Institut für Strategie- Politik- Sicherheits-
und Wirtschaftsberatung, Berlin

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. It offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, economy, international relations, and security and defense.

Maritime Domain Security

A Key Issue of Network Enabled Capabilities

Principles – Ways – Means

by Colonel i.G. Ralph Thiele

1. A Global Issue

Discussing Maritime Domain Issues between Korea and Germany has become a longstanding tradition. Yet, when our countries started their maritime cooperation in 1883[1], the seas were an open space where freedom was the rule. In between the character of the sea has changed. Today the sea has become a shared, global common good, vast but fragile and in need of worldwide management and protection.

The maritime domain is of eminent importance to European security, prosperity and economic stability. 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 protect the EU maritime domain and interests from damaging issues, risks and threats.

Seaborne trade originating from or flowing to the European Union is part of a global web of integrated transport systems. 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. Within the

[1] Unterzeichnung des deutsch-koreanischen Handesls-, Schiffahrts- und Freundschaftsvertrages v. 26. 11.1883

European Union a comparatively high level of Maritime Domain Security is already being provided. Yet, assaults in distant parts of the world frequently endanger and harm seafarers and present a permanent menace to vital Sea Lanes of Communication.

As trade has increased in the past decades so has the threat. Criminal acts and terrorist attacks in or from the maritime domain present major threats to Maritime Domain Security. Among the criminal acts piracy poses a direct problem for international seaborne trade. It is widely dispersed with hotspots in South East Asia and at the Horn of Africa.

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.

Consequently, Maritime Domain Security interests of the EU are at stake anywhere in the world - in the Strait of Malacca or at the Somali coast as well as in the Strait of Gibraltar or in the British Channel. Maritime Domain Security is a global issue.

2. Centre of Gravity Analysis

Operations within the context of Maritime Domain Security are those measures performed by the appropriate civilian or military authorities and agencies to counter the threat and mitigate the risks of illegal or threatening activities in the maritime domain, so that they may be acted upon in order to enforce law, protect citizens and safeguard national and international interests.

Hence, Maritime Domain Security is a broad topic covering many policy sectors, i.e.:

- Foreign policy, Defence, Security and Trade
- Sovereignty/Territorial integrity/Political independence
- Security from crimes at sea
- Resource security
- Environmental security
- Security of seafarers and fishers

Major threats to Maritime Domain Security include

- Threat or use of force against the sovereignty, territorial integrity or political independence of a nation
- Terrorist acts against shipping, offshore installations and other maritime interests, illegal transport of WMDs, unlawful acts
- Piracy and armed robbery at sea
- Transnational organized crimes, e.g., smuggling of migrants, narcotics and arms
- Threats to resource security, e.g., illegal, unregulated and unreported fishing
- Environmental threats, e.g., major pollution incidents, illegal dumping

Consequently, operations in support of Maritime Domain Security will have to focus on terrorism, proliferation, narcotic trafficking, illegal migration, piracy and armed robbery, but should also include smuggling, the protection of national resources, energy security, the prevention of environmental impact and safeguarding sovereignty.

Unfortunately, up to now there is a lack overarching frameworks to bring nations' civilian and military elements together in order to address threats to Maritime Security efficiently, coherently and collectively. National actors are conducting Maritime Security as part of routine, peacetime duties in response to the threats mentioned above. These operations are generally either conducted independently by the armed forces and/or civilian agencies in order to enforce legal powers and safeguard sovereignty or as part of multi-national military operations, which aim to safeguard common defence and security interests.

A centre of gravity analysis shows that critical vulnerabilities, requirements and capabilities need to be addressed in cooperation with national/ multinational partners, agencies and organisations to co-operate effectively to deter, protect against and counter hostile and illegal threats to safety and security in the maritime domain.

- Cr**itical Vulnerabilities**
  - National restrictions on information sharing
  - Lack of visibility
  - Lack of assets
  - Unity of approach
  - Usable data
  - Resource pressures
  - Decision making modalities

- **Critical Requirements**
  - Inter Government co-operation
  - Civil/military co-operation
  - Information networks
  - Availability of Assets, Sensors, Evaluation capacities
  - Coherence of national/organisational initiatives

- **Critical Capabilities**
  - Powerful cooperation and collaboration capabilities
  - Shared situational awareness and decision support
  - Data collection, change detection and evaluation
  - Interoperable communication networks
  - Effective tracking and discrimination of contacts through state of the art hardware (platforms, sensors, links, antennas) and software

What is needed is

- **Cooperation & Collaboration** to promote national inter-ministry, inter-governmental and multinational co-operation for Maritime domain Security along with other actors involved, taking full advantage of existing frameworks
  - To create the appropriate environment to promote the civilian-military aspects of co-operation, information sharing and maritime surveillance
  - to co-ordinate the participation and actions of all organisations and partners. This includes collaboration suites and integration of existing communication networks to an unified, interoperable network

    - to enable Maritime Security within commercial practices; providing for a better situational awareness and understanding of how the commercial shipping sector might contribute to and benefit from Maritime Security, most notably in the energy sector

- **Maritime Domain Situational Awareness** to ensure
    - improved situational awareness reflecting the existing government & defence and security structures
    - that existing maritime-related information exchange initiatives, both national and organisational, and at all levels, are enabled
    - that networks can be linked, relevant information be exchanged, and maritime pictures be improved through a more coherent, comprehensive and efficient approach
    - transforming live data into an information-led approach facilitating decision-making by appropriate national authorities responsible for and directing Maritime Security

- **Operational Force Multipliers** - capabilities strengthening Maritime Domain Situational awareness through
    - platforms, sensors, links, data and sensor fusion, change detection, decision support tools,
    - open sources intelligence capabilities,
    - knowledge development and
    - C4ISTAR facilities in order to deliver an optimised operational contribution to Maritime Security

3. A Comprehensive Approach

The Comprehensive Approach requires a systematic networking of all relevant security actors and levels of decision-making and implementation – from the international level to local levels of interaction. It drastically improves situational awareness. It increases transparency, shortens decision-making cycles, and enhances the ability to employ instruments rapidly. It ensures a deliberate and superior exploitation of one’s own possibilities and optimises – also in an interagency context – the cost-benefit equation through speed, precision, selectivity and parallel, integrated action.

Effective Maritime Domain Security relies on the co-ordinated ability to maintain a comprehensive picture of maritime activity which encompasses territorial and international waters, and to act accordingly. The Comprehensive Approach builds on knowledge, which is to be based on a holistic analysis of the challenges to be addressed. With regard to national/multinational co-operation on maritime domain awareness it needs to create a comprehensive picture of maritime activity based on accessible information. It should cover the deployment of layered maritime security from the high seas to territorial waters, including littoral areas and port facilities.

Of course security aspects need to be embedded into commercial practices. With most of world trade conducted by sea, the maritime environment delivers many goods and services that are essential for society’s needs. As the need for hydrocarbon based energy grows, the need to safeguard maritime-related traffic is becoming more acute. Co-operation and partnership with commercial shipping agencies will be vital in order to achieve a holistic approach to Maritime Domain Security which meets mutually agreed objectives of all parties involved.

In its Maritime Policy the European Union aims at approaching all aspects of the oceans and seas in a holistic and dynamic manner. The vision is to infuse cohesion and commonality into offshore functions and provide interoperability in the surveillance systems. It aims to safeguard Europeans' lives and interests by enhancing Maritime Domain Security through the integration of activities and systems associated with it. As regards the offshore activities, there is much room for the rationalisation of the cross-border and cross-sector functions which the Member States deploy on coastal waters. These include: search and rescue, fisheries inspection, activities to prevent accidents and pollution from shipping, prevention of illegal immigration, trafficking and terrorism, as well as any intentional act to put the marine environment and its natural resources in danger.

4. Awareness

Maritime Domain Awareness is the prerequisite of Maritime Domain Security. Its purpose is to generate actionable knowledge for the maritime domain, i.e. the collection, fusion and dissemination of enormous quantities of data — intelligence and information — drawn from armed forces, government agencies, international coalition partners and forces, and commercial entities. Eventually, the depth of information collected from these various sources will be woven together to enrich a comprehensive situational picture that is envisioned to be fully distributed among users with access to data that is appropriately classified. The ultimate goal of Maritime Domain Awareness, is to identify risks and threats as early — and as far from the own shores as possible. This will buy time to determine an appropriate course of action. To this end it acts as a key enabler for other critical security measures, such as the Proliferation Security Initiative, Container Security Initiative, United Nations sanctions enforcement, counter-narcotic operations, and anti-piracy patrols. Response options available range from intensified surveillance and tracking, to Expanded Maritime Intercept Operations, to the application of non-lethal and lethal force, if necessary.

The availability and management of information, data and spatial planning is vital to understanding the Maritime environment, the compilation of a threat analysis and the implementation of a comprehensive approach to Maritime Security. There are many sources of information, from open source ‘white shipping’ such as AIS, commercially available databases such as Lloyds, to comprehensive Intelligence ‘fused’ pictures, representing national, NATO and coalition interests only.

Sharing information is absolutely essential if this growing network is to effectively detect, identify and track the most dangerous threats, including terrorists, WMD, narcotics, piracy, mass migrations, and arms traffickers. Awareness generated through information sharing will enhance understanding of the global maritime environment, including adjacent ungoverned areas in which terrorists operate, thereby providing opportunities to deal with threats as far away from national borders as possible.

Maritime Domain Awareness consists of three key components: data, information and knowledge. These components are integrated into a role-based Common Relevant Operational Picture (CROP) to create a substantive, layered presentation of the global maritime environment. Numerous governmental, military and business organizations already possess valuable inputs into a CROP. However, no one source captures all of the maritime information needed or currently available. The information exchange between government agencies and with private industry, in particular, sharing common databases, is the real power behind Maritime Domain Awareness Centres.

The challenge is to effectively integrate and fuse the various inputs to achieve the synergies offered by a comprehensive situational awareness picture, while being responsive to the information needs of participating agencies. Through the CROP, specialists will eventually be able to monitor vessels, people, cargo and designated missions, business and logistical processes, areas of interest within the global maritime environment, access all relevant databases, and collect, analyse and disseminate relevant information.

At a tactical level there is a need 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 a respective area of responsibility. The role of regional and national/international situational awareness centres would be to fuse the pictures provided by local centres. They also receive information collected by priority cueing in order to focus available assets in the right areas.

5. Ports

Ports are particular vital and complex environments in Maritime Domain Security as they are exposed to security, terrorism, emergency and operational events which threaten each port's operation and the national government supply chain. Government agencies, port authorities and associated organizations must identify, collaborate, prioritize and respond to these events across organizational boundaries and disparate business processes.

The importance of ports is evident in the volume and significance of the cargo and passenger traffic handled in daily steady-state operations and in mobilizing and launching responses to global disasters and expeditionary events. These critical port operations are exposed to security, emergency and normal operating events that have severe consequences. Inherently, the complex port environments impede economic, efficient and effective port operations and security. A vast number of players and stakeholders are involved, each with their unique processes and systems. As cargo volume grows globally, there are persistent needs to balance economic throughput versus security.

National government supply chains and logistics capabilities are exceptional and complex components of global supply chains. This complexity needs be resolved through collaboration among the disparate supply chain players and by providing better visibility into and synchronization of the interdependent port operations. State of the art Situational Awareness Centres could provide a federated, near-real-time single view of an operational environment to enable a coordinated and collaborative response to any alert. As virtual operation centres – virtual in several dimensions, effectively dealing with multiple operational environments and boundaries and not tied to a physical location – they can be tailored to the operational situation and role of each user. Its multiple display may be shown in 'big board' operations rooms, on notebooks or even on PDA's. This command-and-control capability for critical operations enables near-real-time data visibility for immediate situation awareness and for business intelligence supporting current and predictable events.

Such a Situational Awareness Capability enables government port, logistics as well as commercial ocean shipping operators to focus on the operations, security, safety, economy and/or environment by having end-to-end real-time visibility of events and alerts for situation awareness and operational command and control. This enables time-critical decision making, immediate response, orderly recovery and the ability to mobilize local, national and global resources for a critical incident and to manage daily steady state operations.

Of particular relevance are

- a framework and user interfaces to initially address the requirements of a Situational Awareness for the protection of the critical infrastructure of the maritime domain, particularly ports and canals.
- an integrated, single view of operations, events and alerts to enable response to and recovery from operational, disaster, emergency, defence and security situations.
- the fusion of a diverse ecosystem of government and commercial entities, including port and maritime authorities, coast guards, navies, law enforcement, emergency and fire services, customs, immigration, health services and quarantine, inter-oceanic and regional shipping lines, freight forwarders, road and rail transportation, shipping agents, port terminals and depots
- a unified platform to surface alerts and provide the context to enable a coordinated and collaborative response.
- a role-based, cascading, federating set of Situational Awareness Centres that are tailored to each of the major participants at each port and government agency which in turn link to a national Awareness Centre to provide a national command and control system to supply overall collaboration, coordination and direction.

6. Conclusions

A comprehensive approach to Maritime Domain Security would better safeguard common prosperity and security interests by protecting and supporting legitimate activities while countering the threat of current and emerging terrorist, hostile, illegal or dangerous acts within the maritime domain. By ensuring freedom of navigation and commerce, it would also promote regional, and contribute to global, economic stability and protect maritime trade as the heart of the regional and global economy.

Ensuring Maritime Domain Security requires strong and enduring partnerships between civilian and military authorities. This partnership can build on separate initiatives already in place and the respective strengths of relevant actors in the domain of Maritime Security.
Enhanced cooperation concerning Maritime Domain Security is in the immediate interest of any state involved in maritime trade and capabilities are either already existent or can be built up in an international co-operative manner. Criminal activities and terrorism could be deterred significantly by concerted action that improves the presence of maritime security forces, enables the boarding of suspicious vessels according to internationally agreed legal rules and provides Maritime Domain Security by Maritime Situational Awareness and integrated civil-military capacities.

Particularly the timely fusing of maritime information is an initial priority. Incremental gains in information sharing could allow operational co-operation to develop as mutual confidence builds. For an inter-agency approach to work it must draw together the strengths of the relevant organisations involved in addressing Maritime Domain Security. In better use of limited resources to address the omnipresent, multi-national threat in the maritime domain the output would be most valuable to governments, international organisations and the commercial sector as well.

***

Remarks:

Opinions expressed in this contribution are those of the author.

Lecture given by Colonel i.G. Ralph Thiele, Chairman of the Political Military Society (PMG), Germany, at the International Workshop "Maritime Security – Challenges and Opportunities",, co-hosted by the Konrad Adenauer Foundation Korea, the SLOC Study Group Korea, the Yonsei-SERI EU Centre and Institute of East & West Studies, Yonsei University, February 16, 2011 in Seoul, South Korea.

Ralph Thiele

ISPSW Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung
Berlin, Germany
www.ispsw.de