MARITIME SURVEILLANCE IN SUPPORT OF CSDP

THE WISE PEN TEAM FINAL REPORT TO EDA STEERING BOARD

The Wise Pen Team:
Vice Admirals Fernando del Pozo, Anthony Dymock, Lutz Feldt, Patrick Hebrard,
Ferdinando Sanfelice di Monteforte
26 April 2010

MARITIME SURVEILLANCE IN SUPPORT OF CSDP
THE WISE PEN FINAL REPORT TO EDA STEERING BOARD

Table of Contents

Executive Summary.

More information is being generated and exchanged more quickly and more official information is becoming more accessible to the public than ever before, but the traditional nature of navies and the shipping industry has caused them to lag behind these developments in respect of surveillance information. Increasing maritime insecurity, not least terrorism, piracy and illegal immigration, has highlighted the need to improve European security by integrating maritime policy making, sharing information more effectively and transparently and coordinating a collective response to security challenges. Many useful initiatives are already underway, but there is the need to make graduated improvements in co-ordination and integration which are affordable and not technologically difficult. Information sharing is the key and the obstacles to it are essentially cultural and organisational. If the evident political will at the top and developing enthusiasm at the coalface can be complemented by more cooperative action by middle management there is great potential for some early wins.

Definitions. Confusion and competition continue because of a lack of agreed definitions of even basic terms like safety and security. People are talking past each other. Annex A offers clarity but an EU champion is required to get some vital working definitions accepted. We suggest DG MARE.

Cooperation. "Round Table" groups of stakeholders are required at various levels to raise awareness, create understanding, develop trust, build linkages and improve effectiveness. Existing informal forums like CHENS and the North Atlantic Coastguard Forum can be expanded.

Navies. Suspicion remains, but the MSSIS system has been transformed from its initial American military roots to a genuinely open global system (currently over 60 subscribers) to which agencies like EMSA could usefully subscribe. Navies need to change secretive habits and join in too, not just as consumers, but as providers, for which they are well equipped.

Schengen. By comparison with trucks and aircraft, ships get a bad deal from Schengen, due to the conflicting requirements of the Maritime Law Enforcement Agencies. The ongoing work in the Commission might provide a solution to this difficulty.

Active Surveillance. Over 90% of current ship data relies on the ships co-operating and transmitting. Small and illegal vessels currently escape detection. More terrestrial and satellite-based radar, electro-optic, and infra red monitoring is required at key nodes such as straits, ports and nuclear installations. Naval units can provide deployable capabilities.

Stakeholders involvement. A greater involvement of all stakeholders, navies very much included, in collection, collation and distribution of maritime surveillance elements, is required for a real improvement of EU Maritime Domain Awareness (MDA).

Governance. SOLAS, IALA, & IMO show that governance models exist for international maritime cooperation without succumbing to deadlock over legal or sovereignty issues. Governance in maritime surveillance can be similarly achieved by agreeing delegated authorities and responsibilities.

Coastguard. The time is not yet ripe for an EU Coastguard, but elements of the same functionality can be delivered by virtual means. Further advances in realising virtual coastguard functions will emerge naturally as projects already in train, such as e-borders, e-maritime, e-customs, etc., become operational. DG MARE would appear to be best placed to identify and promote the potential synergies.

Architecture. Thanks to the internet and related developments, distributing and protecting data has made the goal of an affordable, COTS based, service-oriented, loosely-coupled federation of systems readily achievable. Indeed it is already evolving through AIS-LRIT-STIRES; SafeSeaNet-IALANET; EU NAVFOR *Atalanta*'s *Mercury* and unifying tools like the EDA's Common Standard User Interface (CSUI), which are ideally suited to handling the complexities of information sharing and synthesising by different authorities for different purposes at different levels.

Protection of Information. Although it is widely understood that the "need to know" principle needs to be replaced by *the need to share*, in practice risk aversion still prevents this happening and a *responsibility to provide* obligation is needed to redress the balance. A Commission directive is required to clarify real and perceived data protection constraints and to remove those that are legally perverse or counterproductive to European security.

Data, Information, Knowledge. A three layer construct facilitates clarity of ownership, protection and distribution providing that the key principle is observed that the "need to share" must replace the "need to know" in a service oriented "federation of systems" approach.

Preferred Approach. The preferred approach is regional. Maritime surveillance is a continuous worldwide process whereas action in response to it tends to be local or regional. The global *white picture* network (see para 78) must therefore be capable of more detailed enlargement for regional level mission purposes. Progressive implementation should permit information and intelligence exchange by first connecting National Maritime Coordination Centres NMCCs through MARSUR on a by request basis, second, developing these exchanges at regional level, and, in the final phase, the RCC would assume the predominant coordinating role.

Any meaningful improvement in maritime surveillance will depend upon a step change in attitudes towards information sharing. Such a change may be driven in part by legislative amendment led by the Commission but chiefly by cultural change at the individual and collective level in Member States and EU agencies. Such cultural change requires leadership, examples of best practice, confidence building initiatives and, ultimately, sanction in the case of conspicuous failure in the responsibility to provide

information of a critical or life-threatening kind. This cannot be allowed to wait for a disaster to precipitate changes for which the need is already evident.

I. Introduction: Trends in the Economy and Maritime Security Context.

It is a very sad thing that nowadays there is so little useless information.
Oscar Wilde, 1894.

1. Despite the recession, the long term expansion, scale and importance of maritime trade remain clear. Seaborne trade has doubled every decade since 1945. International shipping infrastructure is massive: shipbuilding tonnage has doubled since 1990; 93,000 vessels are manned by 1.25 million seafarers trading between 8000 ports. As trade has increased so has the threat. According to the International Maritime Bureau (IMB), between 1995-2005, 3284 seafarers were held hostage; 617 were threatened on board ship; 483 were injured; 349 were killed; 208 assaulted; 112 kidnapped or held to ransom; 164 are missing presumed dead and an unknown number have suffered trauma severe enough that they will never go to sea again. If this were happening to European truck drivers ashore the popular outcry would be enormous, but shipping is out of sight and thus out of mind and compared with aviation security expenditure is minimal even though Al Qaeda is known to have attempted to infiltrate terrorists and explosives into Europe by sea.

The pirates´ booty. Bossasso, Somalia

2. MDA is the *sine qua non* of maritime security and depends on surveillance and information sharing by the international community. Current capabilities to achieve that awareness are developing but remain inadequate and poorly coordinated. The events of 9/11 and subsequent International Ship and Port Security (ISPS) Code notwithstanding, sea-blind publics are generally not aware of their vulnerabilities. Terrorism from the sea (Mumbai) and piracy (Somalia, Gulf of Guinea and the Malacca Strait) seem distant problems to most Europeans. Maritime issues resonate more strongly when they are closer to home with coastal pollution or unusually newsworthy (the MV *Arctic Sea* saga).

3. The economic recession appears to be accelerating the shrinking (in real terms at least) of European military budgets and thus naval assets and capabilities. However, as tailored military Communications and Information Systems (CIS) become less affordable, civil and military technologies are tending to converge and become more affordable. As trade volumes and maritime congestion increase at key destinations and choke points, pressure is growing to take advantage of technology now available for a more active approach to maritime traffic control in the interests of safety, security and efficiency. This need not entail positive control from ashore but greater voyage data

transparency and cooperative planning improves safety and efficiency by phasing departures, transits and arrivals, accommodating ever larger, deeper draught and thus less manoeuvrable ships, in order to reduce the likelihood of collision, pollution as well as saving money by managing fuel more economically. There will be resistance to perceived encroachment on traditional freedom of navigation and secrecy of intentions but the trend is clear and a *laisser faire* approach to incremental risk is no longer politically acceptable.

4. In open democratic societies more and more data is being made available by governments, institutions and commercial organisations both in the interests of democratic transparency and in tapping the intellectual and entrepreneurial capacity of the public – the "LINUX approach"[1]. This enables any individual with an internet connected computer to become a citizen analyst, mining and mashing data to generate information and knowledge. The maritime world, with its thousands of years of history, tradition, difficulty of communication and commercial secrecy has proved slow to adapt by comparison with a young industry such as aviation. Because landsmen are familiar with the security requirements of air travel and unfamiliar with the realities of maritime trade there is a popular but misplaced belief that similar standards of security apply.

5. The relative vulnerability of maritime transportation and sea borders represents a political hazard, if citizens' safety and security is perceived to have been neglected in the wake of some high profile accident or event. Satellites have now transformed maritime communications and navigation and in the information age security lies not in secrecy but in transparency. The maritime world is lagging behind with no technological excuse and an increasing spectrum of risk. Successive headline grabbing events are beginning to change attitudes and the maritime domain is starting to benefit from more joined-up policy making and greater transparency based on better surveillance and information sharing, but much remains to be done to fill in the gaps in surveillance coverage and to join up the fragmented information sharing communities within and amongst member states. Improvements to the maritime surveillance posture in the EU have tended to be be decided in the wake of tragedies of high visibility events, as demonstrated by the case studies posed in Annex B.

6. The second order effects of climate change and hydro carbon depletion are also now beginning to show or are in prospect with rapid and large scale encroachment of the freedom of navigation by alternative energy developments (offshore wind farms, tidal barrages) and increasing access to seabed hydrocarbons as a result of the melting icecap. Environmental and ecological concerns are also encouraging further regulation in the maritime domain and restricting access and activity in formerly open sea space. The scientific community calls for more data collection and exchange to improve their understanding of the maritime domain.

[1] This year about 1,200 exabytes of digital data will be generated globally (equivalent to 1.2 quadrillion written pages) and growing annually at 60%. International Data Corp (quoted by The Economist, Feb 27, page 5 of the Special Report on Managing Information)

7. Overall the trend in the maritime domain is clear – closer monitoring and regulation which depend upon effective surveillance and information sharing.

II. The Interim Conclusions of the Intermediate Report.

8. Although the Intermediate Report was not intended to reach definitive conclusions, some were tentatively advanced. The Team believes that *mutatis mutandis* (i.e., the references to the EU Pillars are no longer extant), they are still valid. To recapitulate:

9. There should be more exchanges between the IMP and CSDP players. This is particularly relevant for maritime surveillance, as one of the most prominent examples of the confluence of military and civilian responsibilities and fields of action.

10. Maritime surveillance is inseparable from the rest of the maritime domain. The Team has researched projects in this field, as well as current activities by the US and Canada. The EU, which controls 40% of world shipping, flags 25% of the ships and carries 90% of its external trade and 41% of its intra-community trade by sea, cannot afford to be left behind by more activist nations who are already addressing the shortcomings of the present safety and security systems. The EU risks to have standards and timetables imposed by external authorities thus closing or limiting access to important external markets.

11. The need for and fear of a monolithic and hierarchical EU system is misplaced. The proposals contained in this final report are consistent with the previously expressed idea that: "The EU´s role is that of a facilitator, establishing standards and best practice, encouraging the removal of barriers, promoting cooperation and reducing waste, duplication and thus costs".

12. The Team has been reinforced in its conviction that the basic culture underpinning the necessary exchange of information is that of the *need to share*, instead of the restrictive one of the *need to know*, which should apply more rarely when protection of the information is paramount. Unthinking or overly defensive use of this criterion should be exceptional rather than bureaucratically routine. Current attitudes and regular abuse of the principle induces unwarranted limitations in the flow of information. The *responsibility to share* lifesaving information also has to be recognised.

13. The team also took note of several initiatives and concepts that will positively influence maritime surveillance, such as the identification of national high level points of contact, and the pilot projects of regional level organisations, which are part of our recommendation of a step-by-step approach, and which are still in development today.

14. Although not included in the Interim Conclusions, the Team believes that the definitions proposed in Annex D of the Intermediate Report should be discussed at a round table and amended where necessary with the aim of achieving a set of working definitions acceptable to all concerned that replaces the present anarchic system whereby different communities develop their own definitions to fit their specific functional needs, resulting in apparent incompatibility, conflict and competition. A common understanding of a shared reference is a prerequisite for sustainable progress

towards better cooperation. This is the reason for incorporating them in this Final Report with some additions and enhanced comments based on further consultation.

III. Changes Since the Issue of the Intermediate Report.

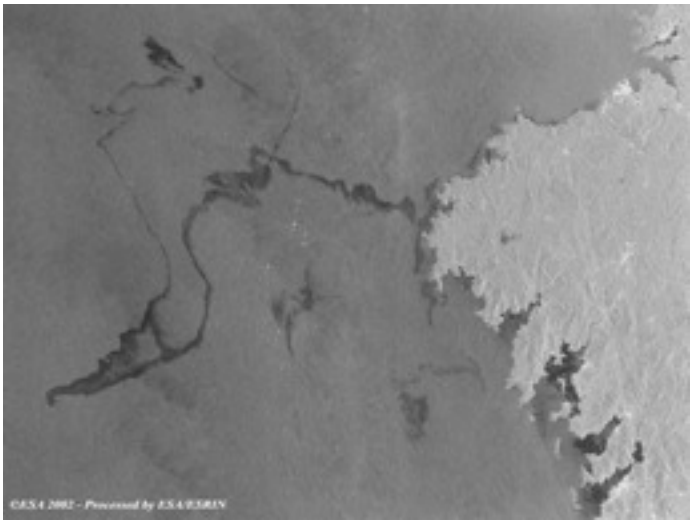
The Lisbon Treaty

15. The Lisbon Treaty came into force on 13 November 2009 when the last national ratification was deposited in Rome. The European External Action Service is being created and will incorporate the EU Military Staff and the Crisis Management and Planning Directorate has been implemented to enable the civilian and military components of the EU to take a more comprehensive and integrated approach to crisis management.

Commission Policy Documents

16. The Commission Communication "Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain" dated 15 October 2009 (COM(2009)538 final), is the cornerstone in the building of better understanding and improved maritime surveillance. It sets out the guiding principles for the integration of Maritime Surveillance by establishing a Common Information Sharing Environment (CISE) and defining the terms involved. The first principle it establishes calls for all user communities to interlink their information systems. The second is the need to establish a non-hierarchical technical framework for interoperability and future integration. The Wise Pen Team believes that these two principles will enable an enhanced sharing of information and interoperability of surveillance systems creating improved situational awareness, efficiency and cost-effectiveness.

17. The Commission also published "Integrated Maritime Policy - A Progress Report" on 15 October 2009. It covers maritime issues emphasising social, environmental and economic policy and charts progress since 2007. In its present form the IMP does not attempt to take a fully comprehensive approach to maritime policy beyond Commission competences. The limited integration achieved is nonetheless significant and the 8 chapters spell out encouraging progress in both regional and functional approaches. Maritime Surveillance is part of the IMP, and this should provide an excellent opportunity for further development.



Prestige´s oil spill, 19 November 2002

Council Decisions.

18.The Council Conclusions on the Integrated Maritime Policy, dated 16 November 2009, welcome the idea of establishing an integrated approach to maritime surveillance, through a common information sharing environment.

19.The Council Conclusions on Integration of Maritime Surveillance, dated 17 Nov 2009, took account of the Wise Pen Intermediate Report, and welcomed the Commission´s engagement in the integration of maritime surveillance through a Common Information Sharing Environment for the EU maritime domain.

Other Policy Statements

20.On 5 February 2010 the High Representative of the Union for Foreign Affairs and Security Policy reiterated some key themes relevant to maritime security at the Munich Security Conference. She emphasised that, for the EU, internal and external challenges are intertwined, that none of the threats is purely military, and that it is essential to uphold a comprehensive approach to security.

EU Presidency Activities.

21.The Swedish Presidency issued a report on 17 November 2009 on Integration of Maritime Surveillance, endorsing the idea of integrated support to maritime surveillance through the establishment of a Common Information Sharing Environment, and pointing to the need for a road-map for such development and implementation. It also called for improvement in the necessary coordination between the Commission and agencies, to increase interoperability and cooperation between existing and planned, civilian and military, systems, and to investigate the appropriate legal framework surrounding the exchange of data.

22.The Spanish Presidency, continuing their predecessor´s work in maritime surveillance, organised a Seminar in Madrid on 28-29 January 2010 with the title "Maritime Policies for a Prosperous & Secure Europe". The Seminar identified five possible elements which could strengthen maritime security in Europe: 1) a strategic view of the maritime dimension; 2) a recognition of its necessity at political and institutional level; 3) a greater understanding of the maritime domain based on information exchange, mutual confidence and political willpower; 4) a joint civilian and military approach to the solution of maritime security problems, which brings together all actors with maritime responsibilities and 5) adapting the common legal framework to facilitate this.

23.It concluded that maritime situational awareness and information exchange are key factors in developing an integrated maritime policy and in carrying out maritime security operations (detect, decide and act). The result of the integration pilot projects launched by the European Commission will be crucial to developing a fully Integrated Maritime Policy. These pilot projects have significant civilian and military components which should be catalysts in overcoming obstacles and building confidence. To be successful, the Member States, who are the main actors in maritime surveillance, must

be fully involved. The future European network for maritime surveillance will have to be established in an evolutionary way, step by step, with a decentralised and open architecture that supports higher layers of processed information and knowledge.

24. The Spanish Presidency also circulated a paper in preparation for the informal Defence Ministerial meeting in Palma de Mallorca on 23/24 February 2010, which promoted a comprehensive - civil and military - approach to addressing the current and future security needs of the maritime domain, including coordinating activities to meet the security needs of the IMP as well as CSDP missions and operations. This should overcome the current obviously inefficient structures and fragmented coordination of assets by authorities with maritime responsibilities. The Spanish Presidency proposes the establishment of a Joint Council-Commission Task Force with EDA participation, under the authority of the High Representative of the Common Foreign and Security Policy and Vice-president of the Commission, which should work on three strands identified during the Seminar: (1) to produce a Maritime Security Strategy; (2) to harmonise civilian and military developments in this field; and (3) to search the best cost-efficiency in Maritime Surveillance. This was discussed and met with favour at the Defence Ministerial meeting and should be approved in the formal Ministerial Meeting in April at Luxembourg.

Technical Agreements Developed.

25. On 25 November 2009, EMSA, Frontex and CFCA reached a Cooperation Arrangement in order "*to develop exchange of information and to foster mutual cooperation in the field of maritime surveillance, to improve protection of external maritime borders, to counter illegal/ irregular migration as well as related cross-border crime within the competence of Frontex and to increase maritime safety, maritime security and protection of the marine environment within the competence of EMSA and to enhance the organisation of operational coordination of fisheries control and inspection activities by the Member States within the competence of CFCA*".

26. The Cooperation Arrangement between three important European agencies is a first step towards operational global information exchange. Frontex and CFCA will have access to information collected by EMSA by subscribing EMSA's SafeSeaNet and possibly CleanSeaNet. The three Agencies possess quite different types of data and have to define what kind of data they intend to provide and receive – obviously EMSA has more to offer to Frontex than the other way round. There are also two pilot projects running with EMSA-Frontex-CFCA and France, Spain and Italy. The first is testing the technical feasibility of exchanging VMS (fishing vessel reporting system) information via SafeSeaNet and the other is testing the exchange of local coastal radar images via SafeSeaNet between neighbouring states. All these initiatives should be encouraged and their experiences shared with other stakeholders for mutual benefit. This kind of enabling agreement could be extended to other Agencies, such as the EU SatCen, currently providing satellite imagery data and analysis for CSDP operations and missions.

27.On 18 February 2010, EMSA signed a service level agreement with the Italian Coast Guard to provide the regional server for Automatic Identification System (AIS) for the Mediterranean.

Other Initiatives.

28.Under *Intelligence Surveillance and Enhancing Border Security*, the demonstration programme MARBORSUR of the DG Enterprise and Industry Seventh Framework Programme will soon be launched to provide a "system-of-systems" solution for border surveillance, emphasising the EU maritime extended borders, as part of the EUROSUR system. The MARBORSUR demonstrator should address the acquisition, fusion, exploitation and information sharing relevant to maritime surveillance, including all weather detection and tracking of small boats.

29.Two Pilot Projects intended to increase regional trust, information sharing and cooperation to achieve more effective preventive and enforcing actions have just been launched: BlueMassMed for the Mediterranean and MARSUNO for the Northern European sea basins.

30.The EU's first Concept of Maritime Security Operations is being drafted by the EUMS and is expected to be published in 2010.

31.NATO's Alliance Maritime Strategy has been drafted, and approval is expected in 2010.

32.EDA´s "Network Enabled Capability Synergy Campaign" will also provide significant support to Maritime Surveillance.

New Inputs from Third Parties and Other Contacts.

33.Besides the maritime surveillance systems already in place or being implemented, there are existing networks around Europe supporting maritime safety, security and defence. Most involve informal information exchange meetings with the aim of building trust and confidence.

34.Due to time constraints the Team has been unable to establish personal contact with all the different networks, but the documents and minutes provided to the Team proved that they are representing all European Member States and most of Europe's neighbouring countries.

35.CHENS is the informal group of the Chiefs of European Navies, dealing with security and defence topics. Maritime surveillance is one of their main concerns. The EUMS, NATO and US are observers, and Commanders of ongoing operations, like *Atalanta*, are represented as well.

36.The ChanCom meeting is an adaptation of the former Major NATO Channel Command, an informal meeting of the Heads of the Navies of Belgium, France, Germany, the Netherlands, the United Kingdom, MCC Northwood, EUMS and SACT. Italy, Spain and Portugal participate as observers. Maritime surveillance is also one of their topics.

37. The North Atlantic Coast Guard Forum (NACGF) is a newly (2007) established informal meeting bringing together all the northern EU Member States from France northwards, including the Baltic Sea and the United States, Canada, Iceland, Norway and Russia. Its foundation follows the useful example set by the Pacific Coast Guard Forum. The representatives are from national Coastguards and/or navies, including a strong representation from the national transport ministries. They are concerned with both safety and security aspects, and maritime surveillance is high on their informal agenda.

38. The Barcelona Process and the "5+5" Dialogue represent Mediterranean networks dealing with a variety of political and practical challenges in the Mediterranean. During a recent meeting all the coastal states agreed to establish "relay points" comparable to the National Coordination Centres established by Frontex. All 27 EU Member States and 16 Southern Mediterranean States are part of these networks.

39. The Black Sea Region - already a very important region from a safety and security point of view - a number of cooperative initiatives are taking place. The EU role, both to support MSs in the region, and to establish synergies among all initiatives undertaken (Black Sea Synergy, BLACKSEAFOR, Black Sea Harmony, Black Sea Littoral States Border/Coast Guard Cooperation Forum, etc.), by fostering dialogue with all the major non-EU regional stakeholders, will be essential.

40. The Virtual Regional Maritime Traffic Centre (V-RMTC) is an established and proven network for Maritime Surveillance. It is a virtual network linking the operations centres of all participating navies providing unclassified information on merchant ships over 300 ton, a significant achievement for safety and security in the Mediterranean Sea. The suggestion that this should be linked with the 5+5 Dialog is encouraging and must be supported.

41. During our visits to the United States, Canada and Allied Command Transformation, NATO´s think-tank in Norfolk, we identified many problems, concerns and obstacles in common. But the potential solutions have much in common too, therefore a strong and open exchange of experiences is vital. We are convinced that this is achievable and the involvement of the United States in some of the above mentioned informal meetings could be appropriate. This also applies particularly to Canada as much progress has been achieved in maritime surveillance following a comprehensive approach developed under naval chairmanship.

42. The relationship with the Russian Federation is vital because Russia is a neighbour in the North Atlantic, the Baltic Sea and the Black Sea. She is open to coordination and there is already a first link established in the Baltic Sea.

43. Turkey similarly is a very important neighbour, and its coordination and cooperation are vital to achieve efficient safety, security and defence.

44. We have selected these important networks, in the knowledge that there are many other existing bilateral and multilateral, informal and formal networks, as being the most relevant from the Maritime Surveillance perspective.

Operations.

45. Although the anti-piracy operations *Atalanta* and *Ocean Shield* continue to contain piracy off the Horn of Africa, incidents still occur, and in yet increasing overall numbers. However, the number of successful attempts at boarding has been much reduced relative to the number of total attempts, and piracy is increasingly being displaced from the easier to watch Gulf of Aden to the Eastern coast, and further from the main shipping lanes[2]. Such displacement of localised piracy to dispersed oceanic activity underlines the importance of a comprehensive approach and full situational awareness. There is a widening understanding that anti piracy measures need to be more than just maritime security, as all maritime piracy begins and ends on land a comprehensive approach is vital. The beneficial by-products of better information sharing and cooperating with non traditional partners such as Russia, Japan and China continue to be apparent.

Wise Pen Activity.

46. Since the last report we have continued our programme of research and exploratory visits such as to EuroControl in Brussels, the International Association of Lighthouse Authorities (IALA) and *l´Etat Major de la Marine Nationale* in Paris, the Center for Naval Analyses in Washington, the Volpe Transportation Security Research Center in Boston, the Canadian Coast Guard Headquarters in Halifax, and several German establishments in Berlin, Hamburg and Cuxhaven. We have also encouraged and facilitated contacts and discussions between relevant but unfamiliar stakeholders. We have also visited capitals to look more closely at the different approaches Member States are taking towards improving the integration of maritime surveillance. This involved in Paris a unique set of relationships between MOD, Navy, *Secrétariat Général de la Mer*, and the *Préfet Maritime*; and in Washington the span included the Pentagon, Joint Staff, USN,

[2] The number of "successful" attacks (ending in highjack) in 2009 has been reduced in the Gulf of Aden, although overall has remained in the same figure than in 2008. Meanwhile, the total number of attempts has multiplied by 1,84. Nearly all this considerable increase has happened in the far less navigated East Coast area, where the total number of incidents have multiplied by more than four times the previous year´s figure.

NSC, State Dept, Intelligence Community and the Department for Homeland Security. Our visit to Halifax revealed an advanced level of integration achieved quite quickly, whereas our visits to Berlin, Hamburg and Cuxhaven showed the very real practical constitutional difficulties confronting the newly collocated federal and local agencies attempting to integrate their maritime defence, security and safety activity.

47. We have continued to enjoy regular dialogue with stakeholders of the EU Commission, led by RELEX and DG MARE, and the Council (DG8/9/CMPD/EUMS/EUMC). Our dialogue with NATO deepened in Norfolk in strategy and policy discussions with ACT and the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE).

48. Industry remains engaged in maritime surveillance related research and systems integration. Thales, EADS, SAAB, SELEX-SI, INDRA have all briefed the WP team on their current thinking, although BAE was unable to attend. The EDA expects to take IBM's development work on CSUI forward to the prototype stage. We welcome this.

49. We have also talked to the European Shipowners' Association (ECSA), national lighthouse authorities (Trinity House) and front line civilian operators such the Port of London Authority and Dover Coastguard. All would welcome more joined up maritime surveillance but are apprehensive about the extra costs being borne by them at a time of particular financial stringency.

50. Taking the opportunity of already travelling in Southern Asia region, one member of the Wise Pen Team visited the Singapore Maritime Security Centre (SMSC), for a presentation on the International Fusion Centre (IFC), the Regional Cooperation Agreement on Combating Piracy and Armed Robbery (ReCAAP) and the Malaysian Maritime Enforcement Agency (MMEA), the Malaysian Coasts Guard and the International Chamber of Commerce International Maritime Bureau (ICC-IMB), a non-profit making organisation acting as a focal point in the fight against all types of maritime crime. Some European countries are among the 25 members sharing information with the IFC: United Kingdom, Italy, and France (with a liaison officer). The Netherlands and Denmark expect to join soon, as does NATO. EU might decide to join IFC too.

Assessment.

51. The themes have been consistent and international will to strengthen maritime security continues to increase. Although threats to security and illegal activities such as piracy, trafficking and maritime related crime continue to proliferate, the awareness of the need for information sharing has also increased markedly since our work started. A variety of initiatives are under way to improve surveillance systems and associated networks. However in the absence of clearer incentives and sanctions it would seem that rhetoric still tends to outrun practice in information sharing. If the current secretive, risk avoiding culture is to be transformed into a more transparent and cooperative risk management one, authorities will have to be delegated to a lower level, the responsibility to provide made clearer, and suitable mechanisms developed to reward

good and discourage bad behaviour. As high level exhortation alone does not seem to be working, and the acute sensitivity to perceived legal constraints persists, a review of what truly constitutes commercially sensitive information is probably required. Once identified, a reliable system of access control will be needed to prevent uncontrolled processing of economically sensitive data belonging to companies operating in a market environment.

52. On the other hand, the protection by officials of allegedly very sensitive commercial information can be overdone by being more protective and conservative than the "protected" actors desire or expect. The European Shipowners' Association, for instance, like the shipowners cooperating in the *Atalanta* OHQ showed a very open and positive reaction towards the prospects of wider use of their ships´ data for security purposes, contrary to the belief of some officials. In fact, Maritime Surveillance cannot be effective as long as some stakeholders are either kept out or opposing it.

IV. Maritime Surveillance. Its Aims and Purposes.

Everything can be found at sea, according to the spirit of your quest.
Joseph Conrad.

Global Aspects.

53. The character of the seas has changed. From being an open space where freedom was the rule, the seas have become a shared, common "good" for humanity, vast but fragile and needing worldwide management and protection. The EU has responsibility for around 14,500,000 sq km of sea and 70,000 km of coast. The need for regulation and control of the seas has increased for environmental, economic, safety and security reasons. It is in the interests of both the Member States and of the EU to fulfil the work set out in the IMP, to broaden its approach, and to define an integrated civil/military policy for the sea in order to protect the EU maritime domain and interests from damaging issues, risks and threats. Maritime surveillance is the cornerstone of this policy.

Knowledge of the Maritime Domain.

54. Scientists, regulators and commercial bodies need reliable observations and data if they are to contribute towards a sustainable development of the maritime economy. Each country's Territorial Waters or Exclusive Economic Zone are part of a dynamic global system connected by shifting winds, seasonal currents and migrating species. "Analysis of the processes that govern the present state and future behaviour of these waters cannot rely exclusively on data collected within that country's own jurisdiction. Cooperation across borders is needed. Since atmospheric processes influence ocean currents which, in turn, influence the diversity and distribution of marine organisms, thus impacting fishing practices and exerting an influence on ecosystem health, scientists working in different domains need to have access to and understand data collected and distributed by colleagues from other disciplines including marine and atmospheric chemistry, biology, physics, and marine geology."[3] Navies also have a long established interest in such oceanographic data for submarine and anti-submarine warfare.

Fishing and Leisure Vessels

55. Many thousands of fishing and pleasure craft operate in EU waters. Fishing vessels over 15m belonging to EU MSs are monitored within the EU through VMS, and also outside European waters when engaged in certain fisheries, but smaller fishing vessels of less than 15m in length have no obligation to report. At present in the EU, unlike Singapore for instance[4], privately owned leisure craft are rarely subject to reporting controls, although this may change under the e-borders initiative. Although fishing and

[3] SEC 499, 7 April 2009

[4] Singapore claims a white picture of the Malacca Strait and harbour approaches containing up to 95% of the total traffic.

leisure vessels may become a safety concern in busy shipping lanes such as the Channel or Kattegat and they are less frequently a security problem, they can also be involved in criminal activities. It is essential, therefore, to be able to confirm the identity of all contacts at sea, in order to enhance overall security.

General Traffic

56. Almost 95% of world trade is transported by sea, 25% of it by ships flying European flags, and up to 40% are controlled by European companies. In addition, there are many smaller vessels not subject to formal controls. The majority of merchant vessels are from open registries (so called "flags of convenience"). Many are owned by European entrepreneurs and the beneficial ownership of a significant portion of others is difficult to establish and thus their compliance with international safety and security standards cannot be always be assured.

57. In general, open registry ships "are possibly the most independent objects on earth, many of them without allegiances of any kind, frequently changing their identity and assuming whatever nationality – or ´flag´ – that allows them to proceed as they please"[5]. "The result has been to place the oceans increasingly beyond governmental control. For public consumption, the officials still talk bravely about the impact of new regulations and the promise of technology, but in private many admit that it is chaos, not control, that is on the rise"[6].

58. This trend creates potential problems of environmental threats and of illegal and criminal activities, because control by the flag state is ineffective or non-existent. The possible terrorist exploitation of merchant vessels to inflict damage and losses on other nations is worth emphasising as a potentially catastrophic threat, because the main characteristic of maritime transport is its ability to carry very large amounts of cargo in a single voyage to large centres of population.

59. As international maritime trade is carried out throughout the world, European-flagged or European-owned vessels are also spread all over the globe. In addition, in many MSs there are significant maritime activities besides trade, such as fishing, tourism, scientific research and exploitation of the sea bed. There is an understandable tension between exploitation, commercial interests and information sharing. The fact that these activities

---

5 W. LANGEWIESCHE. *The Outlaw Sea*. North Point Press, NY, 2004, page 4.

6 Ibid. pages 7-8.

are not confined to European territorial waters or EEZ, but also occur in distant waters, presents their flag states with significant problems of protection and control. Europe cannot therefore establish a Maritime Surveillance system closed to any exchange of data with the outer world.

Illegal Traffic

60. Illegal trafficking can be carried out by merchant ships or small vessels, and both are difficult to detect whether conducting illegal migration, narcotics trafficking or the smuggling of arms and other goods. In the EU, Frontex is responsible for tackling illegal migration by sea, which in 2008 involved approximately 100,000 people, mainly transiting on small vessels over quite long distances e.g. between Tarabulus and Sicily, or between Senegal and the Canary islands.

61. Narcotics trafficking requires different techniques, e.g. transferring the cargo two or three times between different ships before the final destination. Fishing vessels, yachts, speed boats, merchant vessels and even submarines are used.

In Summary.

62. With increasingly overlapping activities, with so many risks and threats hiding among regular business, maritime surveillance is becoming more and more a necessity which requires the participation of all stakeholders for mutual benefit.

V. Navies' Contribution to Maritime Surveillance

All matters connected with the sea tend to have, in a greater or less degree, a distinctly specialized character, due to the unfamiliarity which the sea, as a scene of action, has for the mass of mankind.
Alfred Thayer Mahan

63. In such a complex and disturbed context, the first aim of maritime surveillance is to help establish a picture of who's who. Navies have many capabilities to offer, from submarines to satellites, from expertise to data and networking systems. Maritime forces can provide valuable support to EU and national civilian agencies and, where appropriate, conduct routine or contingency maritime security and safety operations.

64. Naval forces have always played an important role in maritime security in general and counter piracy efforts in particular. Apart from warfighting - along with diplomacy, deterrence and forward presence - one of the main roles of a navy has always been to protect merchant shipping and the economic interests of a country. Today some view anti-piracy and other maritime security operations as fundamentally international law enforcement missions carried out with military assets. But even for those nations with coast guards, which have traditionally undertaken constabulary duties at sea, the line between the functions of a navy and a coast guard has been blurred. Most commentators agree that navies should play a broader role in countering piracy and in maritime security operations.

65. This trend can be expected to continue with more effective means but in a more complex landscape. Pirates and terrorists have, for the moment, replaced traditional raiders, but the threats still have to be faced globally. Consequently however civilian responsibilities are apportioned, navies will continue to develop their capacity to track vessels at sea for defence and security purposes. Some experts estimate that currently 10-15% of maritime activity is illegal. Navies and coast guards are complementary and demarcation should not be a matter of dispute as a solution can easily be found by agreeing *supporting/supported* relationships appropriate to the task in hand.

66. Within the EU, navies' involvement in maritime surveillance and security differs from state to state for geographical, historical or legal reasons. In some countries, like Sweden, navies have a limited role in home waters, in others, like France, the Navy is predominant with 25% of annual activity devoted to such missions. This does not imply that navies should necessarily be the predominant actor, but that they should be considered significant stakeholders in maritime surveillance in the interests of efficiency and cost effectiveness in the provision and use of maritime assets.

67. Naval missions encompass the full range of military operations in both blue (deep sea) and territorial waters. They are able to make a very substantial and multi-faceted contribution to EU Maritime surveillance and MDA through:

- Information and intelligence gathering by deployed naval forces and other assets;

- Global command, control and communication networks linking tactical units and operational headquarters with national interagency maritime stakeholders, regional organisations and EU agencies;
- Established security cooperation initiatives including personnel exchange and training programmes;
- Extensive combined exercise programmes focused on maritime security.

Some navies also have assets dedicated full-time to maritime surveillance, fisheries control, and anti-pollution or law enforcement missions. Some also participate routinely in scientific programmes at sea. They remain committed to national maritime security while exploring new and innovative technologies and removing impediments to broader policy initiatives.

68. One of the standing functions of a maritime operation centre is to detect anomalous or suspicious behaviour that may indicate a potential threat. Accurately assessing trends and anomalies requires experience and knowledge. Naval ability to locate, track and anticipate the actions of an adversary is unique and would be of great support to MDA. Even if not directly co-located with their naval equivalents, civilian maritime operations centres must have a close relationship and permanent links in place with them. Several European countries, such as the UK and Italy, have established their National Interagency Maritime Information Centre within the Navy Maritime Command Centre. This collocation ensures better coordination and more cost effective use of maritime patrol assets.

69. Navies can also be helpful in improving trust and cooperation with non-EU countries, as they are experienced in managing joint maritime operations and developing multi-lateral cooperation and exercise programmes. They are able to share information and intelligence at all classification levels with appropriate partners. They can also offer valuable training and formation to third countries wishing to create or develop their maritime surveillance capability. The experience of Maritime HQs in organising training and exercises can provide the essential backbone for preparing and conducting interagency and multinational exercises.

70. Naval task forces are frequently deployed for deterrence or maritime control purposes. Navies can provide SAR coverage and law enforcement in blue waters. A police

mandate can be given to the Commanding Officers of a warship or MPA, as already happens in some navies. To tackle terrorism or even drug smugglers, powerful assets such as shipborne helicopters, marines and high speed craft may be necessary, and, in such “high end of the spectrum” cases, joint training is crucial.

71. The case for formulating a *strategic* level requirement for maritime surveillance knowledge to be displayed or accessed has yet to be made. At the *operational* level, however, it has already been agreed that the EU could be required to provide an OHQ for limited civilian or military missions. To date such missions have been land orientated but it is possible that a future mission could have a maritime dimension in which case the EU Ops Centre would need to be able to display and access maritime surveillance product as part of the requirement to plan, monitor and conduct a Crisis Management Operation. The Ops Centre's current support tool, EUCCIS, due to be accepted into service in Apr 2010, is COTS/GOTS based and therefore should be able to accommodate networked maritime information.

VI. Tools and Networks

Data Gathering Systems

Military

72. To discharge their responsibilities and to facilitate the naval contribution to maritime surveillance described above, European navies use common data and networking systems to compile what is known as the "blue picture", essentially the military version of the overall recognised maritime picture (RMP) achieved through the Maritime Command, Control and Information System (MCCIS). It is a classified system, accessible only to NATO Nations based on a combination of the "need to know" and "need to share" principles. The current version manages up to 5000 tracks. Hardware, software, processing and operation are protected with different layers of classification, which means that for practical purposes it cannot be connected directly to more open systems, and so a direct feed from this system to the wider maritime surveillance community is not yet possible.

73. It follows that a separate, dedicated naval surveillance system for CSDP operations and missions is not envisaged. Within the European area, navies should continue to contribute actively to the federated inherently global systems. Moving from being mere consumers of information to be also providers, warships and aircraft have the ability to provide information gathered by their unclassified navigational surveillance systems without any interaction with their classified combat systems. In an expeditionary context, the global *white picture* will need to be supplemented by local means if available and be supported by the nearest regional centre and hopefully by EMSA. This kind of support should be the object of technical agreements. If necessary this can be supplemented by a CIS application suitable for multi lateral operations such as *Mercury* proven by EU NAVFOR in Operation *Atalanta*. Beyond the *white picture*, MARSUR network will provide the higher level information/intelligence requirement.

Non Military

74. In the maritime surveillance field, both civilian and military, several maritime information systems have been created over the past few years, the vast majority heavily reliant on AIS data. Two of these stand out because of the wide participation by European nations and because both are in the process of integrating other types of data, from the Long Range Information and Tracking System (LRIT) and satellite imagery.

75. The first is the Maritime Security and Safety Information System (MSSIS) initiated by NATO´s Joint Command Naples and implemented by using software developed by the US Department of Transport's Volpe Research Center. It compiles AIS information provided by coastal stations and delivered to MSSIS on a national basis by different national organisations, such as navies, coast guards, departments or ministries of transport, etc. Membership is achieved by simply accepting a simple software End User License Agreement (EULA), which allows the use of Transview (TV32), a computer application accessing the MSSIS network. With this, and the contribution of even a small amount of

AIS data, members gain access to all the data compiled by the entire MSSIS community. Current membership consists of more than 60 nations, including all maritime EU MSs (except Cyprus and Ireland). Candidates for membership described in the EULA as "official government agencies" include:

- Military Organisations, including air, land and maritime forces.
- Government Commerce and Fishery regulation agencies.
- Law Enforcement Agencies.
- Border Security Agencies.
- Government Port Operations and Security Agencies.

76. No attempt is made to draw any distinction as to which particular agency represents which country, nor is there any intention to exclude international organisations of the types listed (NATO itself is an example). This informality in the application and flexibility of the agencies involved has been instrumental in enticing into membership a number of nations with no particular relation with NATO (or the EU), including many around the coast of Africa (Benin, Cameroon, Gabon, Gambia, Ghana, Senegal, Mozambique, Cape Verde, Sâo Tome e Principe, Djibouti, Tunisia, South Africa, etc), in Asia (Singapore, Bahrain), America (Chile, Peru, Dominican Republic, Jamaica, Argentina, Uruguay,…) as well as Australia and New Zealand.

77. The other system of steadily increasing significance is EMSA's SafeSeaNet, which is in the process of being integrated with CleanSeaNet and LRIT into the new SafeSeaNet Tracking Information and Relay System (STIRES). Currently AIS data is fed to SafeSeaNet by EU nations with the result that in many cases, the same data is being provided to SafeSeaNet and to MSSIS by multiple different national agencies. The resultant pool of AIS data is available to participating nations in a similar way to MSSIS. The recent Cooperation Arrangement between EMSA, Frontex and CFCA, referred to above, opens up the possibility of incorporating fishing vessel data from the CFCA's Vessel Monitoring System (VMS), although there is no specific information on this potential development as yet.

AIS picture of the Channel. March 2010

78. The compilation, by either system, of AIS data, with or without other cooperative detection systems, constitutes what is called the *white picture*. It basically consists of all commercial shipping over 300 grt or engaged in international trade, which are required

to have Class A AIS. It is estimated that AIS fitted ships constitute about 35 % of the maritime traffic.

79. The main contributors to this *white picture* are coastal radar stations, which can cover up to 40 NM from the coastline, which are owned and manned by governmental organisations such as the navy, coast guard or other port operators. In many cases, they also contribute data provided by non-cooperative sensors, typically radar co-located with AIS. Maritime operations centres fuse, correlate or validate this vast amount of data to produce the *white picture*.

80. Contacts which only appear in non-cooperative sensors, and which do not respond to electronic interrogation constitute the *black picture*. After those ships with legitimate reasons for not responding, because of, say, systems failure have been weeded out, threats and illegal traffic can be identified such as illegal immigrants, drug or other goods smugglers, pirates or terrorists. Unfortunately a very high proportion – perhaps up to 70% of the total - of non-cooperative contacts is made up of vessels smaller than 300 grt or fishermen of less than 15m in length - which means that illegal traffic is easily concealed. The population of the *black picture* will be reduced if new systems, such as AIS class B, are made compulsory for smaller vessels. .

81. Besides coastal stations, ships fitted with satellite communications can relay their local AIS and radar picture, but permanent satellite communication remains expensive, and tends to be restricted to passenger and larger container ships, as well as most warships of frigate size and above. Successful relay tests have already been made, and the hardware and software needed to complement the regular radar and AIS equipment for this system to work are very inexpensive. However, merchant ships would have to be specifically contracted to provide this service. Although navies on occasion do this (e.g., ships and MPA operating as part of operation *Atalanta*) warships tend to be reluctant to do so on a permanent or regular basis. This is regrettable, not so much for the area potentially added to the coverage by coastal stations, but because it is particularly valuable offshore or in security hotspots, where their contribution would be crucial in helping to clarify and provide analysis of the situation.

82. Finally, several governmental and commercial projects are under way to detect AIS signals via satellite-based receivers. One such system, belonging to the US Coast Guard, is already partially operational, while another is in development by the European Space Agency. As this technology uses the same ship-originated AIS signals, there is clear potential to merge this additional data with the existing MSSIS or SafeSeaNet, thereby increasing the area covered from the coastal regions to almost the entire ocean. Other satellite-based sensors, such as Synthetic Aperture Radar, or infrared and electro-optical imagery, are already being exploited, as routinely demonstrated by EMSA´s CleanSeaNet. When co-located in the same satellite platform, AIS, SAR and imagery systems will provide the additional advantage of easily achievable correlation.

Collective Exploitation

83. No nation or agency has the capability to achieve MDA unilaterally. MDA requires not only the use of one or all of the systems described above but also broad collaboration among many partners, each with potentially essential contributions to effective understanding of the maritime domain. The vision of global maritime surveillance includes:

- A global and worldwide network of regionally based maritime information exchange partnerships. A baseline situational awareness of the maritime domain, essential to fostering cooperation and collaboration among maritime security providers will emerge when participating nations, agencies and other actors voluntarily contribute to unclassified regional networks under the motto "Think global to act local".
- The institution of worldwide standards for broadcasting vessel position and identification. The forces and infrastructure required to achieve full active surveillance of the EU's maritime approaches is unaffordable. The alternative is to establish standards for universal exchange of identification and positional information, analogous to that for international aviation.
- Automated tools (e.g. algorithms & smart agents) that discern patterns, changes, anomalies and potential threats.
- Alerting maritime partners to suspicious behaviour and potential threats.
- Developing a supporting/supported concept to tackle the different threats.

84. Complementing and resulting from forward naval presence, MDA contributes directly to achieving each of the following strategic objectives:

- Securing European countries from direct attack by confronting threats early and at safe distances. Critical to an effective defence in depth posture is the ability to provide early threat detection and interdiction in order to increase time and space for potential response options, afford defence in depth and optimise the advantages of naval forces.
- Securing strategic access and retaining global freedom of action by ensuring that key regions, lines of communication and the global commons remain accessible to all.
- Strengthening existing and emerging alliances and partnerships by addressing common challenges.
- Fostering self-correcting behaviour by merchant vessels, once it will be clear that anomaly controls are carried out by MSs agencies.

VII. Alternative Organisational Approaches.

85. In our Intermediate Report we dismissed a "big bang" approach and a monolithic or hierarchical system of systems in favour of a gradualist approach to a federation or family of non-hierarchical loosely-coupled systems in a service-oriented architecture able to absorb the regional, functional or sectoral solutions already in existence and to benefit from the two pilot projects (BlueMassMed & MARSUNO) now getting under way. Nothing has changed that view which now appears to be widely shared. The issue is not "who controls the database?" but "how are the networks to be organised to facilitate information exchange?" Maritime matters in general and maritime security in particular have been handled differently in every country we have visited. It would therefore be unrealistic to establish a single best practice template, but it is essential that suitable linkages exist or are created at the appropriate levels between maritime stakeholders at the strategic/policy, operational and tactical/front line/point of delivery.

86. While a single executive authority for maritime affairs is desirable, traditional ministerial/departmental/service/agency responsibilities preclude this in many countries. The French concept of a *Secrétariat Général de la Mer*, a very small (12) non budget holding, think tank/ginger group co-ordinating organisation, rather than an executive administration, and which reports directly to the Prime Minister, appears one of the most effective organisational models seen to date. It also provides an effective way to overcome the difficulty that most countries find in generating an authoritative single point of contact for maritime matters.

87. In the absence of an integrated organisation or a single executive authority, the tendency has been to appoint a lead department responsible for policy co-ordination, supported if necessary by an interdepartmental and interagency task force or "round table" group. With the right direction and sufficient collective will this works, but at the operational level there is a clear need for a standing organisation of co-located liaison officers, preferably with the authority to exchange sensitive information and commit assets when required in a timely manner. We observed such newly established joint interagency maritime operation centres working well in Sweden, Canada and Germany and enjoying prospects of much closer integration moving beyond the well established MAOC(N) liaison model in Lisbon. Indeed, the EU Commission is already encouraging MSs to provide single points of contact at the appropriate levels.

88. A concept that has been shown to work equally well in the civilian and military environments at the operational and tactical/delivery level is that of *supporting/supported* where the most appropriate agency is designated to lead with temporary authority over those agencies designated to support in order to provide essential and uncontested leadership during a particular operation, and to overcome difficulties inherent to the use of the information for different purposes. This is a flexible concept where the supported agency can be changed for different phases of an operation.

89. Consolidation of the numerous and varied national and regional agencies with generic coast guard missions - safety and pollution control, constabulary, including counter drug smuggling and organised crime, customs or fishery protection - would be ideally desirable for considerations of cost-effectiveness and consistency in law enforcement across the EU. Even if it were theoretically possible because of the fundamental unity of the MS´s interests, and built on successful experiences such as Frontex and several multinational naval forces, it is still deemed unachievable, at least in the short to medium term, for budgetary reasons - even if there are long term savings to be made, it would require important short term investment - and ultimately because all those missions in the maritime field involve important issues of sovereignty.

90. There are, however, other means to achieve at least part of the benefits of an EU-wide Coast Guard Service without incurring undue cost or infringing sovereign rights or sectoral interests. We see considerable merit in the German model - also followed in some other nations albeit less rigorously - where all agencies, federal, provincial (*Länder*) and local, engaged in coast guard functions, such as customs, water and federal police forces, waterways and shipping administration, fisheries administration, etc., use a common livery with the same distinctive paint scheme for their patrol craft (green hull, slanted stripes with the national colours, and the inscription *Küstenwache*). This adds visual commonality and legitimacy to what is essentially a motley collection of diverse police-like craft with different symbols and colours, whose variable authorities and responsibilities would, in either national or EU terms, be difficult to ascertain by sailors, let alone ordinary citizens.

VIII. Data, Information, Knowledge.

91. We are aware that at first sight maritime surveillance looks a very complex task but, having taken a second look, we have consider that this complexity is essentially only a function of size. There is a huge number of local, regional, national, international, sectoral, civilian and military systems operating in "stand alone mode" and therefore limited in terms of overall effectiveness. There is nothing intrinsically complex in the field of maritime surveillance, other than the challenge posed by the quantity of systems not yet interconnected and operated in parallel. Therefore, as a first step, we recommend the adoption of common definitions for the different classes and levels of information management in this field.

92. The first level is data, defined as "dynamic ship´s data (set)": i.e. ship identity (IMO or MMSI number), time stamp, position, course, speed. We call this a "track", current source AIS, in the near future LRIT plus AIS, any potentially sensitive component having been excluded. This data set should be freely available to all participants in maritime surveillance with no claimed ownership which should be cost free and shared by all involved without restriction. It should be reliable and distributed at a near real time update rate. (Note: this should also include all state vessels with exceptions clearly defined and restricted to operational reasons.)

93. The second level is Information. It is made up of a collection or fusion of several pieces of data or data sets. It can be divided in different sub-levels for practical and management purposes. Besides fusion, correlation and validation are important parts of the process to build information out of data.

94. Sources of information, besides the data elements mentioned, are satellite, shore based and ship or aircraft based imagery from radar, infrared and visual sensors.

95. Information sharing and dissemination can be achieved without restriction where data is simply fused, protection is required for more comprehensive data. Decisions about whether to protect the information remains with the originator of the information, and it must be set against the need to share in a timely way for further action. Sensitive information requires handling by appropriately educated and trained personnel. Protection of information should be limited in time and the reason for restriction explained. All information can be used as a foundation for a layered decision making process. This can be done at a Maritime Operations Centre as well as at an Agency or Regional Maritime Surveillance Centre.

96. The third level is knowledge. This synthesises data (sets) and information. It is the most comprehensive and represents the highest level in the development of a recognised maritime surveillance picture. Knowledge requires the use of all sources and databases, of all actors involved in maritime business, both civilian and military. The protection of knowledge must follow similar principles to protection of information and should be mandatory. But in practice only a very limited amount of knowledge needs

confidentiality, the need to share and the need to communicate should be the norm. Maritime Domain Awareness is the precondition for Safety and Security.

IX. Preferable Approaches.

97.Maritime surveillance must be worldwide and continuous whereas action tends to be local or regional, depending on distance offshore the coasts and the nature of the threat. For example, SAR is usually a local matter while immigration or narcotic trafficking has to be tackled at regional level. There is therefore a need for a global linked network at data level for the *white picture,* and the capability to zoom in for further detail at regional level.

98.There are two different ways to achieve this aim:

- To establish regional situational awareness in a sea basin with a control centre in charge of the regional picture and sharing this picture with other regions. This means designating the regional centres to be in charge, which may be difficult for political reasons; also many countries will be part of two or three marine basins, like Denmark, France, Germany, Spain, and United Kingdom.

- To have all the stakeholders, whether NMCCs, MSs or agencies, on the same network, putting their information at the disposal of all, which could result in excessive duplications unless special procedures are enacted.

99.The organisation chosen must be mission led to give the best response to operational requirements. Our preferred option is a regional one.

100.We have defined three layers of exchange: data, information and knowledge. Some countries prefer only two levels – unclassified and classified. Given the presence of third countries in some basins it would seem better to start with three levels. The first data level would be unclassified and shared through a common basic network. The second one, at information level, can be shared at NMCC or RCC level depending on the agreements set up between the member states either bilaterally or multilaterally. The third level, intelligence or knowledge, would be at NMCC level. The MARSUR and EUROSUR networks can facilitate these second and third levels of exchange.

101.We note that any European organisation will depend on those of MS's. Therefore, as a first step, it seems prudent to establish the exchange at NMCC level and to allow MS to decide whether to sign exchange agreements at regional or sub-regional (local) level on defined areas, if they wish.

102.At tactical level, the need is to build local real time situational awareness. This will be achieved by local sensors: radar, visual, electro-optical and AIS data, enriched with regional information on the inbound tracks. They should also receive lists of contacts of interest in order to generate alerts when they enter the AOR.

103.To-day, the role of the regional centre is to fuse the pictures provided by local centres. They also receive information collected by ships and MPA beyond the coastal radar horizon and from other centres in the country.

104. As a first step, the RCC will exchange data freely with others RCCs, but information and knowledge exchanges will stay at the NMCCs level, except if an agreement has been signed between MSs in a particular basin.

105. As a second step, with the agreement of the MSs, information/knowledge might be shared at RCCs level for regional purposes. And in the last phase, RCCs will be in charge for the global exchange of data/information/knowledge. If a country has a presence in several basins, its NMCC could exercise the regional function in one or both basins as agreed or fuse information for national purposes.

106. At the intelligence level, information has to be worldwide to be able to detect anomalies (e.g. a double AIS code), and continuous to be able to identify significant changes from a normal and referenced level of activity, traceable for ownership and responsibility purposes and gathered through different sources. Information trading, among MSs and third parties, might be the tool to foster an effective two way exchange.

X. Conclusions and Recommendations.

Provide a Means for Informal Exchange of Information.

107. To improve coherence in information exchange we recommend that the Commission and CSDP community establish a series of informal meetings - seminars, workshops or "round tables" of maritime safety and security experts and stakeholders with an interest in improving maritime surveillance. These groups do not need to be formally established, but they will need to exist, if only on a temporary basis at various levels if momentum is to be maintained and success achieved. Typically there may be some reluctance because an agency thinks it has all the information and networks it needs, and it is not aware of how quickly the maritime surveillance whole can become much greater than the sum of its parts.

108. Parliamentary Level: Although it is not for the Wise Pen team to prescribe action at the Parliamentary level, both the European Parliament and the WEU parliamentary assembly have consistently shown interest in defence and security issues, even though maritime aspects have not loomed large. We propose that the High Representative of the Union for Foreign Affairs and Security Policy and the Spanish Presidency could sponsor a presentation and discussion of the issues raised in this report with interested MEPs, with the aim of ensuring the necessary visibility and impetus.

109. Political Level: The Swedish and Spanish Presidencies have initiated meetings at ministry level, hosted by the MoD or their representatives, and the upcoming Belgian Presidency intends to follow suit. This was an important first step but it would appear equally important to invite together the Ministries of Transport, Interior and Defence as an essential next step towards a comprehensive approach. The initiative, mentioned earlier, of the Spanish Presidency to propose the formation of a Joint Council-Commission Task Force with EDA participation, under the authority of the High Representative of the Common Foreign and Security Policy and Vice-president of the Commission, to work on three strands, Maritime Security Strategy, harmonisation of civilian and military developments in this field; and cost-efficiency improvement, is relevant here, as proof of political commitment and practical application of the recommendation to facilitate exchange of information.

110. Execution and Administration Level: With the political support of the Parliament, the Member States, the Commission and the CSDP, experts' meetings should be arranged by DG MARE on behalf of the Commission. These meetings should be designed to achieve mutual understanding and to built trust and confidence. Their purpose would not be to produce documents or minutes, but to initiate open departmentally cross-cutting discussion between all involved in maritime surveillance.

111. National Maritime Coordination Centres Level: Member States should establish National Maritime Coordination Centres with very different competencies within their national constitutional and legal frameworks. They represent the "Focal Points" for all

European activities, for example for EMSA, Frontex etc. A round table could be established with representatives of these National Maritime Coordination Centres.

112. Other important informal forums in existence: The informal North Atlantic Coast Guard Forum and Chiefs of European Navies meetings should also be used for the further development of Maritime Surveillance. The Commission could also use these forums to promote the IMP and to achieve/improve the relation to CSDP.

Subscribing to MSSIS.

113. We recommend that EMSA should be invited to join the MSSIS community as a full member, there being no apparent legal or practical difficulties. This would allow EMSA to increase substantially its knowledge of the *white picture* by being part of the geographically much wider MSSIS in which European navies usually participate, but in many cases without sharing with their civilian national counterparts for a variety of reasons more or less founded on legal considerations. If MSSIS and SafeSeaNet were linked, countries would be able to choose to which of the two they contribute. This would eliminate the duplication of data that can threaten system stability, and save paying multiple fees to the primary source. If the MSSIS contribution of choice is to be the navies - which we recommend - then the whole community of civilian customers of SafeSeaNet would benefit from the addition to the picture of the warships´ own AIS/radar composite image of their vicinity (see recommendation on naval participation in MSSIS below).

Increase Naval Participation in MSSIS.

114. Navies must be encouraged to contribute routinely their ships´ and aircraft´s radar and AIS picture to MSSIS and overcome traditional sensitivities to disclosing the position of warships unless there are genuine overriding operational reasons not to. Warships and maritime patrol aircraft can be very effective at surveillance of hot spots and areas away from main trade routes, precisely because - as different from coastal stations or merchant ships - they can be directed to proceed to where additional information is needed. As owners of a range of particularly effective assets, navies can be key players in the provision of maritime security by extending the supporting/supported concept of operations from the purely military to wider civilian security needs. Supporting picture compilation can be carried out automatically without detriment to other tasks once the “need to know”, “default classification is Confidential”

mindset is overcome, and without any interaction with the ship´s combat system (data to MSSIS is being served by an independent navigation radar and AIS receiver) therefore no risk exists of compromising any militarily significant data or information, other than the warship´s position as indicated above.

Highways of the Sea: Bring Ships into Schengen.

115. Despite general agreement that a greater proportion of European freight should be moved by sea if possible, progress has been slow because of conflicting requirements of the involved agencies, which makes the difficulties significantly greater for shipping than road traffic. Although for years trucks and aircraft have moved seamlessly around Europe on a single set of customs and administrative documentation, ships trading between ports with the EU are uniformly treated as foreign arrivals and require extensive documentation and time consuming clearance.

116. The opportunity now exists to speed up port clearance by registering static data once with EMSA and then filing dynamic data by voyage plans as necessary. The execution of voyage plans can be checked and verified through both cooperative data networks (AIS, LRIT, SafeSeaNet, IALAnet), and active surveillance (VTS, radar etc), and indeed this is under investigation by the Commission. These voyage plans would add what amounts to an additional cooperative detection system, which is both reliable and verifiable constituting a reference against which to check all other dynamic data obtained both by cooperative and non-cooperative systems to highlight inconsistencies. It would also establish an additional layer of trust between the shipping industry, which would confide their commercially sensitive intentions to the Authorities, in the knowledge that it would only be used for security, or eventually safety, purposes. To this scope, the Maritime Surveillance system will allow verification of the navigation patterns between EU ports.

Surveillance Cannot be Achieved Solely by Co-operative Systems.

117. Merchant ship reporting has traditionally required action by the ship – whether manually by paper, VHF radio or satellite calls or automatically by GPS and user fed transmissions (AIS, LRIT, VMS *Blue Box*). As technology has improved and become more widely available and reliable there has been a temptation to rely exclusively on such transmissions. The lesson from the aeronautical community is that this would be a mistake, non-cooperative targets require non-cooperative systems such as radar, electro-optics and infra-red (or in specific circumstances specialised sensors such as HF or OTH radar) to distinguish them from the much more numerous compliant community. There are also concerns that GPS could be a single point of failure through atmospheric interference, jamming or equipment malfunction, which would nullify cooperative systems but only degrade the non-cooperative ones.

Governance.

118.Because of a long history, and the cottage industry like development of maritime trade and activity, governance in the maritime domain has developed from the non-existent, through the chaotic and barely effective, to the complex, distributed and only nascently effective. The governance provided by the IMO has a far more restricted remit than ICAO. Shipping interests including owners and insurers are potent players in the maritime domain and most potential improvements in governance are seen through the prism of cost and commercial convenience. Similarly there is an acute awareness in the shipping community of the cost and value of information. When large quantities of data are being shared between multiple users data quality, timeliness and assurance are vital to the credibility of the system and directly impact its operational utility.

119.Law enforcement, safety regulation and effective security depend on accurate source data. Given that a single controller of a hierarchical system would be unacceptable for international collaborative purposes, some form of distributed governance is required to maintain standards in widely spread, loosely coupled federated system. A stakeholder board is required at policy level to agree organisation, concepts, standards, accreditation, access etc but day to day monitoring and quality control of data needs to be delegated to a technical agency – perhaps in a similar way to that by which EU have MSs´ airspace management delegated to EuroControl and LRIT management to EMSA. At the data level this need not be politically or legally sensitive but funding would be necessary – perhaps partly by the Commission and partly by traffic as in the EuroControl and LRIT models.

120.The BlueMassMed and MARSUNO pilot projects, which should link with and benefit from EDA´s experience in Maritime Surveillance, will establish potentially suitable models of governance for existing federated systems and point the way to solving the governance challenges inherent in more integrated systems. In addition to establishing a satisfactory affordable model for day to day governance, models for governance in crisis situations need to be established and exercised. This process should be supported in a robust way in order to obtain results as soon as possible. The long and successful example of SOLAS and international SAR in practice shows that in discussing governance it is more helpful to discuss delegated authorities and responsibilities rather than sovereignty.

Coast Guard.

121.We suggest it would be helpful both organisationally and operationally if the many EU national or regional organisations deploying craft with coast guard functions adopted a common paint scheme, including the slanted stripes on the hull - that have come to be acknowledged worldwide as identifying coast guard craft – ideally with the EU colour and logo. No change of authority, manning, responsibilities or chain of command would be required at least initially but the mere fact that these craft are visually identifiable as having EU as well as national responsibilities would confer an

additional legitimacy, and by so doing would foster more common training, contacts, and even personnel exchange (much as the navies´ "cross-pollination" or "crosspol" programmes have been used to promote interoperability and common understanding).

122.We recognise that the proposal of the MSs adopting a common livery for their coast guard craft is different in kind from our other recommendations relating to information exchange, but we believe it could be an outward and visible sign of a change of mindset to pursuing commonality in knowledge, unity of effort in response and the expectation of savings through synergies.

123.Irrespective of the acceptance of this proposal, we feel compelled to encourage a deepening of the existing relationships between Coast Guard and navies, within the agreed *supported/ supporting* principle.

Architecture.

124.The Wise Pen Team claim no technical expertise but having consulted widely and visited many locations currently engaged in maritime surveillance we have confirmed our interim finding that the maritime surveillance requirement, both civil and military, does not require a single global system with centralised data fusion and databases built to military specification. The aim should be synchronisation or alignment rather than integration. The requirement is dynamic and can be met in the medium term at least by a non-hierarchical federation of loosely coupled COTS systems that can freely share unclassified data in a service oriented architecture that enables users to develop their own analysis tools (e.g. "smart agents") and applications (visualisation, database mining), and synthesise information from other databases, classified or otherwise, using a common standardised user interface (CSUI) specification such as that developed by the EDA. This CSUI is a common front end workstation that enables multiple users to interact with multiple sources of data from live networks and historical databases using multiple tools and applications to monitor, conduct analysis and exchange information. This can be done within an unclassified or classified framework with access control, variable authorities etc. Although originally conceived for the intelligence environment, it seems ideally suited for achieving MDA.

125.The data fields for the minimum level of compulsorily shared, automatically generated data need to be agreed (e.g. identity by IMO and MMSI number, position, course, speed). Thereafter, additional information, e.g. last port of call, destination,

cargo, crew and passenger information, should be specified on the need to share and responsibility to provide basis. Protocols exist for authorised users to either directly draw down information on demand or, in more sensitive cases, respond to a "I have additional information" tag allowing dissemination on a case by case basis. This practice is becoming well established in the US post 9/11 as a result of the President's Intelligence Community Directive No 501 designed to foster a culture of responsible sharing and collaboration, improve warning capacity and create more accurate and timely analysis in order to forestall significant threats.

126.Given the evolution of maritime surveillance to date – regionally by groups of likeminded states (SUCBAS), and by function (EMSA/Frontex/CFCA), in the immediate future (BlueMassMed and MARSUNO) clustering should be acknowledged as the way forward rather than seeking a "big bang" approach.

127.Transition to improved data-sharing and closer networking of operations is neither difficult nor expensive as Operation *Atalanta*'s rapid development of *Mercury* has shown – basic services and near real time information can be provided through internet web services and secure access.

128.The human element of the architecture should not be forgotten – joint and interagency task forces at the policy level, collocated liaison officers at the operational and tactical levels increase effectiveness by improved communication, awareness and synchronised action. Organisationally, when the quantity of data threatens to prevent effective information management then the principle of subsidiarity is useful – quality control at the lowest responsible level.

129.Finally in developing the MDA architecture it is vital to take industry with you, they are the custodians of affordable technology, and through proprietary technology can be deliberately or inadvertently obstructive if not treated as partners.

Protection of Information.

130.EU rules on security of information (INFOSEC) are contained in the Council Decision of 19 March 2001 (2001/264/EC) amended to 18 June 2007. This important document is a mandatory reference for all matters pertaining to protection of information, and enshrines two principles relevant to this report: first, that information is protected according to its importance to the EU or one of its Member States and second, that the "need to know" (quoted no less than 26 times) is a fundamental principle upon which all decisions relating to information protection are to be based.

131. If considered solely within the strict limits cited in the definitions of the Levels of Classification , these two principles are mutually consistent with the interests of the EU or its MS, in other words, with national or collective security. In the case of maritime surveillance, however, where safety and commercial considerations are almost invariably involved alongside national and collective security, the straitjacket of the "need to know" principle and the *top secret/secret/confidential/restricted* classification

almost inevitably leads to over-classification, even though this is explicitly discouraged earlier in the same document. This is obviously detrimental to the efficiency of a system where any impediment to the rapid and free circulation of information could potentially result in loss of life.

132.Moreover, while it is understood that commercial interests, such as keeping the location of fishermen or spot market tankers concealed, may be legitimate, they do not necessarily entail the level of security provided by a system designed with state security in mind. Commercial interests should be protected by the interested parties´ own security system, for which commercial solutions are readily available, and for which the interested parties should bear the cost. This should simplify the design of an information protection system that is an integral element of data/info exchange between EU and national agencies.

133.We therefore propose that, for the purposes of maritime surveillance, the principle of "need to share" should replace the more restrictive "need to know", which should only be used where state or EU security is at stake. We further propose that, for cases where exclusively commercial interests are the reason to limit the dissemination of data or information, then the term "information protection" should be used instead of "information security"or INFOSEC, which should be reserved for national or collective security, thus clarifying the legal criteria when implementing data/info exchange systems.

Organisational Aspects.

134.The Maritime domain covers a large spectrum of activities such as maritime transport, fisheries, energy, tourism, sport, marine environment and research, security and defence which often interfere or overlap. In its reports, the Commission states that "The EU's Maritime regions account for some 40% of its GDP and population". Different departments, directorates and agencies are dealing with maritime problems and issues, but, until now, nobody has been in charge of coordinating all these activities. In some EU MS, a Secretary or even a Ministry is devoted to this role; this does not exist at EU level. To develop an integrated maritime policy which includes a close relationship with CSDP will require stronger coordination in the future. This could be achieved by the Vice-President of the Commission and High Representative of the Union for Foreign Affairs and Security Policy setting up a high level focus, either an individual or a small

steering group, on maritime affairs. This would facilitate the necessary coordination and dialogue between the stakeholders.

A Step by Step Approach.

135.To achieve a Europe-wide, integrated maritime surveillance system, in which all EU MSs must participate on an equal basis without restrictions on data and information exchange, we recommend:

As a first step:

- to establish a common web network shared by all the stakeholders dedicated to the *white picture*. This picture will be established automatically by AIS data, at NMCC level for LRIT and radar data, initially. BlueMassMed and the North and Baltic experiments will respond at RCC level for radar collected data. There may be agreements between MSs to go further at this stage as for example to share LRIT data between Portugal, Spain, United Kingdom and France;
- to favour participation of all the stakeholders in collecting and sharing data
- to connect NMCCs through MARSUR and/or EUROSUR to permit information and intelligence exchanges on a by request basis.

As a second step:

- to develop regional exchange of information/intelligence by delegating this responsibility at regional level. This can be arranged for different purposes according to the region: for example immigration in Mediterranean and narcotics in the Atlantic.
- A European counter-narcotic mission would be logical in the Caribbean as several Navies/administrations from different MSs are already participating closely with JIATF(S) in Key West, in the United States.

As a third step:

- to set up an organisation where the RCC will have the predominant coordinating role;
- from this to establish the links with other regions of the world, with a common point of contact.

Data, Info and Knowledge Exchange.

136.Present the description of Data, Information and Knowledge contained in this report to the different expert groups and providers of data, information and knowledge. Use it as a baseline to facilitate the willingness to share and to use this approach to built trust and confidence from bottom up. The primary audience must be the "Member States` Experts Sub-Group on the Integration of Maritime Surveillance" chaired by DG MARE,

the MARSUR Working Group 1, chaired by EDA, the informal meeting of the Heads of the European Navies, chaired in 2010 by Denmark, the North-Atlantic Coast Guard Forum, chaired in 2010 by Norway, EMSA, Frontex and CFCA, the three agencies that have signed an agreement about information sharing, therefore they are best suited for this input. Elaborate about the question how far the IMP Chapter III-3 "Marine Knowledge" could be integrated in our third level Knowledge.

Contribution of the Navies.

137. As Navies develop new surveillance systems for defence purposes, common CIS systems can produce greater efficiency and cost-savings.

138. Naval data and information, providing it is not highly classified, can enrich the common picture. Warships and MPA should, where possible, transmit this data continuously. Warships can also collect scientific and oceanographic information for the EMODNET data base.

139. One of the enduring roles of naval operations centres is to detect anomalous or suspicious behaviour that may correlate to potential threats. Accurate assessment of trends and anomalies requires experience and knowledge. Naval ability to locate, track and anticipate threats is unique and would be of great support for MDA. If not co-located with the Naval centres, the NMCCs must maintain close relationships and permanent links with them to ensure coordination of patrol assets.

140. MHQs are used to organising training and exercises. They can provide the backbone for preparing interagency and multinational exercises. Navies can offer valuable training and capacity building to third countries wishing to create or develop their maritime surveillance capability.

141. New technologies can be developed for all stakeholders by using naval facilities and expertise for implementing new programmes for networks, data links, sensors, UAVs and new ship and satellite concepts.

Annex A. Definitions.

Introduction.

1. In the maritime world there is misinterpretation and difficulty in ascribing responsibilities among agencies, whether military or civilian, as well as amongst the many different national and EU civilian agencies. This stems from the variety of definitions of the terms "security" and "safety" and their application in the maritime domain. The terms are often used imprecisely, inconsistently, tautologically or by cross-referring to each other, in defiance of several rules of ISO standard 704 [7]. Further problems occur in translation to and from other languages, where the terms can have the same, different, mixed, or overlapping meanings.

2. When the distinction is made as in English, the consensus seems to be that "security" applies to man-made risks and hostile acts, while "safety" applies to accidental, dangerous or potentially dangerous events. This difference is crucial as it affects the structure, organisation and responsibilities of the agencies involved, so it should be clearly delineated and understood from the outset.[8]

3. Another source of confusion is due to the terms being interpreted in different ways, sometimes as an activity, at other times as an aim or a condition, thereby making it difficult to delineate the fields and separate the responsibilities. In particular, the military tend to consider "security" as a *condition*, rather than an *activity*, implying that no action is required unless the condition or status quo has been disrupted - by inference through hostile action. On the other hand, if "security" is defined as an activity, as is consistent with the EU Regulation 725/2004 (below), it requires constant attention and effort, not just in the face of hostile action, but when confronted by all types of illegal, illicit, and criminal actions, which occur continually in peacetime. In some cases attempts have been made to bridge this distinction by talking of an *ongoing condition* (q.v. the NATO definition quoted above) or *continued condition*. In the context of this study, which aims is to achieve synergy among the agencies involved, where all but one of them are civilian, it would seem more appropriate to adopt the *activity* interpretation. This would not be incompatible with simultaneously using the *condition* interpretation in purely defence-related documents.

---

[7] Just as token examples of cross-reference, cf. NATO´s definitions proposed by the SCs in doc SH/J5/2009 - 207387 3000 TC-538/TT-4427/Ser: NC0027, 21 July, New Alliance Maritime Security Operations Concept: *Maritime Security is the ongoing condition in the maritime environment where international and national laws are adhered to, the right of navigation is preserved, and citizens, vessels and resources are safe*. Also, cf. The EU Maritime Surveillance and Mission Tasks, 22/03/2006: *Security missions are conducted to monitor vessel and cargo movements for reasons of maritime safety, [...].*
As for tautology, see in the same document: *Maritime safety: To continuously maintain and enhance safety in shipping and the protection of life, [...] It concerns: safety of the ship, its crew and its passengers and/or cargo, safety of navigation, environmental safety [...]*, and the near-identical text in the EU Green Book, defying the rule according to which the defined object must not be part of the definition.

[8] One of the very few documents where this distinction is clearly delineated is in the excellent CHENs "Maritime Security Best Practice Guidelines", 24 Nov 2008.

4. This study's proposed definition for "maritime security", which is the cornerstone on which all the others rest, has been adapted from Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security [9], which suits the particular circumstances of the transportation community, which lacks coercive powers to enforce security rules. The changes introduced to the original are intended to cover the needs of other actors, in particular law enforcement agencies, without diminishing or contradicting the old one, and to allow for new concerns that have emerged in the maritime world since that definition was approved. "Maritime safety" has been defined as the obverse of "maritime security", in order to highlight the differences.

5. For other related concepts we propose adopting definitions consistent with the "safety" and "security" distinction above, adapted where necessary from authoritative dictionaries or existing references.

6. Significantly, the set of definitions proposed for the study, as explained above for the "maritime security" one, differs from the various existing definitions in that it has not been designed to fit a specific responsibility, agency, or need, on the contrary, it is intended to have a more universal applicability, without in any way detracting from, or limiting the existing responsibilities. This proposal is submitted in the hope of general acceptance across the EU maritime-oriented communities.

7. Definitions have also been provided for other less contentious terms, but for which we have detected a variety of interpretations that make agreement on specific subjects difficult. Although not strictly a matter of definition, we have also included descriptions of areas in proximity to the EU as there are several that differ between publications.

Definitions and Comments.

8. Maritime Security: The combination of preventive and responsive measures to protect the maritime domain against threats and intentional unlawful acts. Comment: The proposed definition, by including both preventive and responsive measures, aims to cover both law enforcement (civilian and military) and defence operations. Also, the term "maritime domain" (defined below) is more inclusive than just "shipping and port facilities" (which appears to exclude crews and other personnel), which were the items to be protected according to the EU Parliament and Council approved text. The enhanced definition, by concentrating on the unlawful use of the maritime domain, makes Maritime Security an international and interagency, civil and military, ongoing activity to mitigate the risks and counter the threat of illegal or threatening activities in the maritime domain, so that they may be acted upon in order to enforce the law and protect citizens and safeguard national and international interests. Both constabulary and defence agencies have distinct and direct responsibilities in Maritime Security.

[9] *Maritime Security means the combination of preventive measures intended to protect shipping and port facilities against threats of intentional unlawful acts.*

9. Maritime Safety: The combination of preventive and responsive measures intended to protect the maritime domain against, and limit the effect of, accidental or natural danger, harm, damage to environment, risk or loss. Comment: As explained in the introduction, the crucial distinction between man-made (security) and unintentional (safety) risks and dangers is highlighted by using a text that parallels the definition of "security". Maritime Safety, by the use of the inclusive term "maritime domain", is understood to refer to dangers to the ship, its crew and its passengers, and/or cargo, and to navigation; it also covers the prevention of pollution from ships, and includes sanctioning illicit pollution and intervention to limit damage of incidents; finally, liability and compensation for damage incurred by ships are also part of Safety. For completeness and coherence, damage to the environment is included under Safety even if there are occurrences when it is not unintended or accidental, therefore requiring constabulary action, as the actions required to restore the environment to its previous state are the same whatever the origin of the damage. The number of agencies with responsibility in Maritime Safety is extensive: constabulary, traffic control, fishery protection, customs, environmental protection, search and rescue, are but a few with direct responsibility in one or several aspects of Safety and stewardship of marine resources. The Defence Department, despite its extensive capabilities, should normally be seen as having supporting or subsidiary responsibility, rather than primary responsibility in the field of safety.

10. Maritime Domain: All areas and things of, under, relating to, adjacent to, or bordering on a sea, or ocean including all maritime-related activities, infrastructure, people, cargo and vessels and other conveyances. Comment: The deliberate choice of the term "domain" as opposed to more traditional expressions such as "area" or "zone" is intended to provide a less rigid and more all-embracing description of the realm where maritime interests lie, so as not to exclude the air above, used by maritime patrol aircraft, or harbours and other coastal facilities whose economic life depends on both the safety and the security of maritime traffic. As expressed above, restricting the security or safety concerns to "shipping and port facilities" as the EC Regulation quoted above would impose an undue restriction in the execution of responsibilities by many agencies.

11. EU Maritime Domain: That part of the maritime domain encompassed by the EU Member States´ Territorial Waters, Exclusive Economic Zone, Continental Platform, and Search and Rescue Areas, as defined by UNCLOS/SOLAS, together with all cargo and vessels flagged, beneficially owned by, or bound to the EU, as well as any Area of Operations outside the above that has been declared for an EU Maritime Operation. Comment: Given the multi-agency involvement, the EU maritime domain has to include the logical addition of areas defined or declared for different purposes, namely TTW (and implicitly the Contiguous Zone) for jurisdictional matters, EEZ and Continental Platform for exploitation of resources, SAR for protection of human life. Also, given the complexity of the legal responsibilities for ships and cargoes, it has been considered necessary to provide an extensive list of the ways in which EU nations could maintain

an interest in the welfare of cargoes, ships and crews. All these different areas are taken to include metropolitan territories as well as to overseas territories.

12. Maritime Surveillance: The systematic and continuous observation of the maritime domain to achieve effective situational awareness. Comment: The key words are *systematic* and *continuous*, consistent with the interpretation of Maritime Security and Maritime Safety as *activities*. The proposed definition does not limit the types of means of observation, be it radar, AIS, satellite imagery, or any other system.

13. Integrated Maritime Surveillance: Maritime Surveillance to which different agencies contribute in a cooperative manner, in order to achieve synergistic exploitation of enhanced understanding for the benefit of the decision making processes in each contributing agency. Comment: Conceptually, Integrated Maritime Surveillance does not differ from Maritime Surveillance by itself, but it has been considered necessary to include this concept in order to illustrate the need for a cooperative approach to the compilation of information in this field. The accumulated information, however, does not lead directly to a hypothetical "integrated maritime situational awareness". On the contrary, and as noted in the comments to MDA, each sectoral agency or otherwise concerned party must build its own sectoral or regional situational awareness in order to support its own decision making.

14. Maritime Domain Awareness: The understanding of activities carried out in the maritime domain, and surrounding environmental circumstances, to support timely decision making in the fields of Maritime Security and Maritime Safety. Comment: The overall aim of MDA is to understand, prevent wherever applicable and manage in a comprehensive way all the events and actions related to the maritime domain, together with their environment, which could impact the areas of maritime safety and security, including law enforcement, defence, border control, protection of the marine environment, fisheries control, trade and economic interests of the EU. It follows that, even if the underlying information is shared or common, there are as many MDAs as areas where decision making may be independently applied.

15. Maritime Security Operations: Operations carried out by a Security or Defence agency with the aim of achieving or restoring freedom from threat or intentional unlawful acts in the maritime domain. Comment: Maritime Security Operations are not restricted to single agency action. It is perfectly feasible that a police force has primary responsibility for an operation, anti drug smuggling for instance, while receiving support from a naval force. Conversely, a naval force in action against piracy may receive police support in the form of sea-riders" in order to comply with certain legal requirements involving arrests. The twin roles "supporting/supported" should be clearly expressed and accepted in operation orders.

16. Maritime Safety Operations: Operations carried out by an agency with responsibility in the realm of safety, with or without the support of Security or Defence agencies, in order to police the maritime domain against risks to safety or the environment, due to the

failure to observe internationally accepted safety rules. Comment: Similar to the above, Maritime Safety Operations may be conducted by more than one agency, and therefore the supporting/supported scheme should also be applied. Usually the Defence Department would have, as commented in the definition of Safety, a supporting role.

17. EU Maritime Zones: To enable European nations to work together to enhance Maritime Surveillance, the European Maritime Domain is divided into five zones: the Atlantic Ocean, Baltic, Black, Mediterranean and North Seas. The regional organisations formed by the littoral nations in each of these zones are initially intended as pilot projects, the eventual aim being to achieve full integration at EU level. More generically, these zones are also referred to as "sea basins".

18. System of Systems: A set or arrangement of systems that results when independent systems are integrated into a larger system that delivers unique capabilities. Comment: A system of systems is made up of collaborative systems that, for reasons of physical distance or of different primary responsibilities, do not lend themselves to fusion into a single system. A commonality in procedures, databases used, or overall objectives, advise and allow a certain pooling of resources with synergetic effect, without losing physical and organisational independence. This pooling of resources can be made in a centrally organised way, or by an association of peers.

19. Federation of Systems: A System of Systems managed without central authority. Constituent systems are independently managed and have a purpose of their own. Comment: This particular type of SoS fits very well with the needs of maritime surveillance, as the multiple components of the intended organisation keep their operational and managerial independence, which is a requirement as responsibilities are as varied as the number of components, as well as their ability to evolve independently.

20. Data: In the maritime surveillance context, data is a set of quantities, characteristics or identity pertaining to a unit of interest, called a track, usually a ship.

21. Information: The result of correlating two or more pieces of data on the same track that have been obtained from different sources, thereby increasing the confidence level that it corresponds to reality. The compilation of data on different tracks from the same source also becomes information, as it correlates each one with the rest, thus adding value to the mere addition of the individual tracks´ data.

22. Knowledge: A set of tracks correlated from different sources and supported with information of different nature, such as intelligence or historical, becomes knowledge.

Annex B. Case Studies.

Impact of Maritime Traffic Knowledge on Military Operations. The Kosovo Campaign.

Facts.

1. At the beginning of the Kosovo campaign, March-June 1999, NATO´s Military Committee discussed a SACLANT proposal to redeploy the Standing Naval Forces (SNFL and SNFM), with a total of sixteen frigates, from the Adriatic,to interdict in the Strait of Otranto, tankers bound for Kotor, in Montenegro intending to replenish the fuel depots being bombed by Allied air forces were bombing.

2. The proposal failed to achieve consensus because of opposition by some nations, on the grounds that there was a high probability that any tankers bound for Kotor would be Russian, Russia being a well known supporter of Serbia and an opponent of the NATO action. Russia would certainly object to Russian-flagged ships being stopped, inspected and diverted. Moreover, given the political sensitivities at the time it was deemed undesirable to alienate the Russians further. The proposal was discarded, tankers were allowed to proceed to Kotor, and Allied aircraft continued to launch strikes to burn Serbian fuel in depots at Kotor and elsewhere in Serbia and Montenegro, with consequent damage to the environment and property and attendant risk for the aircrew.

3. After the hostilities it was found that twelve tankers had indeed entered Kotor during the eleven weeks of the campaign. None was Russian, and all but one were owned by Western European companies.

Causes.

4. It is doubtful that at the time much else could have been done at the time, as AIS and other reporting systems had not yet been implemented , but nevertheless no attempt was even made to discover through shipping or register companies, planned shipments of fuel to Kotor.

Lessons Learned.

5. Apart from approaching the main shipping companies, that might have also been aware of competitors´ shipping movements, information on Adriatic bound traffic could have been gleaned from Lloyd´s or coastal stations in the Channel, Gibraltar and *the Straits*. A few day's advance warning whether Russian tankers were part of that traffic would have allowed the operation to accommodate political sensitivities.

6. Today AIS signals are detected by a chain of coastal stations and, if that data is were shared through an EU wide system - acquiring the information would be simple . The operation would have been agreed and refuelling of the Serbian depots at Kotor would have been stopped at far less cost, risk and environmental damage than by bombing . In summary, precise knowledge of merchant traffic can be beneficial for planning and executing even non-naval military operations.

Impact on Immigration Control. The Case of the MV *East Sea*.

Facts.

7. On 17 February 2001, the Cambodian-registered freighter "East Sea" was deliberately run aground on a French Mediterranean beach near Saint Raphael. She was carrying 912 passengers, most of them declaring they were Iraqi Kurds (250 men, 180 women and 480 children) from the Mosul region, northern Iraq. Suffering Iraqi oppression, they had paid a human trafficking network $2-4,000 s to go a European country. After selling all their possessions to pay for their journey, they were taken in small groups to Syria, where they waited about a month for a ship. In subsequent questioning , they claimed to be Kurds from north-east Syria.

8. On 10 February 2001, they boarded the "East Sea" from a beach near the port of Latakia and sailed the following day. Crammed into holds in extremely unhygienic conditions, they had no contact with the crew who were masked and apparently of Turkish nationality. Three women gave birth during the crossing.

9. On 17 February, the ship was run ashore on Boulouris beach on the French Côte d'Azur. The crew immediately disappeared and the passengers were taken into the care of the French authorities, 22 had to be hospitalized, although no one was seriously ill. The ship was towed out to sea and sunk a few nautical miles from the coast.

10. The legal procedure for dealing with this type of situation was immediately put into operation using exceptional means given the urgency and large number of cases to be dealt with. Rather than allow the passengers direct entry into France, the French authorities decided to have recourse to the border asylum procedure, in order to decide at this initial stage whether a refugee was entitled to seek asylum. For this purpose, military premises were transformed into a waiting area and every adult was questioned.

11. Asylum seekers are given temporary residence permits valid for a month; they must agree to have their fingerprints taken and are given asylum application forms to fill in. It appears that six of them were Palestinian Lebanese, four obtained safe-conduct, the two others were kept in the waiting area before being released by the judicial authorities with the injunction to leave French territory within seven days.

12. On the 24 and 25 February, the French authorities were informed that some of these Kurdish refugees were moving towards eastern and northern France. Police officers were immediately instructed to watch out for the refugees and remind them that the safe-conduct did not allow them to go abroad. Nevertheless, the Swiss and German authorities arrested some who were trying to enter their territory and handed them back to their French opposite numbers. Many of them had relations or hopes of getting logistical support in Germany and the countries of northern Europe where the Kurdish community is well established. Some suspected smugglers were detected one of whom was arrested but later released for lack of sufficient evidence to press charge s. The operation was profitable for the traffickers who netted around 1 million Euros.

Causes.

13.Due to lack of information exchange between different countries, the course of the East Sea was not reported and no alert raised.

14.Due to unmanned coast stations and lighthouses no contact was made with the East Sea no alert passed to the authorities.

15.Between May 2000 and February 2001 three other cases were noted in the Adriatic (from Albania), the South of Italy and Turkey (from Bangladesh), all with similar results.

Lessons Learned.

16.In France, previously unmanned coastguard stations and lighthouses have had their personnel restored by the Navy .

17.The European Parliament refused to vote for more sanctions or to charge the companies who had had people arrested on board their ships. However, this succession of cases finally led to the imposition of stronger border control through Frontex.

18.The French Navy developed the National Maritime Safeguard Concept, implemented in 2002.

19.Surveillance was reinforced in the Mediterranean and by police focusing on human trafficking networks made successful boarding of ships possible.

The Riddle of the MV *Arctic Sea.*

Facts

20.The *Arctic Sea* was built in 1992 as the *Ochotskaje* in Turkey for the Russian Company Sakhali Shipping. Since 2009 it has been owned by the Helsinki based Finnish Shipping Company "Solchert Management", owned by three Russian managers. It is registered in Malta with a crew of 15 Russian seamen.

21.The *Arctic Sea* spent 14 days in maintenance in Kalinigrad, Russia's freewheeling enclave in the Baltic, before proceeding to Pietasaai/Jacobstad in Finland to load 6400 cum of timber. Before sailing, the *Arctic Sea* had been screened by the local fire department for radiation, without result. On 23 Jul 2009 she departed Jacobstad for Bejaia, Algeria, with an estimated time of arrival of 4 August.

22.At 0300 on 24 July, inside Swedish Territorial Waters off Gotland/Öland, she was boarded by a group of 8 to 10 people. The group left the *Arctic Sea* Sea 12 hours later. This was later confirmed by an EU spokesman. who also reported a second boarding on 31 July off the Portuguese coast during her passage south.

23.On 26 July, the Russian Ambassador in Sweden asked the Swedish Government about the circumstances surrounding the boarding of the *Arctic Sea* by Swedish Police/ Customs on 24 July. On 28 July, *Arctic Sea* entered the English Channel and establish VHF communications with Dover Coastguard Traffic Control.

24.The first media reports about the strange events onboard the *Arctic Sea* were published by the Swedish newspaper "Metro" on 30 July following a phone call from the *Arctic Sea*. On the same day the *Arctic Sea´*s AIS signal was detected by Brest Coast Control, coincident with its radar echo. The following day, 31 July, she continued south down the Portuguese coast. On 3 August her Finnish owners received a phone call from *Arctic Sea*, demanding a ransom of $1,5M.

25.Nothing further was heard until 14 August, when it was reported to be 450 nm north of Cape Verde island Sâo Antâo. This was denied by the Russian Authorities on 15 August. Finally on 17 August the *Arctic Sea* was located 300 nm north of Sâo Vicente, Cape Verde. The Russian frigate "Ladniy" intercepted the ship, freed the 15 crew and arrested 8 alleged hijackers.

Causes

26.No reliable information about the events and its circumstances has yet been published by official authorities, but it can be assumed that the transit of the *Arctic Sea* from northern Finland through the Baltic Sea via the North Sea, English Channel, Bay of Biscay, and Portuguese Coast to the south Atlantic was monitored by all national and European Agencies responsible for maritime surveillance.

27.Since 30 July the media were aware of the anomalies in the strange behaviour of *Arctic Sea*. The case then became a matter of public concern, fuelling speculation about a possible criminal, piracy or secret service conspiracy, which became widely accepted at same time as raising questions about the capabilities of maritime surveillance within the European maritime domain. Neither the media nor the public believed that a ship could disappear and remain undetected for such a long period of time.

Lessons Learned

28.The authorities involved in handling the *Arctic Sea* case lost credibility, public trust and confidence. It is important to develop policies to handle such cases. There is considerable agreement about protecting information for a certain period but equally, after that time, there is a reasonable expectation of a a comprehensive and definitive official case report.

29.The absence of such a report places a question mark over the authorities capacity and ability to act or react in such a situation. A much more transparent policy is required and the responsibility to share information with the public has to acknowledged by all involved. NATO, the EU and in this case a third country, Russia, need to develop a information policies which meet the European public's expectation and right to know.

Annex C. Glossary of Acronyms.

AIS	Automated Identification System
BlueMassMed	EU pilot project for Mediterranean Maritime Surveillance
CFCA	Community Fisheries Control Agency
CHENS	Chiefs of European Navies
CIS	Communications and Information Systems
CISE	Common Information Sharing Environment
CJOS COE	Combined Joint Operations from the Sea Centre of Excellence
CleanSeaNet	Satellite-based oil spill detection
CMPD	Crisis Management Planning Directorate
COTS	Commercial off-the-shelf
CSDP	Common Security and Defence Policy
CSN DC	CleanSeaNet Data Centre
CSUI	Common Standard User Interface
DG 8	Directorate 8 - Defence aspects
DG 9	Directorate 9 - Civilian Crisis Management
DG MARE	EU Directorate General for Maritime Affairs & Fisheries
EC	European Commission
ECSA	European Shipowners' Association
EEZ	Exclusive Economic Zone
EDA	European Defence Agency
EMSA	European Maritime Safety Agency
EMODNET	European Marine Observation & Data Network
ESA	European Space Agency
EU	European Union
EUCCIS	EU Command and Control Information System
EULA	End User License Agreement
EUMC	EU Military Committee
EUMS	EU Military Staff
EUROSUR	European Border Surveillance System
EUSC	European Union Satellite Centre
FoS	Federation of Systems
FRONTEX	European Agency for the Management of Operational Co-operation at the External Borders of the MSs of the EU
GOTS	Government off-the-shelf
HF	High Frequency
IALA	International Association of Marine Aids to Navigation and Lighthouse Authorities
ICAO	International Civil Aviation Organisation
ICC	International Camber of Commerce
IFC	International Fusion Centre
IMB	International Maritime Bureau
IMO	International Maritime Organisation
IMP	Integrated Maritime Policy
INFOSEC	Information Security
ISO	International Standards Organisation
ISPS	International Ship and Port Security
JIATF(S)	Joint Inter-Agency Task Force (South)

LINUX	A free and open source family of operating systems for personal computers, based on voluntary contributions of a great number of independent programmers.
LRIT	Long Range Identification and Tracking
MAOC(N)	Maritime Analysis & Operations Centre Narcotics
MARBORSUR	Maritime Border Surveillance
MARSUNO	Maritime Surveillance North
MARSUR	Maritime Surveillance
MDA	Maritime Domain Awareness
MCC	Maritime Component Commander (NATO)
MCCIS	Maritime Command & Control Information System (NATO)
MDA	Maritime Domain Awareness
MMEA	Malaysian Maritime Enforcement Agency
MMSI	Maritime Mobile Service Identity
MPA	Maritime Patrol Aircraft
MS	Member State of the European Union
MSO	Maritime Security Operations
MSSIS	Maritime Safety & Security Information System
MV	Motor Vessel
NACGF	North Atlantic Coast Guard Forum
NAVFOR	Naval Force
NMCC	National Maritime Coordination Centres
OHQ	Operational Headquarters
OTH	Over the Horizon
RCC	Regional Coordination Centres
ReCAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery
RELEX	Exterior Relations (EU Directorate General)
RMP	Recognised Maritime Picture
SACT	Supreme Allied Commander Transformation (NATO)
SafeSeaNet	EMSA´s Merchant Shipping Information network
SAR	Search and Rescue/Synthetic Aperture Radar, depending on context
SMSC	Singapore Maritime Security Centre
SOLAS	UN Convention on Safety of Life at Sea
SoS	System of Systems
STIRES	SafeSeaNet Traffic Information Relay & Exchange System
SUCBAS	Sea Surveillance Baltic Sea
TTW	Territorial Waters
UAV	Unmanned Air Vehicles
UNCLOS	United Nations Convention on the Law of the Sea
VMS	Vessel Monitoring System
V-RMTC	Virtual Regional Maritime Traffic Centre
WEU	Western European Union