Civil-Military Research Agenda for Maritime Security [1]

18 Dec 2017

Context & objectives

The activity to build up a "Civil-Military Research Agenda for Maritime Security" has been requested by the implementation of Action 5.2.4 of the EU Maritime Security Strategy (16 Dec 2014), later reconfirmed by the European Defence Action Plan (30 Nov 2016).

Council of the
European Union

Brussels, 16 December 2014
(OR. en)

17002/14

Subject: European Union Maritime Security Strategy (EUMSS) - Action Plan

5.2.4. Consider the establishment of a network of R&D experts to create a clear vision and propose a cross-sectoral agenda for maritime security research. The participating experts will be sourced from end-user authorities, research and industry, and will include representatives of Member States, Commission, EDA and EEAS. This network will:

a) Identify capability gaps requiring technological solutions and also promising innovative technologies that will have dual-use or cross-sectoral benefit. These may relate to, among others, maritime surveillance and situation awareness, information sharing, unmanned systems, environmental and energy aspects and innovative sensors;

b) Assess recent and current R&D funding programs (FP7, Horizon 2020, EDA R&T programmes) to determine if coordination on identified and/or possible dual-use and cross sectoral gaps are adequately addressed, including standardization, harmonization and interoperability objectives;

c) Work towards a joint civil-military research agenda for maritime security research based on the above analyses. [MS/COM/EDA]

[1] The text was compiled and edited by the European Commission's Joint Research Centre

EUROPEAN
COMMISSION

Brussels, 30.11.2016
COM(2016) 950 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS

European Defence Action Plan

In line with the objectives of the EU Maritime Security Strategy[70], dual use capability solutions can ensure that both military and civilian authorities could benefit from relevant technologies, products and services. Such solutions developed by the defence industry could be effective in addressing security-related fields, such as maritime surveillance, risk management and protection of critical infrastructures.

By 2018, the Commission will, in cooperation with the High Representative, EDA and Member States, develop specific actions to support a co-ordinated civil military maritime security research agenda and interoperable maritime surveillance capabilities.

The objective of the "Civil-Military Research Agenda for Maritime Security" (MRA) is to create shared awareness between the civilian and the military R&D communities, in order to enable better decisions on investments and prevent unnecessary duplication of efforts. The agenda is not associated with any new or dedicated funding source.

The work on developing the MRA lasted more than one year and took into consideration:

- Existing Research, Technology and Development programming;
- Perceived priorities;
- Inputs from Member States, EC, EEAS and EDA in collaboration/support with Industry and the research community;
- Outcomes of two workshops:
    - 6 April 2016 with Member States experts,
    - 28 Sep 2017 with Industry representatives and MS experts.

Research agenda main topics

The final MRA is organised under nine main topics, as follows:

1. Maritime Surveillance – Concepts, Systems, Sensors, Platforms
2. Interoperability, Information sharing and Cybersecurity
3. Environmental compliance, Energy and Life cycle
4. Decision support systems
5. Port and sensitive area protection
6. Autonomous systems, Networking and Communications
7. Sensor allocation and Modelling
8. Maritime security studies
9. Multi-purpose platforms

Each of these topics is elaborated in the following.

Topic 1. Maritime Surveillance – Concepts, Systems, Sensors, Platforms

Why

Situational awareness in the maritime domain is the first prerequisite for any governance, management or action at sea. Situational awareness needs maritime surveillance (the term here is understood as obtaining information pertaining to the maritime domain). We need to know what vessels are in our maritime area of interest, what they are doing, and in particular, if they pose a problem. Many government branches with different remits are interested in this, but already the Commission's initiative for Integrated Maritime Surveillance (since 2008[2]) and the Wise Pens report (2010[3]) recognised that the information requirements of all these government branches, civilian as well as military, overlap to a large extent.

State of the art

Maritime surveillance is a mature operational task that has been practiced for a long time. However, like many other fields, it has seen some recent step changes following the introduction of new technology. In particular, the AIS ship self-reporting system has led to a wealth of new data on ship traffic. Furthermore, satellite imaging is providing global coverage, and unmanned platforms increase surveillance capabilities, as do improved sensors and improved communications means. Satellite imaging has limited reactivity due to the restrictions imposed by the fixed orbits, but at medium resolutions (4-10 m) commercial offering is promising to tackle that by deploying large constellations. High-resolution observation satellites (<= 1 m) are still expensive, but some systems share civil-military use to reduce the costs. How to deal with this increase of data, fusing and analysing them and combining cooperative and non-cooperative systems, has been the topic of recent R&D, but these developments still have some way to go. The relative merits of radar versus optical satellite sensors remain as well a subject of debate, given the better interpretability provided by the optical but their low percentage of availability due to day/night and clouds/haze.

Over The Horizon (OTH) radar is used in the US and Australia, and in a few Member States of the EU. Even if it has a mixed history, recent improvements provided by innovative waveforms, supported by additional data (like ionospheric conditions) and the current processing capabilities, can make it to another solution to enhance maritime surveillance.

What should be done

Even if we now have more information about maritime activities than 10 years ago, activities and threats have also increased. But more than that, most of the newly available information on maritime movements reflects normal, innocent, economic activity. It is still very difficult to pinpoint the actual problems and threats that are hidden in the data. To positively recognise an infringement or threat, close-in inspection is almost always needed: low-altitude fly-over, boarding and inspection at sea, or inspection upon arrival in port. While such a final step will remain necessary for the real infringement / threat cases, the number of times such inspections are done should be reduced. Small and fast targets

[2] https://ec.europa.eu/maritimeaffairs/policy/integrated_maritime_surveillance_en

[3] https://www.eda.europa.eu/info-hub/press-centre/latest-news/2010/04/25/Wise_Pen_Team_report_on_Maritime_Surveillance_MARSUR

remain problematic, because they can be ubiquitous and mostly innocent, and require short reaction times. R&D should be targeted to develop technologies and procedures not just to find and track more vessels, but to specifically pinpoint high-risk ones. Solutions could be found in: better sensors; better platforms; better communications; better data analysis; and better concepts of how all these components can work together. "Better" covers both higher performance, more targeted at the issue outlined above, and can encompass novel detection methods such as using RF emissions or non-imaging SAR. It also covers lower cost so that more units can be deployed – the maritime domain is still characterised by its wide extent and its remoteness, requiring a large surveillance capacity to be sure no threats are missed. Unmanned systems are used operationally by the military, and although their use in civilian contexts is not yet mature, the technical and regulatory development toward their use is taking place. Wide civilian acceptance in particular requires low-cost unit solutions. 'Unmanned' in this topic refers in the first place to remotely piloted. For autonomous systems the challenges are bigger, but autonomy is very important and therefore treated in a separate topic (number 6). The air traffic insertion issue is something to be solved as quickly as possible in order to exploit the full potential offered by RPAS (Remotely Piloted Airborne Systems), so investment and agreement on common standards by the civil and military communities is needed urgently.

One way to reduce close-in inspections is to be able to detect more from a distance, using improved sensors (e.g., remotely estimating the number of people on board). Another way is *persistent* surveillance and tracking of all vessel traffic over a wide area; while this is now possible for cooperative targets (AIS), it requires unmanned (and low-cost) platforms to also cover the non-cooperative targets. This facilitates knowledge of the provenance of each vessel, which in combination with its behaviour is a very strong risk indicator. Neither way is possible now, but might be attainable with improved technology.

OTH radar still requires more Research and Technology investments. Both the possibilities of Surface Wave Radar and Ionospheric propagation should be analysed for specific threat detection.

(The next topic below discusses some further aspects related to information sharing and data fusion.)

Recommended actions for implementation

R&D projects to use big data and artificial intelligence technologies like deep learning, for the extraction of patterns in data and the identification of abnormal behaviours.
Development of supporting measures to help with integrating developed anomaly detection methods into existing sea surveillance systems.
R&D projects toward the affordability of wide-area persistent surveillance for non-cooperative targets, including dedicated attention to (a) sensors, (b) platforms and (c) complete systems and their concepts of use.
R&D project on improved sensors for stand-off detection of ship loads (e.g., estimating number of persons on board by acoustic or micro-Doppler; estimating weight and density of cargo on board by analysing ship motions and acoustic probing; detection of CBRNE materials).
R&D projects on sensor concepts that are novel to civilian use such as detection of RF emissions, non-imaging SAR, and non-cooperative target recognition by radar.
R&D projects in Over The Horizon (OTH) radars taking advantage of enhanced waveforms and innovative signal processing techniques.
Development of common standards for air traffic insertion to support the use of RPAS in maritime surveillance applications.

Topic 2. Interoperability, Information sharing and Cybersecurity

Why

In order to make good decisions, the available information needs to be sufficient. We would like to find threats at sea directly, which needs only one bit of information (threat / no threat), but that is not possible. Therefore, today's maritime surveillance paradigm is based on collecting as much information on the activities at sea as possible, and then deduce risk indicators from analysis of this. This information (a large amount) is collected by a wide diversity of sources, and needs to be amalgamated. It also encompasses information from the port and land side related to the supply chain, economic parameters, etc. This demands interoperability of the information systems and a disposition for information sharing. In addition, interoperability of equipment is needed for joint operations.

A different aspect of interoperability should be taken into account when dealing with assets like RPAS, which have been identified as very good resources for maritime surveillance; there, it is a prerequisite for a modular design, which enables more economic solutions.

At the same time, however, linking up systems and making data more easily accessible introduces additional cybersecurity risks, which are a serious concern today.

State of the art

APIs (Application Programming Interfaces) have boosted software interoperability. Interoperability and information sharing concerns not only data interfaces (software) but has also strong legal, cultural, motivational and ethical aspects. Interoperability of equipment also concerns hardware standards. CISE (Common Information Sharing Environment for the Maritime Domain) is a major initiative seeking interoperability for data sharing at desired and accepted levels in Europe. INSPIRE is another, related EU initiative (regulation). NATO is advanced on standards and interoperability for the defence side. A basic type of problem with interoperability of information (exchange) is that attributes or categories are defined in incompatible ways in different systems (e.g. attribute, by weight vs. by volume; category, aggregated in two classes vs. in three), which makes unambiguous conversion impossible. In many areas, a gradual move from proprietary standards to open ones can be observed.

Cybersecurity to counter today's serious and growing threats is receiving much attention; however, the maritime domain probably deserves dedicated attention.

What should be done

Work on setting EU-wide (maybe global) standards for the description of information (attributes, categories, etc.) should continue. The common use of specific APIs for interoperability could be considered. The aim should be that newly developed systems will provide information according to (open) standards that enable conversion (are interoperable). This can be done independently of progressing on the other aspects (willingness to share, legal aspects, etc.) which also needs to continue in parallel. There are already numerous civilian and military networks that can provide information necessary to detect potential threats when they arise. However, in order to allow for a timely response, a proper consolidation of these systems and a common analysis would be required. 'Soft' standards may be useful because they are more easily accepted – such as proposed definitions on capabilities, functions, and technical & operational requirements.

While designs for future systems may be optimised for interoperability, existing systems will remain around for years to come, so some investments in better linking those up is still worthwhile.

The previous topic mentioned the growth spurt of observation satellites. The exploitation of big data for analysis has started and should be developed further. Not only is the amount of maritime sensor data quickly growing, also the incorporation of data from other sources such as social and economic ones shows promising results for better assessing risks and threats. A part of the information needed for maritime security is related to trade and the supply chain, and is in the domain of transport logistics operators; some of this information is mandatorily and routinely provided to (port) authorities. The standards for this information should also be taken into account, with a view to improving the efficiency of normal commercial operations while at the same time making use of this information for security purposes. Initiatives like CISE can help in bringing the data from various corners together for optimal exploitation in big data analysis, also across civil and military users.

The development of standard Interoperable, Modular and Scalable Architectures (IMOSA) for the payloads would be very beneficial and would allow to take advantage of the economies of scale, when this concept is used in both security and defence applications of RPAS. This concept fosters the collaboration as it allows the IPR protection of the modules and eliminates barriers for innovation as the modules can be updated independently and through different technologies.

The risks of interoperability should be analysed – the old paradigm of 'need to know' that still limits information exchange is based on valid security concerns which should not be disregarded by the new 'will to share'. Technical approaches to assure data confidentiality and legal conformance should be further explored. Also, a lack of interoperability is a buffer against cyber risks, and probably vice versa.

Experiences with dual-usage of expensive satellite systems have sometimes left civilian users disappointed, so better sharing modalities might receive more attention.

Recommended actions for implementation

Action
Formulation of (soft) standards for information that enable interoperability, focussed on future systems that are relevant for maritime surveillance / maritime security, and taking into account commercial trade operations between logistics companies and (port) authorities.
Study on interoperability of communications systems and the capacity to share data from the different aspects of the various legislations and national constraints.
Study on the security and in particular cybersecurity risks of increased interoperability.
R&D project toward integration of (big) data from a wide variety of sources including from coastal, surface, underwater, air and space-based platforms as well as economic and social data.
Study on ways to achieve integrated and optimised exploitation of all observing satellites – single window, commercial and government systems, dual-use aspects, transparent allocation, rapid dissemination, faster tasking, early warning, cross-cueing, data fusion, global target tracking.
Development of standard Interoperable, Modular and Scalable Architectures (IMOSA) for RPAS payloads as a means to enhance the integration and facilitate European collaboration in the development of complex systems on board RPAS. (Related as well to topic 1.)

Topic 3. Environmental compliance, Energy and Life cycle

Why

There is a general imperative to minimise environmental impact, which includes working on minimum or renewable energy as well as producing less waste. The EU is committed to protecting the environment, which includes reducing energy consumption and greenhouse gas emissions, applying the precautionary principle, and reducing pollution at source. While these considerations are sometimes not the primary concern for security and defence, nevertheless pollution from regular security and defence operations is just as undesirable as that from less crucial operations. Moreover, energy efficiency and lifecycle management can actually save costs, if not in the short term then at least in the long run. Also, societal acceptance of security and defence operations is important, and may be helped by environmentally responsible behaviour, where appropriate. In the past, munitions (including chemical) have been dumped at sea as an easy solution, but now these start to cause problems; it would be better not to repeat that.

Environmental compliance is perceived as a cross-cutting issue.

State of the art

The pressure for sustainability is leading private enterprise to produce 'greener' products and services. Energy efficiency in e.g. engines and lighting has greatly increased. Security and defence users will likely find that off-the-shelf products will be utilised more and more automatically incorporating these improvements. Apart from better battery technology, it is also increased energy efficiency and new technologies to collect energy from sun or temperature gradients that give unmanned platforms their autonomy. The increasingly low cost of components and small systems leads to treating them as disposables, which only increases the high level of (marine) pollution that is now being recognised as a global problem. But at the same time, new biodegradable materials are coming out.

It can be noted that environmental compliance monitoring is an application for which some of the same surveillance systems that are used for maritime (security) surveillance are used, in some cases by civilian security operators.

What should be done

The problem of reducing the cost associated to the life cycle of unmanned vehicles should be addressed in a systematic fashion and within an appropriate scientific framework. One example concerns the cost of data analysis that will likely increase in the near future as sophisticated payloads become available. Another example concerns payload and systems integration.

Recent developments of commercial shipping that utilise batteries (zero-emission) or LNG/biofuel could be assessed for applicability in the security-defence domain.

Methods to gather energy from the environment while at sea should be further explored, to reduce pollution, reduce cost and increase autonomous range at the same time.

The environmental impact of disposable systems should be assessed, as well as the use of biodegradable materials.

Main systems (such as ships) but especially perishables (such as munitions) should take their ultimate responsible disposal into account from the start. In addition, ways to deal efficiently with historic dumped munitions should be devised.

Recommended actions for implementation

Action
Study project on energy collection for own sustenance by maritime surveillance platforms.
Study project on applicability of zero-emission / renewable fuel ship for security-defence use.
Study project on life cycle and environmental costs of unmanned vehicles including low-cost disposable ones.

Topic 4. Decision support systems

Why

Decisions can be operational/tactical (for shorter term issues) or strategic (for longer term issues). However, operational decisions can have long term impacts. Taking optimal decisions involves considering many factors. Today, decisions in maritime security are taken in a data-rich environment, indeed under data overload. But much of all this available data is often not relevant to the issue at hand. Some of the available data can add some value, but only when selected and put together in the right way. In order to make sure that all relevant factors are considered and all relevant data is taken into account as much as possible, a decision support system (IT tool) may be used.

State of the art

Decision support systems have been developed and are being used, but are often very specific for their operating environment (specific users, their capacities, their responsibilities and tasks, and the kinds of impacts that are considered). Indeed, decision support systems will always need to be so specific in order to perform optimally. Nonetheless, considering the types and amounts of data that are becoming available these days and are relevant for maritime security, different specific decision support systems can share a large part of basic commonality. One can think of functions like integrating information about the physical earth (maps, coastlines, bathymetry, seabed), about weather and ocean (winds, waves, currents, tides, sea ice), about human structures (platforms, pipelines, buoys, wrecks), about legal aspects (regulations in effect, jurisdiction, maritime boundaries), about registers (ship registers), and about human behaviour (ship routes, pattern of life). Part of this is nautical data. Some is still closely guarded commercially, but more and more is available from open sources.

What should be done

Analyse potential commonality of decision support systems for maritime security. Design methods for data collection and data fusion that can be exploited by multiple dedicated decision support systems for maritime security. Promote the use of standards (covered under the separate topic Interoperability). Special attention should be given to making use of the Copernicus services and products, but also to data from other global satellite observation systems and open sources. Also, automated methods to make use of human knowledge (expert systems) and the use of artificial intelligence should be addressed. In addition, regarding the evaluation of impacts of the decisions, a more holistic outcome could be obtained if the users of one community would also evaluate their potential decisions with the decision support systems used by other communities[4], in so far as applicable.

[4] One can think of the 7 communities (functions) recognised by CISE, or one can think of neighbouring countries.

Recommended actions for implementation

Action
A study project to identify (a) potential commonalities and the use of standards in decision support systems for maritime security, (b) new and upcoming data sources that could be exploited and (c) possibilities for cross-use of decision support systems between different communities.
Support actions to integrate decision support tools in operational environments, including in legacy systems.
Research on the use of artificial intelligence in decision support systems.
(See also recommendations from topic 7.)

Topic 5. Port and sensitive area protection

Why

By far most of international trade is seaborne, and hundreds of millions of passengers pass through EU ports every year. Being entry/exit points, ports have to combine vital security inspections with high efficiency of the commercial port operations. Their uninterrupted operation is essential to the economy, and also the military relies on commercial ports e.g. for supplies. At the same time, they are potential targets for disruption, together with other maritime/coastal (critical) infrastructure such as underwater pipelines and cables and offshore platforms.

State of the art

In the past years, maritime transport and related infrastructures have not known the same type of media interest as the aviation sector, since the maritime one has not generally been targeted by terrorist attacks. Port controls entail the collection and inspection of documents, physical inspection of vehicles, goods and people, and the use of sophisticated equipment like X-ray scanners, CBRNE detectors and biometrics devices. Port security also comprises area surveillance for intrusion, both from land and sea. Ports, being connection points in a global traffic network, are subject to global security standards, in particular IMO's International Ship and Port Facility Security Code and its EU implementation. Port security has already benefitted from a large amount of research from the civilian side, as has sensitive area protection from the military side. Nonetheless, detection success has considerable room for improvement with there being a need to further improve efficiency and reduce costs. In addition, new types of threats to the maritime critical infrastructure are emerging – cyber-threats, hybrid threats, drone-related, etc. With autonomous shipping becoming a reality, particularly for bulk trades in short sea shipping, the need for cyber-secured environments is a growing necessity.

What should be done

On the technical side, sensors should be improved to have better detection success, for all relevant items, like narcotics, weapons, explosives, CBRN materials, or hidden people. Chemical and biological detection capabilities lag behind those for radioactive and explosive materials. Portable and handheld sensor systems have the advantage to be also deployable at sea during boardings, also e.g. for biometrics sensors.

Perimeter and area surveillance systems should be improved, which includes further automation and less dependence on visual inspections; both on the land side and the sea side (underwater in enclosed surroundings). Loitering airborne platforms (like balloons) are suitable to monitor ports and sensitive areas and their approaches, but while military solutions have been developed for that, their costs should be seriously brought down for uptake by civilian users. Cyber, hybrid and other new types of threats should be given attention in the context of port operations and security of maritime critical infrastructures. The resilience of ports and other maritime/coastal critical infrastructure needs to be actively improved, including obtaining better insight into how the military is impacted by disruptions in civil ports. The protection of minor ports should not escape attention.

The considerations about unmanned / autonomous surveillance systems and networking that are discussed under the other topics are of course also relevant in the context of port protection.

Recommended actions for implementation

Action
A study to find how military users can take advantage of recent developments in port security, and how civilian users can take advantage of recent developments in military area protection.
R&D into further improvement of sensors for close-range detection of threats (ref. the same under topic 1 for stand-off detection).
R&D into a network of heterogeneous distributed sensors for port protection with the inclusion of CBRN, forward scattering radars, acoustics, optronics, etc.
Study to analyse the cybersecurity dimensions in ports and ships in order to decrease their vulnerabilities. (Related to topic 2.)
(See also topic 9.)

Topic 6. Autonomous systems, Networking and Communications

Why

We are currently witnessing a paradigm shift concerning the deployment and operation of unmanned systems at sea – above, at and under the surface. Small units, i.e. platforms with propulsion, sensors, processing and communication functionality, without a human operator, are becoming a reality at acceptable costs. This promises revolutionary improvements and additional capabilities in areas such as maritime awareness, protection of critical infrastructure and hydrography, but also for commercial activities (oil and gas), that should be exploited.

State of the art

The trend is particularly visible in civil applications that require networked autonomous systems to self-organise and operate collectively for extended periods of time, on the order of months or even years, without close supervision of human operators, and adapt their organisation and monitoring strategies in response to on-line perceived events, yielding a persistent presence at sea. Examples include: a) deployment and operation of networked autonomous systems for the inspection of critical infrastructures such as offshore wave and wind energy facilities, b) automatic deployment of, servicing, and data retrieval from underwater benthic stations and groups of benthic landers, as well as inspection / monitoring of the environment in the neighbourhood of the structures deployed, c) automatic deployment and cooperative operation of underwater networks equipped with passive acoustic sensors for the detection of intrusions in protected areas, and d) operation of large groups of autonomous underwater vehicles equipped with acoustic sensor suites to fully automate geophysical and geotechnical seismic surveying operations, with far reaching implications on the surveying of selected regions for the commissioning and decommissioning of underwater infrastructures and seabed mineral / hydrocarbon reservoir exploration. The above mentioned goals will require the use of advanced technological systems standing in sharp contrast with currently available networked autonomous systems that require extensive human operators / systems interaction for the execution of challenging missions. There are big overlaps with military applications.

How to ensure that an autonomous platform that has left the view of its owner is not tampered with, or how to deal with an autonomous platform that wants to dock in a port that it not its home, are open issues today.

The Vessel Data Exchange System (VDES) is currently being defined under international agreement as an extension to the AIS ship reporting system, to bring commercial shipping into a global communications network.

What should be done

This calls for the development of systems that will provide to a large number of underwater, surface, and air assets working in cooperation, the capability to: i) exchange information among themselves using advanced acoustic and optical communication networks, the latter for communications at short ranges, ii) make decisions collectively (based on in-situ acquired data) regarding motion planning and sharing of complementary resources, and iii) subsist on energy they collect from the environment. Furthermore, some of the systems developed should be able to: i) interact physically with the

environment using for example robotic manipulators, ii) perform long duration bottom-resting operations, iii) be deployed from manned or unmanned vehicles, iv) form computational clusters capable of high performance computing, and v) perform unmanned-manned teaming. Besides keeping the current R&D efforts on unmanned autonomous aerial vehicles, R&D efforts should be intensified on so-called intervention autonomous underwater vehicles (IAUVs), a subject that has hitherto only been tackled in a very small number of international projects. Further development and application of artificial intelligence tools is essential.

Besides local communications, also Beyond Line of Sight (BLOS) data transfer is needed, for which efficient communications solutions need to be further developed.

Concepts of operations involving autonomous assets should be developed, and as an aid to discussions it could be considered to define commonly agreed autonomy levels. Liability aspects but also trust and integrity aspects should be studied.

Recommended actions for implementation

Action
Research projects on autonomous systems operating in a network, including manned-unmanned interaction and human control (minimised but not absent).
R&D projects on the communications aspects of networked maritime systems, including underwater and aerial data links and SATCOM for BLOS communications.
R&D projects on intervention autonomous underwater vehicles (IAUVs) and unmanned vehicles that can cross the air-water boundary.
Studies on concepts of operations with autonomous platforms, including the aspects of integrity, trust and liability.

Topic 7. Sensor allocation and Modelling

Why

Modelling and Simulation (M&S) is a very broad subject that gives the possibility to computationally test different conditions through the abstraction of the features of the objects under research into models that can be used to simulate their behaviour and their interaction. In the case of maritime surveillance, meteorological and ocean conditions limit observation and response capabilities at sea. Knowing and predicting sea conditions is a classic subject. However, the increase in observation capabilities (new sensors, new platforms, autonomous operations) now enables much more flexible ways to deal with changing conditions. Spawned by the availability of advanced sensor suites, networked marine robots, and embedded computational systems, there is considerable potential for the development of sophisticated maritime surveillance systems that effectively integrate, in a seamless manner, the different links in the chain of modelling, planning and monitoring.

Through M&S, several approaches, like the use of war games, can be applied to different scenarios and situations in order to understand better how resources and assets should be used and improve the operations effectiveness and commanders' decision making process (synergies with topic 4). Additionally, the modelling of the systems can be used for training the operators in order to enhance, in a very cost effective way, their skills and proficiency in the management of the equipment. And the modelling of sensors can quantify their additional value, which helps both potential buyers (civil and military users) as well as potential sellers (industry).

State of the art

Modelling allows for the forecasting of the ambient conditions at sea that (a) determine the performance of sensors and platforms; (b) impact on the possible materialisation of security threats, their consequences and any response to them. Based on the forecasts, assets that include autonomous systems equipped with appropriate sensor suites can be chosen and deployed in such a way as to (a) maximise their performance and (b) collect the most relevant missing data to improve the next forecasts (mission planning phase for optimal sensor allocation). Finally, after the assets have been deployed at the planned sites or along optimal routes, new sensor data are acquired that will in turn feed the prediction models used.

What should be done

In spite of tremendous progress done in the above areas separately, challenging R&D work must still be done to bring them together under an overarching effort.

Given that models can be done in very different levels, from the strategic to the tactical, the application has to be tailored and analysed in order to get the maximum benefit from these methodologies.

Modelling could be developed to cover both military and civilian user scenarios, so that products can be assessed for both markets simultaneously.

Recommended actions for implementation

Action
R&D project to demonstrate the integration of state-of-the-art elements for met/ocean prediction, risk prediction related to the occurrence of threats, sensor/platform allocation, and communications.
R&D to improve models of sensor performance in bad weather conditions.
R&D on war games methodologies supported by M&S tools to test scenarios and conflict situations to support the decision making process in the maritime domain.
R&D on M&S of the Systems of Systems used for maritime surveillance to be applied for design, operational planning and training.
Analysis of M&S methodologies from the tactical to the strategic level to maximise the effectiveness of assessment for decision making.

Topic 8. Maritime security studies

Why

This topic intends to explore the relations between maritime security and the drivers and consequences of maritime insecurity; to understand how different threats are included in maritime security; to foresight future threats; and to identify strategies, public policies and pre-emptive actions to establish sea governance and mitigate expected threats. The perspective is of course from the EU and its recently formulated ambitions and strategies regarding maritime, defence, security, global action, arctic and space.

State of the art

Already the 2008 UN Secretary General's Report on Oceans and the Law of the Sea has identified a number of threats commonly included in the concept of maritime security: (1) Piracy and armed robbery, (2) Terrorist acts, (3) Illicit trafficking in arms and weapons of mass destruction, (4) Illicit trafficking in narcotics, (5) Smuggling and trafficking of persons by sea, (6) Illegal, unreported and unregulated fishing and (7) Intentional and unlawful damage to the marine environment. Furthermore the EU Maritime Security Strategy clearly identifies the threats to the EU maritime security interests and addresses them through the implementation of the Action Plan. The EU itself has built up an extensive structure of institutions, committees, agencies, operations and corpus of legislation, policies and strategies that in some way or other relate to maritime security. The maritime security concept can also be correlated with different concepts, establishing a matrix that points to different dimensions of maritime security, such as: economic development, national security, energy security and human security. In the same vein, recently the notion of hybrid threats, being coordinated hostile actions that arrive via a multitude of means, has been recognised. There is a general move from a narrower perspective of security to a wider perspective of resilience, which includes the role of civil society and recovery after an adverse event.

When it comes to sharing of technologies and of information or data between the civil and military sides, the flow from civil to military is much easier than the other way around. This is for good reasons, but an indiscriminate one-way flow will lead to losing out on significant economic benefits and on gains in resilience.

Crowdsourcing of data is a new concept that enlists private individuals and entities to collectively act as a big group of data gatherers. Especially out at sea where data are anyway sparse, methods have been tested for commercial ships to share their information such as their local radar- or AIS picture; while the technical feasibility has been demonstrated, there is no wide uptake yet.

Many maritime security studies have already been conducted at national level.

What should be done

In general, the broad scope of understanding maritime security should be improved, so that responses can be optimised not just for micro-impact but also for macro-impact. In such an effort, in particular the

new EU Global Strategy[5] and its very recent Implementation Plan[6] should be taken into account. In relation to the EU itself, it could be explored how maritime security in the EU could be comprehensively (re-) structured and managed to address internal and external security and civil and military responsibilities, to optimally respond to meeting the challenges that the European maritime domain and the neighbourhood will likely remain faced up with in the decade ahead.

More explicit attention could be given to consider which technologies and data that are now seen as exclusively military could be shared with civilian users, e.g. in the areas of maritime awareness and cybersecurity.

Schemes to incite commercial operators to join in crowdsourcing efforts for maritime surveillance data while ensuring the integrity / accuracy of the data should be studied.

The studies on maritime security that have been done at national level could be collected together in one place, to get a better overview of the available knowledge and facilitate sharing and access. This would enable to better exploit this existing knowledge, derive synthetic results and identify possible existing gaps.

Recommended actions for implementation

Action
Collect existing (national) maritime security studies in one place and facilitate their access by an indexing effort.
Multidisciplinary study projects on the broad context of maritime security and the extension to resilience.
Explore how to fully exploit existing doctrines to enhance the management aspects of interoperability and surveillance, covering also the future governance of CISE (ref. Topic 2).
Run cost-benefit studies on sharing military maritime surveillance data and military cybersecurity tools with civilian security users.
Explore how commercial shipping data could be shared to facilitate the enhancement of the situational awareness while safeguarding shipping companies' sensitive data and ensuring data integrity.
Carry out forward-looking studies on enabling technologies and assets capable to support the EU role of providing global security.

[5] A Global Strategy for the European Union's Foreign And Security Policy, June 2016

[6] Implementation Plan on Security and Defence, 14392/16, 14 Nov 2016

Topic 9. Multi-purpose platforms

Why

Military users in order to save costs are increasingly looking for multi-purpose platforms, possibly in a modular approach, including configurations with engagement capabilities. While such capabilities, and in particular armaments, in first instance seems a purely military topic, this aspect still needs to be considered. Any platform that seeks to be fully successful for both civil and military use should not exclude the option to host armed modules. In addition, systems used for guarding purposes in civil security may need to be capable to fend off attacks or disable intruders, which becomes challenging when unmanned systems are used. Non-lethal weapons are the first choice for civil security, but also military users are assigned tasks where these are preferable.

State of the art

Recent developments in armaments are electric power based: high energy lasers and railguns. This reduces dependence on ammunition and makes electric power the primary weapons resource, which might facilitate modular designs of systems / platforms where the weapon is an optional module.

Non-lethal weapons are available in many kinds, and novel ones include e.g. high intensity sound, or the deployment of nets to counter flying drones or propeller-driven vessels. Laser weapons that are currently being developed have the capacity of adjusting their power on a continuous scale in order to only incapacitate systems instead of destroying them. Also jamming and electromagnetic pulse may be used to incapacitate in particular unmanned systems.

What should be done

Modular systems with platforms that can choose to mount different payloads depending on the task at hand, amongst which payloads with engagement capability, should be developed taking into account both civil and military use. This should lead to better economies of scale. The use of measured, non-lethal, force by unmanned platforms should be better evaluated, both for civil and military scenarios. Counter-drone measures can be further developed.

Recommended actions for implementation

Action
R&D on including optional engagement capabilities in a modular dual-use platform design.
Studies on the use of measured force by unmanned platforms in civil and military scenarios.