Initiate information exchange** between organisations, at the European level;
- **Use standards**, checklists, methods and tools for **risk analysis and management**;
- **Develop** targeted **training and courses**.

Open issues and proposals in the security management of PIT systems – The S-Port national case

As a final presentation, Dr. Nineta Polemi, assistant professor at the University of Piraeus, introduced the audience to a set of identified open issues and recommendations in the context of Ports' Information and Telecommunication (PIT) systems. Her presentation focused on ports being considered as transport critical infrastructures and being at the centre of the maritime environment.

The following open issues were depicted:

- **Existing maritime security standards**, methodologies and tools are **monolithic** and **concentrate solely on physical security**;
- **Commercial ports** are not considered as critical infrastructures and the **security** of their **information** and **telecommunication systems is not organised**.

A set of propositions was then presented to the audience, amongst which the following key points were made:

- **Effective protection** of all layers of **PIT systems** may be organised through a **combination of IT and CIIP standards**, after a series of enhancements (e.g. considering ports' specific IT and cyber, isolated and interdependent threats, evaluating the impacts and risks considering ports as critical infrastructures, etc.).
- Targeted **maritime security management methodologies** (MSMM) implementing these new standards should be defined.
- **Maritime interoperable security management tools** should be developed.

As an illustration to this presentation, an introduction to the S-Port initiative[1] was also given. This initiative is a pilot project currently being developed by a consortium grouping the University of Piraeus, Intracom, the Information Security and Critical Infrastructure Protection Research Group (AUEB/CIS) and mVision. It aims at offering an open-source secure and collaborative environment for the security management of Port Information Systems.

Recommendations on Cyber security for the maritime sector

Following the presentations described above, the workshop proceeded into a number of open discussions on the following topics:

- Recommendations on legal initiatives;
- Recommendations for the Member States;
- Identification of the relevant stakeholders in this particular context;
- Identification of the appropriate means needed to address these recommendations.

A first point was made, identifying the overall cyber security issue in the maritime sector as being a **global issue**. As such, it is not limited to the European context, and should probably be raised to the International Maritime Organisation (IMO).

[1] *See also* http://s-port.unipi.gr

Secondly, the **lack of information exchange** on cyber security incidents and on other cyber related threats (e.g. fraud, e-crime, etc.) facing the maritime sector was highlighted. Communication must be strongly improved on these topics. It was suggested to use the ISAC concept in order to share intelligence and exchange information on cyber security incidents. The role of European CERT teams on cyber-security incidents happening in the maritime sector was also discussed, as this role should be clearly defined in their constituency.

A third point was made on the **implementation of ICT systems in ports**. The level of ICT implementation maturity strongly varies from one port to another, while security is not always a priority. Therefore, a first step towards achieving cyber security at port level would be the implementation of ICT systems that are secure by design. Propositions were also made regarding a possible categorization of ports, similarly to enterprises (small, medium, large, etc.), with the criticality of a port being linked to its size. Similarly, cyber security maturity models could also be defined for this context. It was also stressed that cyber security should not target only major/mature ports. Less mature ports should be offered the opportunity of implementing cyber security initiatives.

Next to this, the **awareness** issue was raised. It is acknowledged that the maritime sector currently lacks proper knowledge on cyber security and the associated issues. Therefore, one of the priorities in implementing cyber security within this sector would be to raise the awareness level towards cyber security and the associated risks. At a more practical level, it was recommended that ship crews be fitted with people having the appropriate knowledge regarding the technologies being used, including basic cyber security skills. Accesses to systems could also be restricted, with proper access controls being put in place. Recommendations were also made regarding the provision of cyber security training to the relevant people, with possible certifications (e.g. for ship captains). It was acknowledged that this training should not consist in technical cyber security courses but should instead focus on giving a familiarization with the commonly encountered issues. It was also suggested that ENISA could bring advice on this training.

Recommendations were also made regarding the approach that should be taken towards **implementing cyber security** in the maritime sector. This approach should be top down (from authorities to ports) and based on a holistic and broad risk management perspective. It is important to show what assets are at risk, what risks they are facing and what possible impacts the occurrence of a cyber security incident could have. This is of utmost importance when underlining the reasons why ports and authorities should invest in cyber security. Additionally, risk scenarios could be defined to bring a more concrete illustration to this issue, while figures could also be provided to give a financial perspective. Additionally, proper linkage should be defined between the various stakeholders. As such, the correct links with the authorities as well as the right actions to perform in case of an incident should be clearly specified.

It was also agreed that a standard-based approach would be longer and more complex to implement than a **good-practices approach**, while still being important and feasible considering the current support that the maritime sector is showing towards standardisation. Besides defining standards, Member States should not establish too many regulations related to this subject to avoid restricting the possible intervention of the private sector. However, as ports tend to be more and more privatised, there is a real and growing need of auditing them, as well as put in place an accreditation system. Related to this, it was also noted that privatisation brings an international aspect to ports, depending on the origin of the owners. In order to ensure a European standardisation, it was commonly agreed that the requirements that must be met by ports must be set by the port's national authorities, not by the owner's. As such, EU standards must be enforced instead of de facto standards.

The next topic that was covered was related to the **motivation** of the relevant stakeholders towards achieving cyber security in the maritime sector. As was clearly stated, there is currently a

lack of consideration by Member States on the virtual cyber security threats they are exposed to. Clear economic drivers must also be identified in order to attract the private sector.

The **data exchange** between Member States within the maritime context was also addressed. Member States should remain owners of the data they submit, while only exchanging subsets of it. Appropriate identification and categorization of the data in this scope should be required, in order to facilitate an agreement on data exchange between the various stakeholders.

Finally, a list of **relevant stakeholders** was defined. As such, the following were identified as having a major importance:

- Member States;
- The Maritime Chamber of Commerce;
- The International Chamber of Commerce;
- Relevant representatives from the ship industry.

The possibility to create a new agency that would act as a centralisation point at the European level was also discussed and balanced with the possibility of implicate the European Maritime Safety Agency in that role.