Neptunus, *e.revue*
Université de Nantes,
vol. 22, 2016/3
www.cdmo.univ-nantes.fr

Human Sea – Marisk –
Colloque 3 et 4 octobre 2016
Cité internationale des congrès – Nantes
« *Sûreté maritime et portuaire : intérêt public ou affaires privées ?* »
Table ronde présidée par le PC1EM **Laurent GALY**

English version
The European program ERC Human Sea Research and the International Conference on Safety and Maritime and Port Security Marisk held on 3 and 4 October 2016 in The City, the Nantes International Convention Centre, the conference "Economic Challenge and master the new maritime risk: what blue growth? "

ENSAM students "PC1EM" realized, under the direction of Laurent Galy, teacher at the ENSAM, a synthesis of the discussion of the round table "Maritime and port security: public or private affairs? "

This synthesis is also avalaible in french version.

French version
Le programme européen de recherche ERC *Human Sea* et la conférence internationale sur la sûreté et la sécurité maritime et portuaire *Marisk* ont organisé les 3 et 4 octobre 2016 à La Cité, Le Centre des Congrès de Nantes, le colloque « Challenge économique et maîtrise des nouveaux risques maritimes : quelle croissance bleue ? »

Les élèves administrateurs de l'ENSAM « PC1EM » ont réalisé, sous la coordination de Laurent GALY, enseignant à l'ENSAM, une synthèse des échanges de la table ronde « *Sûreté maritime et portuaire : intérêt public ou affaires privées ?* »

Speakers / Intervenants

- **Chris TRELAWNY**, Special Adviser to the Secretary-General, Subdivision for Maritime Security and Facilitation, Maritime Safety Division, IMO
- **Christophe CLARAMUNT**, Professor, Director of Naval Academy Reserch Institute (IRENav), Technopole Brest

- **Hussein Mowlid ADEN,** Director, Djibouti Ports and Free Zone Authority. General Manager, Port Secure Djibouti FZCO
- **Kathy DUA**, Consultant Port Security & Safety, Port of Antwerp – Harbour Master's Office

Authors of Synthesis : ENSAM Students / Auteurs du compte rendu : élèves de l'ENSAM
- A3AM Marine JASPERS (École nationale de la sécurité et de l'administration maritime)
- A1AM du CHAZAUD - synthèse de l'intervenant Christophe CLARAMUNT
- A3AM JASPERS - synthèse globale
- ASP JEZEQUEL – synthèse de l'intervenant Chris TRELAWNY
- ASP LEPERLIER - synthèse de l'intervenant Kathy DUA.
- ASP THOLO – synthèse de l'intervenant Hussein Mowlid ADEN

Mercredi 12 octobre 2016, Nantes

Version française

English version

"*Maritime and port security: public interest or private business?*" During the conference chaired by Laurent GALY, four international participants from the public and private sector both presented their point of view on the subject: M. Chris TRELAWANY, Special Adviser to IMO's Secretary General, M. Christophe CLARAMUNT, Professor and Director of the IRENav (French Naval Academy Research Institute), M. Hussein Mowlid ADEN, Director in Djibouti Ports and Free Zone Authority and Ms. Kathy DUA, Port of Antwerp Safety Consultant. "What is the role of private organizations in the management of security? Should States be sovereign on these aspects?" This report presents both syntheses of the conference (I) and participant by participant (II).

I) Maritime and port security: public interest or private business?

Security, which means preventing malevolent acts, is implemented on several levels in the maritime field and ports: the ship, the port and its infrastructures. Cyber-criminality is added to other threats such as terrorism, piracy and various traffics. Around one cyber-attack is revealed each week. In the aftermaths of 09/11, maritime and port industries have considered safety as a major concern. Thus, IMO, which implements security of shipping, defines in 2003 in its IPSP Code the responsibilities of the public and private actors in the field of navigation and port safety.

Maritime and port fields level unique security stakes. Due to economic and geopolitical reasons, security threats are a major stake. In fact, hampering ports and shipping should have major effects on States and their economies due to the role of shipping in their economies. Besides, the relative isolation of ships at sea involves them furthermore to these topics.

Maritime and port security is first of the States' responsibility due to their sovereign mission of guarantee of public order. The implementation of security allows to struggle against criminality in general and needs for collaboration of various services of the State such as port State inspectors and police. Security is also of public interest because of the major role that shipping had in the economy of a country. For instance, 78% of the GDP of Djibouti comes from its port activities.

States gather to implement maritime and port security at the international level. IMO is the place for international cooperation in that field. Besides the ISPS Code, which implements security for ships and port infrastructures (security plans, inspections), IMO also develops security through Codes of conduct for regions impacted by piracy. An example is Djibouti Code of conduct, which contributes to struggle against actions of pirates from Somalia.

Security is also implemented by the cooperation of public authorities at the regional, national and local levels. In the European Union, States are inspected by the European Commission, which verifies the good implementation of the ISPS Code, publishes reports with recommendations and sometimes fines. For instance, the commission inspected the port of Antwerp in 2007: it deemed efficient its safety system for oceanic terminals but underlined the need for a security plan for the entire zone.

States have a key role especially due to their means (sovereignty, financial, legal), to their role of inspection of local systems and thanks to collaborations that they can build. In 2012, for instance, Djibouti created its national coastguards, with the cooperation with the US Coast Guards. At the local scale, ports also have an important responsibility in the implementation of safety.

Security topics directly threaten maritime and port activities. It is also a private business due to its economic stakes: private stakeholders have a major role to play in the implementation of security. Djibouti's port activities are, for instance, currently threatened by maritime terrorism, traffics (drugs, weapons, human beings) and illegal immigration. The ISPS Code puts in place, for instance, security plans that maritime companies must write, implement and tried out. Private initiatives can also be proved essential in the implementation of security. In Antwerp, for instance, public-private forums are held every year thanks to a private initiative (think-tank and members of the civil society).

Security procedures and measures must not slow down the economic activity. Thus, for instance, it would be unthinkable to fence the port of Antwerp for security reasons since 409 km of public roads cross the 130 km2 of the infrastructure.

Private players must cooperate with the public players for the implementation of security. In the field of cyber threats, for instance, initiatives of formation implemented by the chair of cyber-defence of naval systems are developed in cooperation between industrial companies (DCNS, Thales) and State structures (Naval Academy, CO Cyber, DGA…). Another example: following an audit of the European commission of 2007, the authorities of the port of Antwerp have begun a close cooperation with safety services. Belgian local security committees gather authorities from the port, the maritime police, the local police, safety teams and users. Also, public and private players work together within an information network that collects remarks on unusual events. They participate in joint formations and exercises.

To conclude, maritime and port security is both public and private players' business and interest. The efficiency of the implementation of security is thus depending on the cooperation of those actors. In order to face major threats, the current international challenge for security is the application of the ISPS Code and the harmonization of safety and security standards (FAL Convention of IMO). The formation of public and private players remains a major stake.

II) Syntheses of the participants

- **The approach to maritime security – Chris TRELAWNY**

IMO (International Maritime Organisation) is a specialized agency of the United Nations created in 1948 in order to deal about maritime issues. In a nutshell, IMO's motto is "*safe, secure and efficient shipping on clean oceans*". This definition shows the two main aspects of this organisation: safer shipping and cleaner oceans. In order to reach this goal, especially in safety and security, IMO has developed some conventions that deal with specifics points. The most famous are the Load Lines (which deals about safety of merchandises), the MARPOL (on maritime pollution), and especially the SOLAS (International Convention for the Safety of Life at Sea), which includes security items and charge public and private actors with responsibilities on shipping and port security. Specials measures are reinforced by the ISPS Code (adopted in 2003, in the aftermaths of the 9/11). IMO is funded by flag State. Panama is thus the biggest contributor to this international organization, because it gives 17% of its global budget.

With all these conventions, IMO contributes to abolish piracy in three regions: Somalia with Djibouti Code of Conduct, Gulf of Guinea with another Code of Conduct and in South-East Asia with the ReCAAP (Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia). IMO has also played an active role in struggling against migrants' traffics.

Maritime issues have changed between 2004 and today. Threats have evolved: piracy and armed robbery have fallen while cyber-attacks, terrorism, wildlife affect and illegals traffics have increased. Also, sustainable development is new issue and prevention against terrorism has grown better. Ports create wealth. Port safety is both efficient and effective.

However, there is a huge challenge for maritime safety and security: the need for a cooperation between the ports players – public and private actors, national, regional and international actors. The

aim is to succeed in harmonising standards and norms, best practices and to build a real cooperation. The FAL Convention (Convention on facilitation of International Maritime Traffic), adopted in 1965 (which came into force in 1967 and soon amended by the FAL 40 in 2017; theses amendments will come into force in 2018), is the best tool of IMO in that field. Its goal is to improve harmonization and simplify procedures and documentation used for international shipping. But to reach this goal, practices must be improved, especially through "win-win concessions". Moreover, the ISPS Code must be promoted and implemented.

To conclude, it is essential for every players of port activities to help for expansion, with more cooperation and improve security and safety, which include struggle against traffic and corruption. We need more standardization, more training. Aerial sector is the best model for possible enhancement.

- **The Cybersecurity applied to maritime field – Christophe CLARAMUNT**

We can see in our modern societies a progressive extent of the use of computers and automatics and in industry in particular. That extend go with a general spreading of malevolent software, forming up an exploding threat for last years. In 2007, synchronised devastating attacks in Estonia against official sites, media, bank system is a clear step into cyber-warfare era. Then in 2010, Stuxnet virus destroyed centrifuges of the Iranian programme for uranium enrichment. This is another huge step into attacks by Advanced Persistent Threats (APT), able to target industrial objectives, such as SCADA systems (Supervisory Control and Data Acquisition for industrial automatons). Theses APTs implement complex and specific architectures of attacks, written in planned strategy and conducted in long lasting time. And today, there are no more weeks without big scale cyber attack reported in media.

France is conscious of theses threats, at political level (Bockel Report 2012), at strategic level (Strategic Defence and Security Reviews (*Livre Blanc*) of 2008 and 2013), at joint level… Chief of Defence Staff considers cyberspace to be the 5th warfare environment after land, air, sea and space and this global warfare is carried out by the Cyber General Officer in Strategic Joint Headquarters (CPCO in Paris Balard). In this framework were created Cyber-defence of Naval Systems chair, but also many education initiatives, partnership with academies (Naval Academy, Telecom-Bretagne…) and industry actors (DCNS, Thales). French State is committed with new and reinforced structures such as Cyber Command, Armed Forces Services Headquarters, DGA (delegation for armament), ANSSI (National Agency for Security of Information Systems), CALID (Analysis Centre for Cyber-defence)…

Maritime actors are especially sensible to cyber threat, due to geopolitics and business concerns. In addition, maritime world is very vulnerable: ships at sea are partially isolated, with limited crews and more and more complex technologies aboard, controlling almost all the ship's functions and some of the more vitals (navigation, engines, weapons systems for warships). Theses systems are quickly deprecated (on average one ship's life lasts 30 years), leaving the ship more vulnerable faced to the constant development of the cyber threat. More than ships, it is also a whole ecosystem of ports, harbours, oil and marine renewable power infrastructures that can be targeted. All the situations caused by human actions, mistakes, failures can be provoked by cyber-attacks (missile launching, load ripping, collision, grounding, oil spill…), with human consequences (passenger ships), and other damages.

Cyberspace is physical, logical and social. Threats really exist and come from States, enterprises, criminal or terrorist organisations, hackers. This cyber-war is included in a global information war that covers military and industrial intelligence, psyops… Organisations are more and more targeted. APT are developing.

To be secured, a system needs to guarantee availability of its service, integrity of information and confidentiality of its secrets. Security policies are technical and non-technical (physical protection, organisation, human considerations).

Cyber-security is composed of cyber-protection (protection to prevent attacks), cyber-defence (detection, adaptation, response) and cyber-resilience (continuation of mission).

In this very complex framework, Naval Systems Cyber-defence chair conducts research around issues like SCADA, real-time, sensors, AIS signals.

Cyber, in spite of appearing nebulous to seafarers, is now completely integrated in their work environment. Cyber-security has become a significant base for safety, and for security as well.

- **From French enclave to Strategic crossways: The prominence of Djibouti in the Horn of Africa – Hussein Mowlid ADEN**

Since 2008, Djibouti port facilities have welcomed and furnished a set of services to more than 300 navy ships per year. Regarding the extension of the only US African-based permanent base and the current re-settling of the French navy, Djibouti became an international hub involving new cooperation methods. The last opening of the IMO funded centre for regional maritime activities underlines the importance of Djibouti for the international community.

Djibouti is now in a capacity growing process regarding its maritime infrastructures. Both the Djibouti Port Administration and the free zone authority are looing closely to these activities that would enhance the leading role of the Port in the region.

Djibouti is also a port of importance because of its commercial activities. As a former French colony, a major part of its existing infrastructures are coming from this heritage. Moreover, Djibouti is situated in a strategic crossway between many routes linking Europe, Asia and Eastern Africa. 78% of Djibouti's GDP is related to port activities. The existing infrastructures are the port, a free zone, an oil terminal and a container terminal.

Since 2009 Djibouti represents a world-ranked hub and is continuously increasing its commercial traffic. Between 2009 and 2015, we can notice an obvious increase in trade particularly in the field of containers. Between 2008 and 2015, more than 40 navies used Djibouti port facilities within the framework of trade securing in this strategic area.

The Republic of Djibouti is widening its port and maritime infrastructures. The Djibouti Port Administration and the Free Zone Authority are keeping an eye on these developments and will ensure the compliance with international rules.

In the medium and long term, Djibouti plans several new infrastructure projects for a total of 40 billion US dollars: a gigantic and quite ambitious project built on many sites all over the bay, on a great part of the coastline and in the inland. For instance, this project plans the building of new terminals, shipyards, rail transport infrastructure and new free zones.

The port of Djibouti and its activities are currently facing various threats: maritime terrorism, which is a consequence of the weakening of the neighbouring States and the development of piracy (Somalia, Yemen), but also drug trafficking and arms dealing with Djibouti as crossroads to Europe and Asia.

Because of its strategic situation on the coastline, Djibouti is also a central point for human beings trafficking. Djibouti's backcountry is synonymous with an influx of migrants from Africa in direction of the Arabic Peninsula and Europe.

The government of Djibouti focuses its maritime policy on security, safety and marine environment. As a matter of facts, Djibouti has ratified most of international agreements such as the SOLAS convention or the ISPS Code. The compliance with international standards remains key for this State, which wants to make trade as easy as possible. This led to the creation of national coastguards four years ago, in collaboration with US Coast Guards. Djibouti is also an important operational centre of the international fighting system against piracy, which is warning but still rife in the region.

Djibouti and the rest of the continent need regional and international cooperation between private and public actors for the establishment of security measures. National security plans submitted by Djibouti every year are revised and put into place with the support of the US Coast Guards, particularly for the training of port safety personnel. The cost of safety is very high. The part of safety spent in Djibouti is 2 to 3%, higher than in most other African States. The investment proves to be key because an ineffective safety would have serious economic consequences for this country.

In view of the current economic situation and budget cuts, questionings remain: who should pay? Should recipients or economic operators pay? Should we consider it as public service or as national safety measures?

- **Public-private Partnership in Port Security, Kathy DUA**

Mrs Kathy DUA, security and safety consultant for the port of Antwerp introduced the original security management of this huge 130km^2 for 163km of quay infrastructure. For obvious economic and efficiency reasons, turning a port into a closed zone seems impossible and quite unrealistic. In fact, 409km public roads cross the port area.

The security plan of the port of Antwerp was designed in a narrow partnership between the port authorities and both the users and the public services. Since 2004, ship captains have the responsibility of the implementation of the ISPS Code requirements. But a real security strategy was expected from port authorities and port State both: the port security plan (PSP) was a crucial step in Belgium in order to fight against diverse threats, from criminal activities to terrorism. The speaker and the audience underlined the responsibility of the State in the prevention of radicalization phenomena. This public-private partnership has been fostered by the "National Authority – Maritime Safety", which conducts maritime safety policies backed for this by various administrations (Defence, Environment, Foreign affairs, etc.). This policy is conduced by the "Local Committees – Maritime Safety", gathering port authorities, maritime police, local police, security teams and users (dockers, captains, owners etc.)

Every year, public-private forums, initiated by think-thanks and the civil society gather federal judicial police, task forces, attorneys and seamen to discuss port security and specific measures for Antwerp issues. Such initiatives enlighten the tremendous need in the sea world for complementarity between the three levels of security (ship security, port facilities security, port security). ISPS Code chimes plainly in this path. However, despite the multi-actor cooperation and the procedures and specific measures of the port, State must remain the milestone of port security. That is the vision of security in the port of Antwerp.

Innovative systems have been implemented in the port. The *port information network* is one among many examples. This system is a common online platform for port authorities, users and public forces centralizing reports of unusual observations by everybody noticed everywhere in the port zone.

The joint formation for public and private actors to create common values and reflexes is absolutely necessary to ensure a high standard security level. Then, large-scale exercises are implemented each year in the port (*Flash Fire* in 2010, *Winterwatch* in 2011, *Black Wolves* in 2014…). Experience reports are systematically addressed to national authorities.

Complementarily, additional to official guidelines including the European Commission *European handbook of maritime security exercises and drills (Exercitium)*, the port of Antwerp has developed video-ludic instruments to apprehend a complex and technical environment: the very serious game « Port of Antwerp security game » is a unique way to do it.

Port security is a constant challenge that needs various supports, encompassing both prevention *ex ante* and a capability to manage terrorist and criminal occurrences *ex post*. In a fiery security context, in a strategic environment as the port of Antwerp, maritime security must be a common work. There is a need for a well-balanced intelligence involving the private sector and public services.

« *Sûreté maritime et portuaire : intérêt public ou affaires privées ?* », : sous la présidence du PC1EM Laurent GALY, quatre intervenants internationaux issus des mondes public et privé ont développé leur point de vue sur le sujet, M. Chris TRELAWANY conseiller spécial du secrétaire général de l'OMI, M. Christophe CLARAMUNT professeur et directeur de l'IRENav (institut de recherche de l'Ecole Navale), M. Hussein Mowlid ADEN, directeur au port de Djibouti et Mme. Kathy DUA, consultante en sûreté pour le port d'Anvers. « Quelle est la place des entreprises dans la

gestion de la sûreté ? Les Etats doivent-ils être souverains sur ces aspects ? ». Après une synthèse des interventions sous le prisme de la problématique de la conférence (I), la note présente des synthèses par intervenant (II).

I) Sûreté maritime et portuaire : intérêt public ou affaires privées ?

La sûreté, qui consiste à prévenir les actes malveillants, est mise en place à plusieurs niveaux dans les domaines maritime et portuaire : le navire, le port et ses infrastructures. Aux menaces de terrorisme, piraterie et trafics divers s'ajoute la cybercriminalité : environ une attaque cyber d'envergure est révélée par semaine. Au lendemain du 11 septembre 2001, les industries maritime et portuaire se sont mobilisées autour des enjeux de sûreté. Aussi, l'OMI, qui assure notamment la sûreté des transports maritimes, détermine, dès 2003, via son code ISPS, les responsabilités des acteurs publics et privés en terme de navigation et de sûreté portuaire.

Les domaines maritimes et portuaires recouvrent des enjeux particuliers en matière de sûreté. Leurs dimensions géopolitique et économique les rendent particulièrement sensibles aux menaces de sûreté : au vu de la dépendance des économies actuelles au commerce maritime, une entrave a celui-ci pourrait avoir des conséquences graves pour les Etats et leurs économies. Par ailleurs, l'isolement partiel des navires à la mer les rend également plus sensibles à ces problématiques.

La sûreté maritime et portuaire est avant tout de la responsabilité des Etats du fait de leur mission régalienne de maintien de l'ordre public. La mise en œuvre de la sûreté permet plus généralement de lutter contre la criminalité et nécessite la collaboration de différents services étatiques tels que les inspections de l'Etat du port ou la police judiciaire. La sûreté est également un intérêt public du fait du rôle vital qu'a généralement le commerce maritime dans l'économie d'un pays. 78% du PIB de Djibouti est, par exemple, issu des activités portuaires.

Les Etats s'organisent entre eux pour mettre en place la sûreté maritime et portuaire au niveau international. L'OMI est l'instance privilégiée de coopération interétatique dans ce domaine. Au-delà du code ISPS, qui prévoit la mise en œuvre de la sûreté au niveau des navires et des installations portuaires (plans de sûreté, inspections), l'OMI développe également la sûreté par des codes de conduite propres aux régions sensibles en terme de piraterie. Un exemple est le Code de conduite de Djibouti qui participe à contrer les actions des pirates somaliens.

La sûreté est également mise en œuvre par la coopération d'acteurs publics à l'échelle régionale, nationale et locale. Au sein de l'Union européenne (UE), les Etats sont inspectés par la commission européenne qui vérifie notamment que le code ISPS est bien mis en œuvre : elle édite des rapports avec des recommandations et éventuellement des amendes. Elle a, par exemple, audité le port d'Anvers en 2007 : ses dispositifs de sécurité pour les terminaux océaniques ont été salués mais elle a souligné qu'il fallait un plan de sûreté pour l'ensemble de la zone. Les Etats ont un rôle clé notamment du fait de leurs moyens (souveraineté, financiers, légaux), de leur rôle d'inspection et d'audit des dispositifs locaux et des collaborations qu'ils peuvent créer. En 2012, Djibouti a, par exemple, créé les garde-côtes nationaux avec la coopération des garde-côtes étasuniens. Au niveau local, les ports ont aussi une responsabilité importante dans la mise en œuvre de la sûreté.

Les problématiques de sûreté menacent directement les activités maritimes et portuaires. Aussi est elle également une affaire privée du fait de son enjeu économique : les acteurs privés ont un rôle clé à jouer dans la mise en œuvre de la sûreté. Les activités du port de Djibouti sont, par exemple, menacées actuellement par le terrorisme maritime mais également par les trafics en tout genre (drogue, armes, êtres humains) et l'immigration clandestine. Le code ISPS prévoit, par exemple, des plans de sûreté que des compagnies maritimes doivent élaborer, mettre en œuvre et tester. Des initiatives privées peuvent également s'avérer importantes dans la mise en œuvre de la sûreté. A Anvers, par exemple, des forums public-privé se tiennent tous les ans à l'initiative d'acteurs privés (*think-tank* et membres de la société civile).

Les procédures et les mesures de sûreté ne doivent pas ralentir l'activité économique. Ainsi, par exemple, il serait inenvisageable de clôturer le port d'Anvers en invoquant la sûreté car 409 km de voies publiques sillonnent les 130 km2 de l'infrastructure.

Les acteurs privés doivent collaborer avec les acteurs publics pour la mise en œuvre de la sûreté. Dans le domaine de la lutte contre les menaces cyber, par exemple, les initiatives de formation mis en œuvre par la chaire de cyber-défense des systèmes navals sont développées en partenariat entre des industriels (DCNS, Thales) et des structures de l'Etat (Ecole Navale, CO Cyber, DGA…). Autre exemple dans le domaine portuaire : à la suite d'un audit de la commission européenne de 2007, les autorités du port d'Anvers ont engagé une étroite collaboration avec les services de sécurité. Les comités locaux de sûreté maritime belges réunissent les autorités portuaires, la police maritime, la police locale, les équipes de sécurité et les utilisateurs. Les acteurs publics et privés sont également associés au sein d'un réseau d'information et de centralisation des observations d'événements inhabituels et associés dans des formations et exercices.

Ainsi, la sûreté maritime et portuaire est l'affaire et l'intérêt de tous, acteurs publics et privés : c'est du partenariat entre ces acteurs que dépend l'efficacité de sa mise en œuvre. Face aux menaces, le défi international actuel pour la sûreté est l'application du code ISPS et l'harmonisation des standards de sécurité et de normes de sûreté (Convention FAL de l'OMI). La formation des acteurs publics et privés demeure un enjeu clé.

II) Synthèses par intervenant

- **L'approche de la sûreté maritime – Chris TRELAWNY**

L'OMI (Organisation Maritime Internationale) est une agence spécialisée de l'ONU dans les questions maritimes créée en 1948. L'OMI assure la sûreté, la sécurité et l'efficacité des transports maritimes sur des océans propres. En effet, ses activités peuvent se regrouper en deux catégories : permettre une navigation sûre ainsi que maintenir la propreté des mers. Pour ce faire, notamment dans le volet de la sûreté et sécurité, l'OMI dispose de conventions juridiques portant sur des points particuliers. Les plus connues sont la Load Lines (sur le chargement des navire de commerce), la MARPOL (sur la pollution maritime) mais surtout la SOLAS (sur la sauvegarde de la vie humaine en mer), qui contient un volet sur la sûreté maritime. Elle détermine en effet les responsabilités des acteurs publics et des acteurs privés, en ce qui concerne la navigation, mais aussi la sûreté des installations portuaires, détaillée dans le Code ISPS, datant de 2003 (créé suite aux attentats du 11 septembre). L'OMI aussi, loin de travailler seule sur ces thématiques de sûreté portuaire, coopère avec d'autres organisations internationales, comme l'OIT, ou encore l'OMC, toutes deux concernées par ce secteur d'activité. L'OMI est financée par les États du pavillon ; ainsi, le Panama est le plus gros contributeur de l'organisation internationale, en participant à hauteur de 17 % du budget global.

L'OMI a entre autres permis grâce à ses convention de participer à la diminution des attaques de pirates dans trois régions du monde : en Somalie avec le Code de conduite de Djibouti, dans le Golfe de Guinée avec un autre Code de conduite et en Asie du Sud-Est avec le ReCAAP (Accord régional sur la lutte contre la piraterie et le vol à main armée contre les navires en Asie). L'OMI a également eu un rôle actif dans la lutte contre le trafic de migrants.

Les enjeux maritimes ont beaucoup changé entre 2004 et 2016. D'une part les menaces sont différentes : si les actes de piraterie et de vol à main armée ont chuté, les cyber-attaques, le terrorisme, la pêche illégale et les trafics en tout genre ne font qu'augmenter. D'autre part, le développement durable maritime s'est fortement développé ainsi que la prévention contre le terrorisme. Les ports créent de la richesse et leur sûreté et leur sécurité ne cesse de s'améliorer.

Cependant, en matière de sécurité et de sûreté, un défi de taille reste à relever : assurer une coopération entre les divers acteurs du secteur – acteurs publics et privés, mais également nationaux, régionaux et internationaux, pour arriver à une harmonisation des standards de sécurité et les normes de sûreté, en les améliorant par la même occasion. La Convention FAL (Convention sur la facilitation du trafic maritime international) de 1965 (entrée en vigueur en 1967 et prochainement amendée lors de la FAL 40 en 2017 ; amendements qui rentreront en vigueur en 2018) est le meilleur outil de l'OMI dans ce domaine. Son but est d'harmoniser et de simplifier les procédures et documentations nécessaires aux voyages internationaux. Mais pour parvenir à cela, il faut améliorer les pratiques,

notamment en faisant comprendre qu'il faut faire des concessions pour que tous soient gagnants, promouvoir le code ISPS, son application et la sécurité des ports.

Ainsi, il est important pour tous les acteurs ayant à faire au secteur portuaire d'aider à son développement, en coopérant et en améliorant leur sécurité, sûreté, ce qui passe notamment par la lutte contre tout trafic ou corruption. Il faut aller vers la standardisation et vers plus de formation, en prenant notamment exemple sur le secteur aérien, en avance de plusieurs années sur ce terrain.

- **La Cybersécurité appliquée au domaine maritime – Christophe CLARAMUNT**

L'extension progressive de l'usage de l'informatique et de l'automatique dans nos sociétés modernes en général et dans l'industrie en particulier s'est également accompagnée d'une montée des logiciels malveillants, formant une menace qui a explosé ces dernières années. En 2007, les attaques simultanées en Estonie des sites officiels, des médias et du système bancaire marque la bascule dans l'ère de la cyberguerre. Puis en 2010, la destruction des centrifugeuses iraniennes du programme d'enrichissement d'uranium en 2010 par le virus Stuxnet montre l'extension du domaine d'attaque cyber aux SCADA (systèmes de commande et de contrôle d'automates industriels), et la conception d'*Advanced Persistent Threats* (APT), architectures d'attaques complexes, spécifiques, s'inscrivant dans une stratégie planifiée et conduite dans la durée. Aujourd'hui, il ne se passe plus de semaine sans qu'une attaque cyber d'envergure ne soit dévoilée dans les médias.

La France a pris conscience de ces menaces, que ce soit aux niveaux politique (Rapport Bockel 2012), stratégique (livres blancs de 2008 et 2013), interarmées (CIA/DIA, PIA…). L'état-major des armées (EMA) considère le cyberespace comme le 5^{e} domaine de lutte après la terre, l'air, la mer et l'espace, et la lutte est coordonnée par l'officier général Cyber (Amiral Coustillière) du Centre de planification et de conduite des opérations (CPCO, à Balard). C'est également dans ce cadre qu'a été créée la chaire de cyberdéfense des systèmes navals du Pr Claramunt et que sont menées des initiatives de formation Cyber, particulièrement en Bretagne (Pôle d'excellence Cyber et partenariats avec des écoles : École navale, Telecom-Bretagne…), partenariats avec des industriels (DCNS, Thalès). Les structures de l'État sont aussi engagées et fortement renforcées : CO Cyber, EM^{x}/SIC, DGA, ANSSI, CALID…

Les acteurs du domaine maritime sont particulièrement sensibles à cette menace cyber, à cause de l'enjeu géopolitique et économique que ce domaine représente, mais également parce qu'il se révèle très vulnérable : les navires à la mer sont en isolement partiel, armés par des équipages de plus en plus réduits mais recelant une complexité technologique croissante qui intéresse toutes les fonctions du navire et notamment les plus vitales (navigation, moteurs, systèmes d'armes pour les navires de guerre…), et rapidement dépassés (la durée de vie moyenne d'un bâtiment est de 30 ans, ce qui rend les systèmes plus vulnérables à la progression constante de la menace). Mais c'est également tout un écosystème d'infrastructures portuaires, pétrolières, d'énergies marines renouvelables qui peut être ciblé. Les situations habituellement issues d'actions humaines, de fautes ou de pannes peuvent être aussi causées par des cyberattaques (départ missile, instabilité due à un arrimage faussé, abordages, échouages, marées noires…), avec des conséquences humaines (navire à passager par exemple), matérielles (explosion d'une cargaison dangereuse par exemple), économiques (cargaison perdue), ou encore géopolitiques.

Le cyberespace est à la fois physique (les ordinateurs et les composants réseau), logique (architecture réseau et logicielle, informations stockées) et social (communications, interactions sociales, domaine sémantique). La menace existe, c'est-à-dire que l'intention malveillante est bien réelle et peut provenir d'acteurs étatiques, d'entreprises, d'organismes mafieux ou terroristes, de hackers, *etc*. La cyberguerre s'inscrit dans une guerre de l'information généralisée qui recouvre également une guerre du renseignement (militaire et surtout industriel), une guerre électronique, une guerre psychologique… et les mobiles sont variés : renseignement (cyber-espionnage et cyber-guerre), argent (cybercriminalité), idéologie, vengeance, jeu (cyber-activisme). Les organisations sont de plus en plus visées et les attaques ciblées se développent (APT).

La sécurité d'un système cherche à garantir la disponibilité du service, l'intégrité (non-altération des informations) et la confidentialité (non-compromission des secrets). Les politiques de sécurité sont tout d'abord techniques (sécurité par conception, confinement, chiffrement, systèmes de détection…), mais aussi non-technique (accès physique, organisationnelle et humaine).

La cybersécurité se partage entre cyberprotection (dispositifs et organisation de la protection en amont), cyberdéfense (détection de la menace, adaptation du système, réponse à l'attaque) et cyberrésilience (poursuite de la mission malgré l'attaque).

Dans ce cadre très complexe, la chaire de Cyberdéfense des systèmes navals traite de nombreux sujets, en axant notamment ses recherches sur les problématiques des SCADA, des systèmes temps-réel, de la sécurité des capteurs, de la défalsification des signaux AIS.

Le cyber, alors même qu'il peut sembler éthéré aux marins, fait désormais pleinement partie de leur environnement de travail. La cybersécurité est bien devenue une des bases de leur sécurité comme de leur sûreté.

- **A partir de l'enclave française aux stratégiques *crossway* : L'importance de Djibouti dans la Corne de l'Afrique – Hussein Mowlid ADEN**

Depuis 2008, les infrastructures de Djibouti ont accueilli et fourni des services à plus de 300 navires militaires chaque année. Avec l'expansion de la seule base permanente des militaires américains sur le continent, la reconfiguration de la présence militaire de la France et de l'établissement d'installations militaires italiennes, japonaises et autres, Djibouti est devenu un hub international maritime et naval où de nouvelles méthodes de coopération et de relations sont en cours de développement.

Pourquoi Djibouti est important en tant que port de commerce ? Ancienne colonie française, une grande partie des infrastructures existantes sont issues de cet héritage de la France. Djibouti est situé à la croisée de plusieurs grandes routes maritimes vers l'Europe, l'Asie, le Moyen-Orient ou encore l'Afrique de l'Est. 78 % de son PIB est issu des activités portuaires. Les infrastructures existantes sont : le port, la zone franche, le terminal pétrolier et le terminal à conteneurs.

Depuis 2009 Djibouti constitue un hub international et ne cesse d'augmenter son trafic de marchandises sur ses installations portuaires. Entre 2009 et 2015 on remarque une augmentation visible des échanges notamment avec les navires porte-conteneur. Entre 2008 et 2015 plus de 40 marines nationales ont utilisés les infrastructures portuaires de Djibouti dans le cadre de la sécurisation des échanges dans cette partie stratégique du commerce international.

La République de Djibouti est en train d'élargir ses ports et infrastructures maritimes. Les ports de Djibouti et l'Autorité de la Zone Franche surveillent ces développements et assureront leur conformité aux normes internationales.

A moyen et long terme Djibouti possède plusieurs projets d'infrastructures nouvelles d'un montant total de près de 40 milliards de dollars US : un projet gigantesque assez ambitieux et avec plusieurs chantiers s'étalant sur toute la baie et une grande partie du territoire littoral mais aussi intérieur. Par exemple, ce projet comprend la construction de nouveaux terminaux, d'ateliers de réparation navale, de dispositifs de transport par rail ou encore de nouvelles zones franches.

Le port de Djibouti et ses activités sont actuellement menacés par plusieurs problèmes : terrorisme maritime lié aux Etats faillis voisins et leurs réseaux organisés de piraterie (Somalie, Yémen) mais aussi trafic de drogue et trafic d'armes en provenance des mêmes Etats et utilisant Djibouti comme plateforme d'échange et d'envoi vers l'Europe et l'Asie.

La position littorale stratégique et la situation géographique de Djibouti placent aussi l'Etat dans une situation centrale dans le trafic d'êtres humains. L'arrière-pays de Djibouti expose cette dernière à un flux de migrations internationales important en provenance d'Afrique et à destination de la péninsule arabique et de l'Europe.

- **Le partenariat public-privé dans la sécurité portuaire – Kathy DUA**

Mme Katy DUA, consultante sécurité et sûreté du grand port d'Anvers a présenté à l'auditoire l'organisation originale de la sûreté dans cette énorme infrastructure de 130km^2 pour 163km de quais. Pour des raisons d'efficience économique, il est impossible et non souhaitable de faire d'un port un

espace clos (pas moins de 409km de voies publiques sillonnent le site). Les autorités du port d'Anvers ont orienté sa sûreté autour d'un partenariat étroit avec ses utilisateurs ainsi qu'avec les pouvoirs publics. Si les armements se doivent de respecter les obligations du code ISPS depuis 2004, une stratégie de sûreté était attendue de la part des autorités portuaires et de l'Etat du port. Le *port security plan* (PSP) a constitué en la matière une étape importante en Belgique afin de lutter contre des menaces polymorphes, de nature aussi bien criminelles que terroristes. Il a été rappelé à cette occasion la responsabilité de l'Etat pour prévenir en amont les phénomènes de radicalisation. Cette coopération public-privé est encouragée par *l'autorité nationale pour la sûreté maritime*, chargée de conduire les politiques de sûreté maritime et empruntant ses compétences à différentes administrations (défense, environnement, affaires étrangères…), et mise en œuvre par les des *comités locaux de sûreté maritime* réunissant autorités portuaires, police maritime, police locale, équipes de sécurité et utilisateurs.

Il convient de souligner également l'importance des *forums public-privé* qui se tiennent tous les ans à Anvers à l'initiative de *think-thank* et de membres de la société civile, réussissant à réunir police judiciaire fédérale, forces d'intervention et autorités portuaires. De telles initiatives illustrent l'importance pour les acteurs du monde maritime d'une réelle complémentarité entre trois niveaux de sûreté : la sûreté des navire, la sûreté des infrastructures portuaires et la sûreté du port. Le code ISPS s'intègre pleinement dans cette démarche, et des procédures et des mesures de la part de l'Etat du port doivent permettre d'assurer la sécurité dans les zones portuaires. C'est le chemin choisi par le port d'Anvers.

Des systèmes innovants ont été mis en place sur le port comme un *port information network*, permettant de relier autorité du port, usagers, pouvoirs publics et de centraliser les observations d'évènements inhabituels qui pourraient être faites par tous dans l'enceinte du port.

La formation conjointe des acteurs publics et privés est tout à fait capitale pour parvenir à un haut niveau de sûreté. Ainsi, des exercices sont réalisés sur une base annuelle et un retour d'expérience est réalisé et envoyé aux autorités nationales belges. Parmi les exercices pluri-acteurs de grande ampleur réalisés chaque année dans le port d'Anvers, on peut ainsi citer *Flash Fire* (2010), *Winterwatch* (2011) ou encore *Black Wolves* (2014). En complément de ces exercices variés, des outils créatifs accompagnent les *guidelines* officielles, notamment le *European handbook of maritime security exercises and drills* (*Exercitium*) de la Commission européenne. C'est notamment le cas dans le port d'Anvers où a été développé un moyen ludique d'appréhender l'environnement complexe et technique de ses infrastructures par l'intermédiaire de la réalité virtuelle et d'un *serious game* : le *Port of Antwerp security game*.

La sûreté portuaire est un enjeu de chaque instant, réclamant des moyens variés, capables de prévenir en amont et d'appréhender en aval la survenance du risque terroriste et criminel. Dans un contexte tendu et dans un environnement stratégique comme celui que constitue le port d'Anvers, la sûreté maritime ne peut être que l'affaire de tous et ne saurait être gérée qu'en réelle intelligence entre le secteur privé et la force publique.

English translation

"*Maritime and port security: public interest or private business?*" During the conference chaired by Laurent GALY, four international participants from the public and private sector both presented their point of view on the subject: M. Chris TRELAWANY, Special Adviser to IMO's Secretary General, M. Christophe CLARAMUNT, Professor and Director of the IRENav (French Naval Academy Research Institute), M. Hussein Mowlid ADEN, Director in Djibouti Ports and Free Zone Authority and Ms. Kathy DUA, Port of Antwerp Safety Consultant. "What is the role of private organizations in the management of security? Should States be sovereign on these aspects?" This report presents both syntheses of the conference (I) and participant by participant (II).

III) Maritime and port security: public interest or private business?

Security, which means preventing malevolent acts, is implemented on several levels in the maritime field and ports: the ship, the port and its infrastructures. Cyber-criminality is added to other

threats such as terrorism, piracy and various traffics. Around one cyber-attack is revealed each week. In the aftermaths of 09/11, maritime and port industries have considered safety as a major concern. Thus, IMO, which implements security of shipping, defines in 2003 in its IPSP Code the responsibilities of the public and private actors in the field of navigation and port safety.

Maritime and port fields level unique security stakes. Due to economic and geopolitical reasons, security threats are a major stake. In fact, hampering ports and shipping should have major effects on States and their economies due to the role of shipping in their economies. Besides, the relative isolation of ships at sea involves them furthermore to these topics.

Maritime and port security is first of the States' responsibility due to their sovereign mission of guarantee of public order. The implementation of security allows to struggle against criminality in general and needs for collaboration of various services of the State such as port State inspectors and police. Security is also of public interest because of the major role that shipping had in the economy of a country. For instance, 78% of the GDP of Djibouti comes from its port activities.

States gather to implement maritime and port security at the international level. IMO is the place for international cooperation in that field. Besides the ISPS Code, which implements security for ships and port infrastructures (security plans, inspections), IMO also develops security through Codes of conduct for regions impacted by piracy. An example is Djibouti Code of conduct, which contributes to struggle against actions of pirates from Somalia.

Security is also implemented by the cooperation of public authorities at the regional, national and local levels. In the European Union, States are inspected by the European Commission, which verifies the good implementation of the ISPS Code, publishes reports with recommendations and sometimes fines. For instance, the commission inspected the port of Antwerp in 2007: it deemed efficient its safety system for oceanic terminals but underlined the need for a security plan for the entire zone. States have a key role especially due to their means (sovereignty, financial, legal), to their role of inspection of local systems and thanks to collaborations that they can build. In 2012, for instance, Djibouti created its national coastguards, with the cooperation with the US Coast Guards. At the local scale, ports also have an important responsibility in the implementation of safety.

Security topics directly threaten maritime and port activities. It is also a private business due to its economic stakes: private stakeholders have a major role to play in the implementation of security. Djibouti's port activities are, for instance, currently threatened by maritime terrorism, traffics (drugs, weapons, human beings) and illegal immigration. The ISPS Code puts in place, for instance, security plans that maritime companies must write, implement and tried out. Private initiatives can also be proved essential in the implementation of security. In Antwerp, for instance, public-private forums are held every year thanks to a private initiative (think-tank and members of the civil society).

Security procedures and measures must not slow down the economic activity. Thus, for instance, it would be unthinkable to fence the port of Antwerp for security reasons since 409 km of public roads cross the 130 km2 of the infrastructure.

Private players must cooperate with the public players for the implementation of security. In the field of cyber threats, for instance, initiatives of formation implemented by the chair of cyber-defence of naval systems are developed in cooperation between industrial companies (DCNS, Thales) and State structures (Naval Academy, CO Cyber, DGA…). Another example: following an audit of the European commission of 2007, the authorities of the port of Antwerp have begun a close cooperation with safety services. Belgian local security committees gather authorities from the port, the maritime police, the local police, safety teams and users. Also, public and private players work together within an information network that collects remarks on unusual events. They participate in joint formations and exercises.

To conclude, maritime and port security is both public and private players' business and interest. The efficiency of the implementation of security is thus depending on the cooperation of those actors. In order to face major threats, the current international challenge for security is the application of the ISPS Code and the harmonization of safety and security standards (FAL Convention of IMO). The formation of public and private players remains a major stake.

IV) Syntheses of the participants

- **The approach to maritime security – Chris TRELAWNY**

IMO (International Maritime Organisation) is a specialized agency of the United Nations created in 1948 in order to deal about maritime issues. In a nutshell, IMO's motto is "*safe, secure and efficient shipping on clean oceans*". This definition shows the two main aspects of this organisation: safer shipping and cleaner oceans. In order to reach this goal, especially in safety and security, IMO has developed some conventions that deal with specifics points. The most famous are the Load Lines (which deals about safety of merchandises), the MARPOL (on maritime pollution), and especially the SOLAS (International Convention for the Safety of Life at Sea), which includes security items and charge public and private actors with responsibilities on shipping and port security. Specials measures are reinforced by the ISPS Code (adopted in 2003, in the aftermaths of the 9/11). IMO is funded by flag State. Panama is thus the biggest contributor to this international organization, because it gives 17% of its global budget.

With all these conventions, IMO contributes to abolish piracy in three regions: Somalia with Djibouti Code of Conduct, Gulf of Guinea with another Code of Conduct and in South-East Asia with the ReCAAP (Regional Cooperation Agreement on Combating Piracy and Armed Robbery against Ships in Asia). IMO has also played an active role in struggling against migrants' traffics.

Maritime issues have changed between 2004 and today. Threats have evolved: piracy and armed robbery have fallen while cyber-attacks, terrorism, wildlife affect and illegals traffics have increased. Also, sustainable development is new issue and prevention against terrorism has grown better. Ports create wealth. Port safety is both efficient and effective.

However, there is a huge challenge for maritime safety and security: the need for a cooperation between the ports players – public and private actors, national, regional and international actors. The aim is to succeed in harmonising standards and norms, best practices and to build a real cooperation. The FAL Convention (Convention on facilitation of International Maritime Traffic), adopted in 1965 (which came into force in 1967 and soon amended by the FAL 40 in 2017; theses amendments will come into force in 2018), is the best tool of IMO in that field. Its goal is to improve harmonization and simplify procedures and documentation used for international shipping. But to reach this goal, practices must be improved, especially through "win-win concessions". Moreover, the ISPS Code must be promoted and implemented.

To conclude, it is essential for every players of port activities to help for expansion, with more cooperation and improve security and safety, which include struggle against traffic and corruption. We need more standardization, more training. Aerial sector is the best model for possible enhancement.

- **The Cybersecurity applied to maritime field – Christophe CLARAMUNT**

We can see in our modern societies a progressive extent of the use of computers and automatics and in industry in particular. That extend go with a general spreading of malevolent software, forming up an exploding threat for last years. In 2007, synchronised devastating attacks in Estonia against official sites, media, bank system is a clear step into cyber-warfare era. Then in 2010, Stuxnet virus destroyed centrifuges of the Iranian programme for uranium enrichment. This is another huge step into attacks by Advanced Persistent Threats (APT), able to target industrial objectives, such as SCADA systems (Supervisory Control and Data Acquisition for industrial automatons). Theses APTs implement complex and specific architectures of attacks, written in planned strategy and conducted in long lasting time. And today, there are no more weeks without big scale cyber attack reported in media.

France is conscious of theses threats, at political level (Bockel Report 2012), at strategic level (Strategic Defence and Security Reviews (*Livre Blanc*) of 2008 and 2013), at joint level… Chief of Defence Staff considers cyberspace to be the 5th warfare environment after land, air, sea and space and this global warfare is carried out by the Cyber General Officer in Strategic Joint Headquarters (CPCO in Paris Balard). In this framework were created Cyber-defence of Naval Systems chair, but also many education initiatives, partnership with academies (Naval Academy, Telecom-Bretagne…) and industry actors (DCNS, Thales). French State is committed with new and reinforced structures such as Cyber

Command, Armed Forces Services Headquarters, DGA (delegation for armament), ANSSI (National Agency for Security of Information Systems), CALID (Analysis Centre for Cyber-defence)…

Maritime actors are especially sensible to cyber threat, due to geopolitics and business concerns. In addition, maritime world is very vulnerable: ships at sea are partially isolated, with limited crews and more and more complex technologies aboard, controlling almost all the ship's functions and some of the more vitals (navigation, engines, weapons systems for warships). Theses systems are quickly deprecated (on average one ship's life lasts 30 years), leaving the ship more vulnerable faced to the constant development of the cyber threat. More than ships, it is also a whole ecosystem of ports, harbours, oil and marine renewable power infrastructures that can be targeted. All the situations caused by human actions, mistakes, failures can be provoked by cyber-attacks (missile launching, load ripping, collision, grounding, oil spill…), with human consequences (passenger ships), and other damages.

Cyberspace is physical, logical and social. Threats really exist and come from States, enterprises, criminal or terrorist organisations, hackers. This cyber-war is included in a global information war that covers military and industrial intelligence, psyops… Organisations are more and more targeted. APT are developing.

To be secured, a system needs to guarantee availability of its service, integrity of information and confidentiality of its secrets. Security policies are technical and non-technical (physical protection, organisation, human considerations).

Cyber-security is composed of cyber-protection (protection to prevent attacks), cyber-defence (detection, adaptation, response) and cyber-resilience (continuation of mission).

In this very complex framework, Naval Systems Cyber-defence chair conducts research around issues like SCADA, real-time, sensors, AIS signals.

Cyber, in spite of appearing nebulous to seafarers, is now completely integrated in their work environment. Cyber-security has become a significant base for safety, and for security as well.

- **From French enclave to Strategic crossways: The prominence of Djibouti in the Horn of Africa – Hussein Mowlid ADEN**

Since 2008, Djibouti port facilities have welcomed and furnished a set of services to more than 300 navy ships per year. Regarding the extension of the only US African-based permanent base and the current re-settling of the French navy, Djibouti became an international hub involving new cooperation methods. The last opening of the IMO funded centre for regional maritime activities underlines the importance of Djibouti for the international community.

Djibouti is now in a capacity growing process regarding its maritime infrastructures. Both the Djibouti Port Administration and the free zone authority are looing closely to these activities that would enhance the leading role of the Port in the region.

Djibouti is also a port of importance because of its commercial activities. As a former French colony, a major part of its existing infrastructures are coming from this heritage. Moreover, Djibouti is situated in a strategic crossway between many routes linking Europe, Asia and Eastern Africa. 78% of Djibouti's GDP is related to port activities. The existing infrastructures are the port, a free zone, an oil terminal and a container terminal.

Since 2009 Djibouti represents a world-ranked hub and is continuously increasing its commercial traffic. Between 2009 and 2015, we can notice an obvious increase in trade particularly in the field of containers. Between 2008 and 2015, more than 40 navies used Djibouti port facilities within the framework of trade securing in this strategic area.

The Republic of Djibouti is widening its port and maritime infrastructures. The Djibouti Port Administration and the Free Zone Authority are keeping an eye on these developments and will ensure the compliance with international rules.

In the medium and long term, Djibouti plans several new infrastructure projects for a total of 40 billion US dollars: a gigantic and quite ambitious project built on many sites all over the bay, on a

great part of the coastline and in the inland. For instance, this project plans the building of new terminals, shipyards, rail transport infrastructure and new free zones.

The port of Djibouti and its activities are currently facing various threats: maritime terrorism, which is a consequence of the weakening of the neighbouring States and the development of piracy (Somalia, Yemen), but also drug trafficking and arms dealing with Djibouti as crossroads to Europe and Asia.

Because of its strategic situation on the coastline, Djibouti is also a central point for human beings trafficking. Djibouti's backcountry is synonymous with an influx of migrants from Africa in direction of the Arabic Peninsula and Europe.

The government of Djibouti focuses its maritime policy on security, safety and marine environment. As a matter of facts, Djibouti has ratified most of international agreements such as the SOLAS convention or the ISPS Code. The compliance with international standards remains key for this State, which wants to make trade as easy as possible. This led to the creation of national coastguards four years ago, in collaboration with US Coast Guards. Djibouti is also an important operational centre of the international fighting system against piracy, which is warning but still rife in the region.

Djibouti and the rest of the continent need regional and international cooperation between private and public actors for the establishment of security measures. National security plans submitted by Djibouti every year are revised and put into place with the support of the US Coast Guards, particularly for the training of port safety personnel. The cost of safety is very high. The part of safety spent in Djibouti is 2 to 3%, higher than in most other African States. The investment proves to be key because an ineffective safety would have serious economic consequences for this country.

In view of the current economic situation and budget cuts, questionings remain: who should pay? Should recipients or economic operators pay? Should we consider it as public service or as national safety measures?

- **Public-private Partnership in Port Security, Kathy DUA**

Mrs Kathy DUA, security and safety consultant for the port of Antwerp introduced the original security management of this huge 130km^2 for 163km of quay infrastructure. For obvious economic and efficiency reasons, turning a port into a closed zone seems impossible and quite unrealistic. In fact, 409km public roads cross the port area.

The security plan of the port of Antwerp was designed in a narrow partnership between the port authorities and both the users and the public services. Since 2004, ship captains have the responsibility of the implementation of the ISPS Code requirements. But a real security strategy was expected from port authorities and port State both: the port security plan (PSP) was a crucial step in Belgium in order to fight against diverse threats, from criminal activities to terrorism. The speaker and the audience underlined the responsibility of the State in the prevention of radicalization phenomena. This public-private partnership has been fostered by the "National Authority – Maritime Safety", which conducts maritime safety policies backed for this by various administrations (Defence, Environment, Foreign affairs, etc.). This policy is conduced by the "Local Committees – Maritime Safety", gathering port authorities, maritime police, local police, security teams and users (dockers, captains, owners etc.)

Every year, public-private forums, initiated by think-thanks and the civil society gather federal judicial police, task forces, attorneys and seamen to discuss port security and specific measures for Antwerp issues. Such initiatives enlighten the tremendous need in the sea world for complementarity between the three levels of security (ship security, port facilities security, port security). ISPS Code chimes plainly in this path. However, despite the multi-actor cooperation and the procedures and specific measures of the port, State must remain the milestone of port security. That is the vision of security in the port of Antwerp.

Innovative systems have been implemented in the port. The *port information network* is one among many examples. This system is a common online platform for port authorities, users and public forces centralizing reports of unusual observations by everybody noticed everywhere in the port zone.

The joint formation for public and private actors to create common values and reflexes is absolutely necessary to ensure a high standard security level. Then, large-scale exercises are implemented each year in the port (*Flash Fire* in 2010, *Winterwatch* in 2011, *Black Wolves* in 2014…). Experience reports are systematically addressed to national authorities.

Complementarily, additional to official guidelines including the European Commission *European handbook of maritime security exercises and drills (Exercitium)*, the port of Antwerp has developed video-ludic instruments to apprehend a complex and technical environment: the very serious game « Port of Antwerp security game » is a unique way to do it.

Port security is a constant challenge that needs various supports, encompassing both prevention *ex ante* and a capability to manage terrorist and criminal occurrences *ex post*. In a fiery security context, in a strategic environment as the port of Antwerp, maritime security must be a common work. There is a need for a well-balanced intelligence involving the private sector and public services.