# Maritime Security from a Systems View

**From Cold War Systems to multinational Civilian-Military Information Exchange**

## The Past

Inter-governmental and inter-services approach, civilian-military co-operation or standardization are no new idea or concept. History has numerous examples, and maybe modern standardization has its roots in the ancient civilizations of Babylon and early Egypt, where physical standards for weight and measurements of the Sumerians were carved in stone. Later Gaius Marius restructured the Roman Legions and standardized their equipment in the Marian Reform – Dr Urbanovsky called it in the « Brief History of Defence Standardization » the « probably first recorded Defence Capabilities Initiative in history ».

During the II World War submarine losses increased significantly due to the grouping of commercial ships in allied convoys. Key issue for the hunters as well as the hunted was in both cases always secure and undetected communication. One aimed to guide his convoys away from detected sub packs, the other tried to analyze the convoy routes to guide sub packs towards their targets. Only the combined effort of masters and geniuses in mathematics, cypher technics, radar and sonar technology made it possible to reach the appropriate information level and achieve the necessary awareness in military operations. The inter-governmental, inter-services approach and civilian-military co-operation (CIMIC) of this time was the key to success and victory in history.

The technologies, developed during the war, boosted our private lives afterwards and determined the battle ground for the Cold war. The Advanced Research Projects Agency Network (Arpanet) was the beginning of military and civilian Communication, Command and/or Control (C3) Systems and therefore is the offspring of the electronic networking – the Internet. The systems were however strictly divided in land, air or maritime purpose and designed to support the duties of the accredited users groups. Information exchange between military and/or civilian systems was not only unwanted, they had to be prevented for security of the nation and/or coalition. With the melt-down of the Iron Curtain and a change in politics new concepts evolved

for global networking. Now countries tried to get independent from rigid and slowly advancing coalition systems. Nations started to develop and field their own systems interoperable with NATO. With the increasing terrorist threat, piracy, environmental danger and disasters – the new challenges of the asymmetric warfare - it became clear, that civilian and military, government and non-government organization, with their compartmented systems, could no longer handle the tasks independently, nor could it be financed due to economic crises. We are back in history.

**Today**

The monolithic system design for a singular user community cannot satisfy the complex demands of an inter-government and inter-services strategy and civilian-military co-operation of today. Operational systems today are often used as mere information portal or for plain e-mail exchange, while other systems reached their limits in performance, have bandwidth limitations and major obstacles in upgrading and modernizing. Operators use an average of 20 % of the today's total system's functionalities; 80 % are therefore ballast and mostly also obsolete. Systems created by only ministerial guidance or political protectionism, without consideration and involvement of the future user community, are condemned to failure.

The obsolete system designs and the resulting limited interoperability are one problem, but even greater challenges are national and coalition information security requirements. The security standards and documents relating back to the time of the Iron Curtain are explicitly created to prevent information exchange outside a certain user group or community. Nearly all nations are hampered by their own regulations and restrains in this respect.

Co-operation from private humanitarian associations to highly classified military systems is required today. Concepts like Network Centric (NC) are the military approach to it. Best practice to build a system for these new demands is an iterative engineering process. However, in reality experimental software is sometimes used for a new concept and even is used operational without any prior development study. This « mission driven system implementation » has to be later straightened out in the documentation, added to the supply chain and fitted into the existing systems. This is the hard way around and prone to mistakes.

Situational Awareness is a challenge in operational matters, but it is also a question of basic concepts and believes. In this complex situation, only a carefully evaluated system - backed up by studies and experiments - will be able to fulfill the task and all Information Exchange Requirements (IER), utilizing the principle of « need to share » versus « need to know ».

The rapid advance in information technology and the available high bandwidth of land-based network as well as mobile units with limited and expensive satellite bandwidth have to be taken into consideration. Having technically evaluated some of the maritime systems, one can say that the Scandinavian countries – especially Finland – have currently the most advanced sea surveillance system and inter-agency networks in the hemisphere. Singapore, Italy and Brazil have at the same time the emphasis on political networking. These countries gained through their networks a high political profile and became most valuable partners in co-operations like NATO or EU.

The European Defense Standards Information System (EDSIS) went online in 2009 and the participating Member States of the European Defense Agency (EDA) provide material standards in the European Handbook for Defense Procurement (EHDP), listing more than 10.000 military standards, specifications and related information. Since creation of NATO, the Standardization NATO Agreements (STANAGs), Allied Publications (APs) and Multinational Publications (MPs) have been developed in support of the mission networks. About 1.700 STANAGs and 900 AP’s are available, whereof 65% cover « operations », 25% « hardware » and the rest are for administrative matters of the alliance. However, it wasn’t until the year 2000 when finally the NATO Standardization Organization (NSO) was established, in which the NATO Military Committee for Standardization (NCS) is now heading the NATO Standardization Agency (NSA).

The production of STANAGs is guided by principles specified in the NATO Policy of Standardization and the procedures of the Allied Administrative Publication 3 (AAP-3) « NATO Directive for the Production and Management of Standardization Documents ». A STANAG is linked to various necessities, the most important being the interoperability requirements. In the ratification process a Draft STANAG is submitted to the allied nations which are expected to formally reply with an implementation schedule. A STANAG can therefore not simply be adopted through a silence

procedure as national implementation remains the crucial key to achieve interoperability goals.

A new option for decision makers is the Standardization Recommendation (STANREC). It is like a « code of practice » that can be adopted by through a silence procedure and it does not require a formal statement for national implementation. Therefore a STANREC is a more flexible adoption system for publication of standards not necessarily related to interoperability.

**Tomorrow**

There is ample corroboration that more integrated Maritime Situational Awareness or Surveillance holds an enormous positive potential for all parties involved. Sector-oriented worldwide cooperation is taking place on organization and coalition level on matters relating to border control, maritime safety and security, fisheries. In the European Union the WISE PEN Team was formed to evaluate the possibilities for an inter-governmental and inter-services approach and civilian-military co-operation.

One result was the first consultation between the three pillars of border control, Frontières Extérieures (FRONTEX) and the European Maritime Safety Administration (EMSA) for maritime safety, and the European Defence Agency (EDA), being responsible for security and defense matters. Further work in a concerted fashion is needed to achieve appropriate Maritime Situational Awareness (MSA, NATO) or Maritime Surveillance (MARSUR, EU) for the benefit of all users and their different tasks. Progress in this area will render surveillance more efficient and maritime government functions more effective both in operational and economic terms.

The creation of integrated networks delivering Maritime Situational Awareness data from surveillance, monitoring, tracking, identification and reporting in a network centric approach must answer some basic guide lines: the right information (1), in the right place (2), at the right time (3), in the right format (4), for the right user (5), and in the right amount (6).

Legal frameworks are necessary for the establishment of integrated Maritime Surveillance or Situational Awareness networks. A singular network covering all aspects is an unrealistic approach due to the difference in the tasks of all involved

agencies and governmental organizations as well as the different structure of coalitions and political organizations.

A more promising and realistic approach is the interfacing of national systems and networks. Progress towards solutions will only be achieved with clear definitions of operational requirements, but it involves also four major areas like politics (1), legal affairs (internal and external) (2), technical (standardization, interoperability) (3) and organisational and administrative responsibility (4). All these four requirements must be observed to ensure a smooth progress towards the ultimate aim of safety and security and the six basic guidelines must be followed to avoid an information overflow for users by linking the seamless entities.

A further key issue is the protection of personal data, sensitivity and/or confidentiality. In general confidentiality means that data may not be passed to third parties that are not bound by the same confidentiality rules as the agreed recipients. The same principle applies for personal data. The core of situational awareness (or surveillance) initiatives is therefore based on national, international and community or organizations laws and security measurements and information management.

In the European Union projects like the Privacy and Identity Management for Europe (PRIME) are designed for a user-driven data security with an effective Identity Management and e-security for Internet, e-mail, mobile phone and collaborative work groups. Following PRIME, the project PrimeLife covers subjects like social networking and other services. The EU project Future of Identity in the Information Society (FIDIS) evaluates Identity Management in e-government covering aspects like e-pass, RFID, electronic documentation, user identity and verification in logistics and locally based services under « Ubiquitous Computing » (always present computing).

Obsolete standards are still being used in systems and agreed new standards are not fully implemented. Countries being a member of NATO and the EU are facing the challenge of harmonizing these in national systems. Real problems arise, when Standards one the same subject from NATO, EU and other organizations start differing. Nevertheless standardization is one key towards Interoperability, which has three different categories.

Operational (1), procedural (2) and technical (3) Interoperability require national and international military and civilian standards. As a foundation of effective joint, multinational and interagency operations, a consistent and ubiquitous provision of functional services and operational procedures must be provided, integrated and accepted by the operational and technical communities. A full integration of standards must be enforced into existing and developing command, control communication & information system as well as the weapons control including the related network architectures for cross-domain information exchange.

**Standardization of tomorrow**

Change happens in the mind. We would like one server, one screen supplying all the necessary information for a task. Each system today collects additional data to the raw data, like the history of the tracks and the investigated anomalies. There are networks with more than 100.000 tracks of vessels with the Automatic Identification System (AIS), same accounts for air or land systems. To evaluate and store all available information in one system requires immense calculation power and huge databases plus an increase of the number of trained operators and technicians. Linking these networks carries danger of duplication.

Most promising solution to enhance the global situational awareness is to connect existing national surveillance systems and to exchange only the missing tracks or the delta in information. This reduces the risk of technical failure and links all available systems into a powerful virtual computing cloud. In addition each nation decides on its own terms which information is to be released and available for data retrieval. Such a principle reduces the data traffic and simplifies the decision for release of information and IT-Security.

To solve the above issues and achieve a quicker response to operational demands - from user requirements to a finished product or system solution – projects need to be clearly determined and bureaucracy has to cut short. Important decisions must be made by experienced minds; great minds think alike.