“Improving Awareness to address a Changing Security Environment in the Maritime Domain”

2019 MARITIME SECURITY REGIMES ROUNDTABLE

REPORT OF PROCEEDINGS

INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

1. INTRODUCTION.

1.1. BACKGROUND.

As a part of its Programme of Work (PoW), the Combined Joint Operations from the Sea Centre of Excellence (CJOS COE) is actively involved in identifying gaps, seams and shortfalls in Maritime Security including the critical requirement to maintain Maritime Situational Awareness (MSA). Furthermore, CJOS COE determines ways and means to address these gaps to improve the effectiveness of global MSA as well as interoperability of all key stakeholders in the maritime domain.

Enhancing the MSA Network' is one of CJOS COE's projects in its PoW for 2019. Its purpose is to identify the key maritime security stakeholders (nations, NATO, law enforcement agencies, international organizations, non-governmental organizations, etc.), to develop an engagement matrix with their contact data, and to identify what information exchange requirements are needed and which protocols should be established for the purpose of improving MSA.

The key to success is improved cooperation between key players, particularly amongst Maritime Security Regimes (MSR), a term used to describe a group of states and/or organizations who act together within an agreed framework of rules and procedures to ensure security within their regional maritime domain. Since 2008, CJOS has contributed to this effort by holding the Maritime Security Conferences, later renamed 'Roundtables' (RT).

MSR Roundtable Series

The inaugural MSR RT meeting was held in Madrid in June 2015. The second MSR RT was hosted by the CJOS COE at the Slover Library, Norfolk, Virginia, USA, in April 2016. The results of both conferences were presented by CJOS COE in Kiel (June 2016) upon COE CSW invitation.

The third MSR RT meeting (2018 MSR RT) was hosted by CJOS COE in Norfolk in April 2018.

Recently, the fourth MSR RT was hosted again by CJOS COE in Norfolk, on 30 April and 1 May 2019.

1.2. OBJECTIVES.

The establishment of a comprehensive MSA network through mutual support of Allies and Partners will provide for the identification of appropriate communications and exchange mechanisms, which will ensure the best possible information is shared as effectively as possible in support of enhancing global MSA. This is what drove CJOS COE to host this event, in partnership with three other highly qualified organizations specializing in the maritime domain: the Centre of Excellence for Operations in Confined and Shallow Waters (COE CSW), the Turkish National Maritime Security Centre of Excellence (MARSEC COE) and the NATO Maritime Interdiction Operational Training Centre (NMIOTC).

The continuing message from the previous MSR RTs and Conferences since 2008 is that we must improve cooperation and understanding between key stakeholders and regimes (merchant shipping community included). Naturally, there are certain national and commercial barriers to be overcome, but generating confidence and trust among members over time will facilitate the necessary cooperation.

Trust and confidence in the maritime domain requires an understanding of time, space, risk, oceanography, the global supply chain, critical infrastructure and the environment, as well as an understanding of the nature of the threat, and the capabilities, readiness and location of multi-agencies assets capable of responding to that threat, prior to setting the information sharing process.

In the field of maritime security, the numerous international processes of coordination and cooperation are based on acceptance of the importance of the world's seas and oceans to the wellbeing and prosperity of the people that depend on them as a global common. There is an undeniably close link between the security of the seas and the development and economic wellbeing of nations.

The protection of the maritime commons and its users is also cause for international concern owing to the increase in illicit uses of this space. Its physical conditions make it a particularly conducive environment for activities that seek to evade and undermine authority of States. Trans-national phenomena such as terrorism, organized crime, the proliferation of weapons of mass destruction, smuggling and resource trafficking, especially when combined, have an undeniable maritime dimension. Human migration, climate change and challenges to a world order based on human rights and the rule of law must be addressed in a holistic and collective approach, especially in the field of maritime security.

Finally, technological progress has brought cyber vulnerabilities to the fore. The maritime shipping industry has exploitable vulnerabilities, and more needs to be done to counter emerging threats. Shipping companies such as Knutsen OAS have switched their focus from piracy to cyber defense, as there has been an increase in cyberattacks against this industry. Shipping companies have taken several measures to prevent future cyberattacks,, but there is still much to do to attain the goal of a secure environment when it comes to cybersecurity, a landscape that changes rapidly and deserves to be included in every MSA meeting.

Taking into the context stated above, the following were the principal objectives for the 2019 MSR RT:

- Identify the contemporary challenges with improved information sharing and collaboration among the MSRs from across the global maritime community of interest;
- Identify and share how all stakeholders can contribute to the security of the sea and its lines of communications;
- Examine the role of law to improve MSA, information sharing, and the timely response to evolving security threats; and.
- Underline the importance of cyber intelligence in maritime security, addressing its scope and challenges, including hybrid threats.

1.3. STRUCTURE/METHODOLOGY.

The forum was conducted at the unclassified level and the audience (approximately 90 participants) was drawn by invitation from an international community of maritime security practitioners. This included a strong cross-section of government, non-government, military, academic and industry stakeholders in a collaborative setting to discuss the challenges to building, maintaining, and sharing maritime security information, and to propose solutions that contribute to an enhanced global network for MSA – the foundation of effective maritime security.

The theme of the 2019 MSR RT was 'Improving awareness to address the changing security environment in the maritime domain.' Employing the successfully proven panel format from previous events, the 2019 MSR RT was structured around 4 panels. An introductory presentation was given by the panel chair framing the subject of the panel discussion, followed by a number of panelist speakers, each providing their perspective on the themes based on individual backgrounds and experiences. Each panel's theme and supporting presentations were designed to trigger questions and stimulate discussion. Organized by one of the four co-hosting COEs, each panel was asked to examine one of the different sub-themes, developed from findings and recommendations from the 2018 MSR RT Report of Proceedings as well as from additional themes proposed by the co-organizing centers:

- **Intelligence, Surveillance and Reconnaissance (ISR) and Governance in the Maritime Domain**. Discuss the ways to improve the basic maritime data and information at the appropriate level in maritime domain, both at the national (cross sector) and international (cross border) levels; identify and share how ISR operations can be adopted by all stakeholders, civilian and military, in order to contribute to the security of the sea and its lines of communications, and form the basis of an agreed Governance structure for improved information sharing and collaboration among the MSRs from across the global maritime community of interest.

- **Cyber Defence against Hybrid Threats in Maritime Domain**. Highlight the cyber threat rising in maritime domain and discuss how cyber capabilities are a critical enabler of success across all missions, and ensure that these capabilities are leveraged by commanders and decision-makers from tactical, operational and strategic level.

- **The role of Cyber Intelligence in Maritime Security**. Underline the importance of cyber intelligence in maritime security, and of cyber security in commercial maritime industry; define the main cyber risks and threats and how to address them.

- **Legal Considerations, Strategic Priorities and Achieving MSA Requirements**. Examine the role of law to improve MSA and to better position the acquisition of data, information sharing; identify anomalies, and have a clear awareness of evolving security threats and timely responses to address them.

With these themes, the aim of the 2019 MSR RT was to achieve a better understanding of the current global MSA environment, examine what is/is not working, and determine the best practices that can be employed amongst the maritime stakeholders to globalize MSA.

The intent was to continue providing a worldwide focus for the RT and have participants coming from the maritime community and other concerned actors representing as wide a perspective as possible.

Report of Proceedings

A team from CJOS COE with the aim of determining key points and security themes analyzed each speaker's presentation, along with subsequent questions and comments.

The result of this analysis and final product of the MSR RT for all participants is this Report of Proceedings. This report provides a number of findings, recommendations and conclusions, drawn from the discussions and subsequent CJOS COE´s team analysis. To get the most out of the report, read it in conjunction with the individual presentations, which are posted on our website (www.cjoscoe.org).

Engagement Matrix

CJOS COE invited civilian and military professionals from around the world who play leading roles in maritime security affairs in their respective nations or geographic regions. CJOS COE considers the identification of these experts, as well as the other attendees, its main effort and one of the most critical aspects of a successful output. The list of professionals invited by CJOS COE to this and former MSR RTs is called 'CJOS COE MSR List of Contacts' or 'Engagement Matrix', and can be made available upon request.

1.4. THE MSR RT ROADMAP.

In order to ameliorate the loss of momentum between annual plenary events, the idea of developing the MSR RT into a persistent on-line forum was adopted this year.

This forum is being used as a framework for smaller working groups that remain continuously engaged in their respective maritime security-related themes. Whilst this initiative will have a cost in terms of the group members' time, the collective benefit to all stakeholders should make that investment thoroughly worthwhile. The key is active engagement, but efficiency and ease of access is important.

CJOS proposed the creation of 3 groups:

- Maritime Situation Awareness.
- Information Sharing, Interoperability and Integration.
- Cyber Defense in the Maritime Domain.

The battle rhythm, objectives and leadership of these groups are yet to be defined in a Terms of Reference document that will be drafted between CJOS COE staff and other stakeholders. The intent is for each MSR RT attendee to be an active contributor to at least one group.

Besides the routine online work within each group, a plan is being developed to bring the groups together in a late-fall session that could be scheduled around the NATO TIDE Sprints, the annual NATO Allied Command Transformation event centered on innovation. This event would provide an opportunity to gather the groups together to develop cross-discipline work.

The MSR RT will continue each spring, as it has in years past. While all of these are excellent opportunities to come together to address Maritime Security, there is always potential for other regional MSR events (hosted by other COEs) to connect the same community and add a new perspective to the body of work and momentum.

2. PANEL SESSIONS AND KEYNOTE SPEAKERS.

Prior to the commencement of the panel presentations, the Director of CJOS COE, Vice Admiral (USN) Bruce Lindsey addressed and thanked all attendees for their presence and support of the event. He highlighted that one of the critical tenets of

success within any mission is interoperability, stating that in order to deliver the mission we must be integrated and aligned with other key enablers in the maritime operational community. Extrapolating this idea to terms of maritime security, we may contend that maritime security can only be established with the mutual support of all components of the maritime community in order to ensure the best possible information is shared as effectively as possible in support of enhancing global MSA.

2.1. PANEL 1 – ISR AND GOVERNANCE IN THE MARITIME DOMAIN.

Panel 1 aimed to promote discussions over how to improve awareness and address a changing security environment in the maritime domain. The specific objectives of the panel were as follows:

- Improve the exchange of basic maritime data and information at the appropriate level in the maritime domain.
- Identify and share how ISR operations can be adopted by all stakeholders, civilian and military, to contribute to the security of the sea and its lines of communications.
- Form the basis of an agreed Governance structure for improved information sharing and collaboration among the MSRs from across the global maritime community of interest.

Panel members:

- Chairperson: Vice Admiral (Spanish Navy) Eugenio Díaz del Río, Chief of Staff, Maritime Allied Command.
- Mr. Lee Stuart, Program Manager, Naval Cooperation and Guidance for Shipping (NCAGS), and MSA Manager, at the US Fleet Forces Command Center.
- Mr. John Hammersmark, Director, Security and Crisis Response at the Norwegian Ship-owners Association.
- Mr. George Guy Thomas, President, C-Sigma Consulting Center, creator of Satellite AIS (S-AIS), and advisor to MARSEC COE.

Vice Admiral Díaz del Río provided an initial setting for discussions by introducing the problem of the complexity of the seas, in terms of vastness of its coverage area, the challenges of knowledge over the horizon and the sheer volume of maritime related-activity, which encompasses not only good actors but also the threats, which benefit from the freedom of the seas.

He provided some definitions of Maritime Security, and divided it in two categories: firstly, the need to know what is happening at sea (MSA); secondly, what to do and with what means (Maritime Security Operations, MSO). Regarding MSA, he depicted its multi-domain, multi-spectrum, and multi-platform character.

Vice Admiral Díaz del Río then spoke on how MARCOM is pursuing MSA in the NATO Areas of Responsibility by gathering information from NATO and Allied nations' commands and forces, merchant industry, and then integrating and disseminating the maritime picture. Although the process seems simple, it has taken many years to achieve what it produces today. He referred to Operation Sea Guardian, an operation conducted in the Mediterranean by a variety of NATO assets that focuses on three permanent tasks: MSA, counterterrorism, and capacity building as an example of a MSO.

Finally, he mentioned the requirement to develop and use long range, long endurance sensors and artificial intelligence as essential to process the huge amount of data received, as key enablers for the future MSA.

Mr. Stuart provided a presentation on Commercial Maritime Industry and MSA, which included the way USFFC manages MSA and the different instructions and guidance employed in the US, an area in which the DoD has been very dynamic in its efforts.

As an expert on NCAGS, he provided his view on commercial maritime industry and how to understand them thorough the military lens. He defined the commercial maritime industry as the “life blood” of the global economy, contending that without shipping, intercontinental trade, the bulk transport of raw materials and the import/export of affordable food and manufactured goods would simply not be possible.

He underlined the importance of knowing the different types of trade and vessels to support MSA, since they must face different threats and different threats require different defence.

Mr. Stuart also spoke on sea lines of communications and choke points. He underscored the importance of knowledge of activities within these spaces, what entities are present and what entities are approaching, aas well as the ability to share that information with all partners concerned., Furthermore, from the tenet that economic prosperity is inextricably linked to regional stability and regional maritime security, Mr. Stuart asserted that illicit acts and threats to security and welfare of all nations typically cross regional and sub-regional boundaries. In this context, the role of naval power in securing the maritime domain gains in prominence, as MSA is a critical enabler for Maritime Security., This in turn is a critical enabler for economic growth, which enables a more stable international environment.

Mr. Stuart defined MSA as the effective understanding of anything associated with the maritime domain that could affect the security, safety, economy, or environment of the homeland, stating that “effective understanding” occurs when a decision maker’s comprehension of the relevant information allows him to make appropriate decisions and take appropriate actions. All nations that share the responsibility for maintaining maritime security by countering threats should subscribe to this definition.

Mr. Hammersmark provided a Norwegian shipping industry perspective on MSA and commercial shipping by showing the AIS-generated arteries of commercial shipping monitored by the Norwegian Control Fleet. He reviewed the most concerning areas for Norway, namely Nigeria and the Gulf of Guinea, Libya, the strait of Bab El Mandeb, the Gulf of Aden, and the Malacca strait, and spoke on how Norwegian shipping has contributed to MSA process by active and aggressive reporting.

Norway established a Maritime Security diagram composed of a triangle whose sides are represented by 1) the Norwegian Shipowners Association, which plays a governing role in Contingency Planning and Crisis Response 2) the Norwegian Shipowners’ Mutual War Risks Insurance Association (DNK), which is in charge of insuring all Norwegian controlled ships from war, piracy, terrorism or cyberattacks, and 3) the ship owners themselves.

Of particular note, the sensor system used by Norway to track its shipping, “Raptor”, similar to AIS, encrypts data and therefore is almost impossible to intercept or deceive. This allows DNK to have a clear maritime picture when ships are transiting through high risk areas.

Mr. Hammersmark finished his presentation by remarking that commercial shipping can provide very valuable real-time information that can be useful to intelligence building for the military. He stated that in return, commercial entities should receive prompt responses to requests for intelligence from navies. He also mentioned the need to create a common language and definitions for maritime security issues, mentioning the International Maritime Bureau (IMB) as a potentially well-suited body to accomplish this.

The last speaker of this panel, Mr. Guy Thomas, provided a presentation on Collaboration in Space for Global MSA. He highlighted the global consequences of happenings at sea, their impact on safety, security, environment, economy and resources, and the fact that international global collaboration in the maritime domain is required for global Maritime Security, most especially from the space.

He referred to the genesis of Satellite AIS in 2008 as a milestone in bringing the maritime picture into the globally interconnected world, and concluded that in 2050 commercial space would be the crucial component to Global MSA once having compared every type of platform, from satellites to undersea in a research carried started in 2001 by C-Sigma as US Science and Technology Advisor for MSA.

Mr. Thomas presented the space domain as “the Silver Bullet” in collaboration regarding MSA. Being a new capability, overrunning classification-related issues that limit its access to all potential information providers, thus increasing maritime awareness, it will help protect the environment and conserve marine resources. Currently there are several space-based observation capabilities in force (S-AIS, synthetic-aperture radars (SAR), optical and video systems) and others are expected to be operating soon (ELINT, COMINT).

Regarding space-based MSA, Mr. Thomas noted its importance since three of the four global commons converge on it: maritime, space and cyber (AI, machine learning, big data), with major recent advances in the last two ones.

Mr. Thomas ended his presentation by suggesting the development of an International Committee, co-lead by NATO and MARSEC COE, which would include organizations of importance in Maritime Security, such as the IMO, FRONTEX, the European Maritime Security Agency (EMSA), Global Fishing Watch (GFW), etc., with the goal of developing a plan to create a Global Space Coordination Center and possibly regional centers.

2.2. PANEL 2 – CYBER DEFENCE AGAINST HYBRID THREATS IN THE MARITIME DOMAIN.

The objective of the second panel was to highlight the rising cyber threat in the maritime domain and discuss how cyber capabilities are a critical enabler of success across all missions. Furthermore, the panel emphasized the importance that commanders and decision-makers from tactical, operational and strategic levels leverage these capabilities.

Panel members:

- Chairperson: Commodore (Hellenic Navy) Stelios Kostalas, Commandant, NMIOTC.
- Mr. Alberto Domingo, Head, Cyberspace Capabilities, NATO Allied Command Transformation (ACT).

- Mr. Christos Vidakis, Principal, Risk Advisory, Deloitte.
- Lieutenant Commander Dimitrios Megas, NMIOTC.
- Professor Maria Papadaki, University of Plymouth.

Commodore Kostalas began the panel by introducing the Hybrid Threats - how NATO and EU define (or fail to define) these threats, and by outlining covert activities from both state and non-state actors that have resulted in regime changes and territorial annexations in the past decade.

One of the components of hybrid threats are cyber threats. Cyberspace, where the majority of these threats develop, is inextricably linked to all aspects of modern life, to include Defense and Security. Cyberspace has been defined as a new operational domain (as that of air, surface, subsurface) within various sectors (industry, commercial, military, civilian, etc.), and is a major concern of NATO.

Maritime Operations rely heavily on Information Systems. This drove NMIOTC to host the 3rd Cyber Security Conference, a demonstration of the commitment within the center to tackle cybersecurity issues in the maritime domain.

Lieutenant Commander Megas provided a presentation on cyber security in the maritime domain. He demonstrated how maritime cyber threat is included among a number of threats in maritime security, the latter being considered a hackers playground, as computerized maritime systems are highly vulnerable to cyber threats. These systems are widely located: harbors and ports, navigation systems, rigs, offices, headquarters, maritime vessels. Amongst the vulnerable maritime systems are numerous systems (i.e. communications, navigation systems (GPS, AIS, ECDIS), tracking and identification systems and ship control systems)

He mentioned that the nature of “networked” maritime systems results in a series of common vulnerabilities. He gave the examples of combat communications and engineering, and position, navigation and timing systems (PNT) systems as targets. He also provided a number of examples of maritime cyber incidents, showing the resultant effects such as sensor data spoofed or blocked, data display and crews compromised, control systems and communications disabled.

He referred to human factors as the weakest link, since they are the origin of nearly all security incidents, and are often costly as they involve insiders who may have access to sensitive information. NMIOTC, along with other partners from academia, is addressing this issue and has started a course aimed at providing an understanding of the maritime cyber aspects, as well as cyber defense exercises for navies like the “Cyber Gordian Knot” which trains crews on detecting, responding, preventing, and containing threats to systems.

Mr. Domingo’s presentation theme was NATO Cyberspace Operations, and provided the Alliance’s point of view on the cyber realm. He stated that with the 2016 Warsaw Summit’s declaration, NATO recognized cyberspace as a domain in which NATO must defend itself as effectively as it does in air, on land and at sea. The ability to protect and to conduct operations in and through the cyberspace has become a pre-requisite of safeguarding the Alliance´s freedom of action and decisions in all other domains of operation. Therefore, NATO needs to move from Communications and Information Systems (CIS) and cyber defense into the ability to conduct operations in and through cyberspace.

He depicted the military tasks the Commander must accomplish concerning cyberspace in case of the military mission, namely:

- Protect and defend the Alliance cyberspace against attacks, prevent them before they happen, defend against them when they do happen, and recover from them once they have happened.
- Plan, conduct and execute cyberspace activities, including the integration of national sovereign cyber efforts
- Gain and maintain shared situational awareness of cyberspace, which can be comprised of relevant data from the technical, operational and strategic levels.

Finally, he identified challenges to NATO regarding cyberspace, including the need to update the CIS Security Policy. He stated that the current policy is insufficient to keep pace with rapidly developing technology and that the lack of contact between the Alliance and other stakeholders (industry, academia) will result in decreased interoperability The answer is to increase information sharing (i.e., trust).

Mr. Vidakis' presentation provided a business perspective on current maritime threat landscape, and two approaches to mitigate cyber risks: the Bow-Tie approach and the Real-Life approach. He also explained how through the last 10 years, cyber issues have progressed from an era of compliance, in which only known threats were addressed, to an era of risk and resilience and the current so-called "next era of cyber everywhere", focused on managing risks out of organizations' control.

He mentioned the maritime and ports industry is characterized by an elevated number of connections between assets in movement in a complex land and sea-based environment. The maritime industry is driven by a need to become more cost effective, more efficient, reliable and safer. To achieve this, it is essential to introduce digital technologies in vessel's Operation Technology (OT) and Information Technology (IT)[1] environments moving forward to the digital ship version.

Mr. Vidakis provided two samples of the maritime threat landscape. Firstly, AIS, an open by design system with its communications not including any authentication, and the resultant vulnerability of its messages being easily be intercepted. Secondly, the Electronic Chart Display and Information System (ECDIS), where a malicious person with physical access could load incorrect/outdated maps, access the underlying operating system or spread malware/ransomware.

Professor Papadaki's presentation introduced the audience to the aforementioned exercise "Cyber Gordian Knot", co-organized by her university and NMIOTC.

She began by explaining how cyberattacks represent a prominent global risk because global interconnectivity can widely affect sectors like energy, transports, funds, hospitals, digital infrastructure, etc., and how disruption in shipping and maritime industry could have far-reaching consequences.

Prof. Papadaki provided several examples of notable incidents that have occurred in the maritime domain throughout the last decade: Stuxnet Worm, GPS spoofing including on NATO exercises, attacks against ports (Antwerp, Barcelona, San Diego), showing how these can affect to trust. She stated three major takeaways:

[1] Operation Technology supports physical value creation and manufacturing processes. It therefore comprises the devices, sensors and software necessary to control and monitor plants and equipment. On the other hand, Information Technology combines all necessary technologies for information processing.

- The potential impact of cyber-attacks on critical infrastructure can be catastrophic.
- The costs of recovering from the cyberattacks effects are significant.
- Preparation is key to overcoming cyberattacks when they happen. Shipping companies are still unprepared for cyberattacks, and a vast majority of their personnel lack sufficient training. Therefore, it is necessary to consider the human element in strategy and security design.

The last bullet above refers to a general skill shortage when it comes to cyberspace. This led to the exercise "Cyber Gordian Knot", whose aim was to provide a new and unique training opportunity to navies' cybersecurity teams where they can be familiarized with current cyberattacks, and advances in cyber defense tactics, techniques and practices.

2.3. PANEL 3 – THE ROLE OF CYBER DEFENCE IN MARITIME DOMAIN.

This second panel, focused on cyber issues, had the following objectives:

- Underline the importance of cyber intelligence in maritime security, to define its gathering tools and the process of analysis for MSO.
- Describe the need for cyber security in the commercial maritime industry and to underline the importance of preparation to face a cyberattack and raising staffs' awareness.
- Define main cyber threats for the maritime environment, and
- Underline the need for Cyber Threat Intelligence (CTI) mechanisms in different levels, as well as the importance of sharing the cyber intelligence in the maritime domain.

Panel members:

- Chairperson: Captain Sumer Kayser (Turkish Navy) , Director, MARSEC COE.
- Mr. Daryl Williamson, Director, Commercial Development, Lloyd's List.
- Commander Onur Aymak, Head of Cyber Security Branch at MARSEC COE.

Captain Kayser opened the panel by explaining its objectives, and then presented an overview of Multinational Maritime Security Exercise 2018 (MARSEC-18), which was focused on terrorism at sea. He shared experiences and lessons identified from the exercise, especially regarding the cyber risks in the maritime domain.

He also focused on strategic and operational aspects of MSO and emphasized improving cooperation, collaboration and awareness amongst all maritime security stakeholders (civil and government agencies, military, law enforcement and international organizations). Additionally he mentioned the importance of Civil-Military Cooperation (CIMIC) in maritime security activities and MSO.

Mr. Williamson focused on cyber intelligence in the commercial world. He stated that the commercial realm is not as familiar with cyber intelligence as military entities are. To mitigate the risk, he reiterated the importance of information sharing and conveyed that organizations and companies are not willing to share the required information about security breaches and cyberattacks in the interest of protecting their reputations and revenue loss.

In his words, responding to complex problems require a holistic rather, than partial or linear approach. In his mind, key factors to the solution are innovative and flexible

approaches, the ability to work across agency boundaries, effectively engaging stakeholders, a comprehensive focus or strategy and tolerating uncertainty and accepting the need for a long-term focus.

Commander Aymak discussed the intersection of maritime intelligence and cyber domains and defined the cyber security essentials, cyber threats, and cyber threat intelligence in the maritime domain. He underlined the need for CTI mechanisms in different levels, and spoke about CTI processing phases and the importance of sharing the cyber intelligence in the maritime domain.

He also mentioned about the ships' vulnerabilities to cyberattacks and emphasized the importance of human factors and raising staffs' awareness in order to reduce incidents.

He finished by stating that cyber risks and incidents are growing each day and that securing the ships and harbors' systems is crucial; cyber awareness should be increased. Amongst actions to take, CTI mechanisms should be created and implemented at different levels in order to facilitate sharing fast and accurate data and information amongst organizations. Lastly, cyber incidents should be reported immediately in order to prevent further attacks.

2.4. PANEL 4 – LEGAL CONSIDERATIONS, STRATEGIC PRIORITIES AND ACHIEVING MSA REQUIREMENTS.

The fourth panel's main objective was to examine the role of the law in improving MSA, information sharing, and timely responses to evolving security threats. To that purpose, panelists discussed:

- The role of the law to better position the acquisition of data.
- The identification of anomalies.
- Awareness of threats.
- Timely responses.
- Terminology.
- National and international legal considerations.
- Best practices in managing the flow of information and integrated decisions.

Panel members:

- The panel was introduced by Mr. Jorg Schildknecht, Legal Advisor, COE CSW.
- Chairperson: Mr. Brian Wilson, Deputy Director, Global Maritime Operational Threat Response Coordination Center.
- Mr. Gary Khalil, USCG Intel Attorney/Counsel to US National Maritime Intelligence Integration Office (NMIO).
- Commander Ian Campbell, Legal Officer, Australian Navy.
- Mr. Frederick Kenney, Director, Legal Affairs and External Relations Division, IMO.

Mr. Wilson spoke about the United Nations Security Council Resolutions (UNSCR) and historical aspects of how the UNSCRs have influenced maritime security. Specifically, he mentioned how between 1947 and 2007, the UNSC adopted resolutions every year and a half with a maritime impact, and then from 2008 until today, the Security Council approved measures every 4 months, on average. This is evidence of the increased role of MSA through the last decade.

Additionally, he noted how resolutions have played a role, mostly as an umbrella, to many military operations regarding inspections on the high seas of suspicious activities or ships. Concerning this, the Security Council has addressed continued misuse of electronic systems designed to advance safety and security of interests in the maritime environment, or the execution of deceptive maritime practices. He highlighted UNSCR 2397 as an example of the Security Council's concern pertaining to any North Korea-flagged, controlled, chartered, or operated vessel that intentionally disregards requirements to operate their automatic identification systems (AIS) in order to evade UNSCR sanctions. By turning off this system, they masked their full movement history. This type of behavior requires member states to exercise enhanced vigilance with regard to such vessels conducting prohibited activities.

The contents of these resolutions highlight contemporary focus on AIS and are evidence of the evolution of this technology from its use solely for collision avoidance to its current employment as both collision avoidance and a ship tracking system.
Mr Khalil stated that the role of law is integral in all aspects of MSA. He explained that law and more importantly, lawyers, should be involved in all aspects of planning and conducting of operations from the strategic level (law and policy development, international agreements), through the operational level (developing ROE), to the tactical level (being available to support Commander's decisions).

Lawyers are enablers and can help, not only with determining the legal aspects of a mission, but also as intermediaries among commands and liaisons on policy matters with higher headquarters. It is essential to consult lawyers early and integrate them in the team from the beginning,

Commander Campbell briefed on how Australia handles maritime security and the issues that are unique to Australia. Australia has six states and 2 onshore territories, as well as 36,000 kilometers of coastline as well as a vast offshore area of interest, which makes communications and cooperation a must for maritime security.

Australia is an example of a country with a heavy component of maritime interests, with a wide variety of offshore infrastructure, principally associated with oil and gas exploitation, and communications. They have instituted a Maritime Border Command, which is the lead governmental organization for security in the offshore maritime domain Australia has developed their own Maritime Identification System (AMIS) that collects, fuses and plots positional data to persistently track target to build their maritime picture. They also have multiple surveillance and response assets to maintain MSA, in addition to a and a wide variety of legal regimes in place to protect the infrastructure, including powers to use force to use these assets that are consistent with Australia´s international obligations.

Of significant interest was the fact that 98% of Australia's voice and data communications travel via underwater cables and estimates show that about $US 10 trillion worth of commerce-related transactions run through the same cables every day. These cables are vulnerable to damage (deliberate or unintentional), especially in more shallow waters.

Finally, Mr. Kenney informed the audience on the role of his organization, IMO, to act as the global standard-setting authority for the safety, security and environmental performance of international shipping, and to create a regulatory framework for the shipping industry that is fair and effective, universally adopted and universally implemented.

His main points were about countries and ships not following the proper regulations. For example:

- Entities purporting to be authorized to act on behalf of the Administration of a country, issuing fraudulent certificates of registration, as in the case of Sierra Leona, or Tanzania. IMO has identified more than 200 ships with fraudulent registrations.
- Vessels flying the flag of a State where no international registry has ever existed (Congo, Fiji, Micronesia, Maldives, Nauru, Samoa).
- Defrauding IMO to get access to IMO web accounts (Micronesia, Nauru).

Of note was the fact that fraudulent registration and issuances of certificates are a threat to a safe and secure maritime environment due to the illicit activities they enable. This includes evading UN sanctions, migrant ghost ships, non-compliance with safety and security regulations masked by falsified paperwork, endangering the vessels' crew, and posing threat of damage to the marine environment.

The IMO produced a new module on registries within Global Integrated Shipping Information System (GISIS) by creating a "register of registries." In addition, they have recommended best practices to assist in combating fraudulent registries, and are working on an easily reachable database of vessels, by IMO number and vessel name, of vessels currently the subject of, or designated pursuant to, UNSCRs.

2.5. KEYNOTE SPEAKERS.

The MSR RT included two presentations from keynote speakers selected to raise interest in other issues not directly dealt with within the panels, but also related to maritime security issues. These were:

- Captain (Ret) John M Sanford, from NMIO.
- Mr. Alan Hope, Program Manager, Sea Link Advanced Analysis (S2A) at US Naval Research Laboratory.

Captain Sanford's presentation about "Maskirovka, Russia's masking of its real intent", started with a historical review regarding Russia's attempt to counterbalance the tactical advantage of the US' situational awareness. This began with the creation of the Maskirovka program, a denial and deception strategy formalized during the Soviet era, which included the use of wartime reserve modes (WARM), and electronic warfare-related tactics such as meaconing, intrusion, jamming and interference (MIJI).

A new, so-called Maskirovka 2.0 was designed to permit Russia to re-establish (by force, when necessary) its sphere of influence. The threat vector has expanded and encompasses hybrid threats such as:

- coercion,
- media manipulation
- fossil fuel price control,
- cyberattacks,
- political agitation,
- use of 'agents provocateurs',
- the deployment of military forces in clandestine status,
- the development of surrogate forces by providing arms, equipment training, intelligence, logistic support, and command and control, as

seen in Chechnya, Ukraine, Syria, and Crimea and also used as a strategic campaign to exploit divisions in Europe and the West.

The most conspicuous example of the effects of Maskirovka 2.0 in the maritime domain was the attack on Maersk in 2017. The spreading a destructive malware on Maersk's command and control systems seriously affected the computers' master boot records and caused at least $US 10 billion in damages.

This strategy led to the conclusion that cyber is definitely the next form of clandestine warfare attack. Conscious of the importance of this, the US issued its 2018 National Cyber Strategy and Implementation Plan. NMIO was integrally involved as the National Intelligence Manager for the maritime domain. A significant result of this was as an increase in contractual cyber standards for services and hardware, network protection, training on cyber, increase the number of port security specialists and bi-directional information sharing between US Government and the private sector.

The second keynote speaker, Mr. Hope, provided a presentation about "Sea-Link Advanced Analysis (S2A)", an unclassified tool widely used in global maritime data sharing and comprehensive MSA. For decades, MSA analysts had to manually associate millions of uncorrelated tracks to detect just a handful of vessels. Until automated multi-source data fusion tools like AIS were implemented, large scale MSA was difficult to achieve, requiring a significant amount of person-hours with only a fraction of the maritime environment being monitored on a daily basis.

By the beginning of the century, most vessels were still tracked manually, with approximately 400-600 produced daily. A few attempts to create automated trackers were tested, but none became available worldwide. The advent of AIS data increased and played an important role in expanding vessel tracking. Circa 2004-2007 several multi-source data fusion efforts were initiated, some of which evolved into S2A, a reality today that produces and maintains over 125K active tracks every day, and is available to all users.

S2A is a comprehensive MSA tool that gathers, merges, and analyzes data from a myriad of sources: commercial (although these have a cost), US Government, other partner nations, etc., which can be leveraged for a variety of maritime use cases. It contains a data aggregator, which normalizes all tracks to a specific format and provides universally unique identity number to each track, and assigns to each track the following data:

- Vessel position data based on AIS, port/coastal radar ship detections.
- Vessel schedule data, such as actual and estimated port arrivals and departures.
- Vessel metadata: vessel name, call sign, MMSI number, IMO number.

S2A supports US Navy and Coast Guard with partner nation data sharing and collaboration, so S2A fuses all US and partner data to produce a worldwide vessel-tracking picture. Its unclassified nature allows it to reside on an Internet cloud with access controlled by user PKI certificates. The data sharing is possible through Partner Data Pools (PDP) that result from data sharing agreements between the US Navy and Partners with scopes that vary on a case-by-case basis (may be limited to a specific geographic area).

Despite the US being responsible for administering and enforcing access rules for PDPs, partners always have full access to datasets that they contribute, so they can

store, view and analyze their own data and those from the PDPs they join, thus contributing to more effective worldwide MSA.

The next steps for this tool are the addition of new unclassified maritime data sources (S-AIS, RadarSat), port and shore-based AIR and radar data and continue to enhance data fusion processing.

3. FINDINGS AND RECOMMENDATIONS.

Finding 1.1. Complexity is inherent to the maritime environment. Vastness of the seas, and the huge amount of activities carried out in it makes it a challenge to achieve the desired MSA. Besides, illegal actors take advantage of the free character of seas to carry out their activities.

- Recommendation 1.1.1. Foster cooperation and build solid relationships within the global maritime community of interest to achieve a MSA that covers the entire, vast surface of the seas, thus ensuring the best decisions are made. No single nation or organization has the capability or capacity to achieve a requisite and sustainable level of MSA unilaterally.
- Recommendation 1.1.2. Focus MSA on Sea Lines of Communications and choke points, since most commercial routes are concentrated on them, underscoring the need to know what is going on there and in their surroundings.
- Recommendation 1.1.3. Support research to achieve integration systems able to merge multi-domain (underwater, surface, land, air, space), multi-sensor (EO, IR, acoustic, radar), and multi-platform (submarine, ships, unmanned vehicles, etc.) sources on a consolidated shared network.

Finding 1.2. Societies underestimate the importance of seas. Many potential stakeholders who could support the information sharing process in the maritime domain are not aware of the importance of the maritime environment for the global economy.

- Recommendation 1.2.1. Educate societies on the importance of the seas for global economy and maritime security as a critical enabler for economic growth.

Finding 1.3. There are a number of national naval MSA-related initiatives ongoing around the world, but they lack synchronization and alignment of their activities. Despite different MSA networks specialized in their respective areas of responsibility (for example, MARCOM, USFFC, other national networks like Norway or Australia), exchange of information among them is not optimal. This is critical in a globalized environment such as the maritime, within which the consequences of any issue are widespread and have the potential to affect everyone.

- Recommendation 1.3.1. Invite Maritime Operations Centers, including NCAGS sections from Allied nations, to forthcoming MSR RT events to better raise awareness on the need to cooperate and enable contact among stakeholders.
- Recommendation 1.3.2. Extend invitations above to inter-agency partners (police, coast guard, merchant industry) to broaden the scope of collaboration and to better understand their perspectives and requirements and how they can better contribute to MSA.
- Recommendation 1.3.3. Develop a world-wide common baseline of definitions for identification, classification and tracking of vessels of interests in order to maintain synchronized MSA of potential threats or risks

Finding 1.4. The most concerning areas or maritime security for Norway are Nigeria-Gulf of Guinea (piracy, armed robbery), Libya, Bab-El-Mandeb (Yemen situation) and Somali Basin/Gulf of Aden (piracy, armed robbery), Malacca Strait. This sentiment is echoed completely by the maritime community, since the risks and threats are more visible in those areas than in any other maritime regions.

- Recommendation 1.4.1. Priority should be given to information sharing efforts amongst key players in those specific high-risk areas, thus optimizing synergies and results.
- Recommendation 1.4.2. Gather experts from the mentioned areas to enable them provide their points of view and requirements in maritime security during forthcoming MSR RT events.

Finding 1.5. The shipping industry is part of the security solution in the maritime environment. The MSR RT has requested that it share its interests and requirements. Although they cannot provide intelligence, commercial shipping can deliver real-time information to military counterparts. Other sources for information sharing include people, tech-gadgets and networks.

- Recommendation 1.5.1. Include the shipping industry in any MSR-related meetings since they are an essential part of the security solution. This will improve the exchange of basic maritime data and information at the appropriate level in the maritime domain both at the national (cross sector) and international (cross border) levels.

Finding 1.6. Regional and global maritime security are worldwide requirements and data and information sharing is critical. It is also widely agreed that maritime security flows from MSA. However, very little has actually been done about it at a cross-regional scale, especially in the less well-developed nations of the world, the ones that need it the most. Indeed, in areas such as Africa, the Indian Ocean, South-East Asia and the southwestern Pacific much remains to be done. The oceans are a global commons and improving maritime security anywhere directly improves the maritime security on the entire globe. It is in global maritime community's best interest to build just such a system that should include reporting hierarchy, system and definitions/language. Currently there are a number of systems working in different regions of the globe. If those initiatives were pooled and the efforts became a collaborative whole, they would even be more accurate and useful.

- Recommendation 1.6.1. Foster the implementation of an unclassified mechanism to share data and information on the maritime domain more openly than even before. A panel in forthcoming MSR RT could be a good opportunity to deal with this issue by bringing together some of the actors from the Engagement Matrix concerned, representing the following aspects inherent to those systems: software (tools), hardware, language, reporting hierarchy.

Finding 2.1. Regarding cyber security, human factor is the weakest entity. A huge percentage of all security incidents involve human errors, often costly as they involve insiders who may have access to sensitive information. There are some initiatives underway in form of courses aimed at familiarizing staffs and crews with maritime cyberspace aspects, and exercises, both cyber-oriented like "Cyber Gordian Knot" or more generic but with a strong cyber component, like MARSEC series, which is a must in addressing these issues in the maritime.

- Recommendation 2.1.1. Continue crew and staff training and education regarding cyber by fostering courses and exercises. When, possible these exercises especially the specific cyber-oriented, should be as comprehensive as possible, encompassing the participation of actors other than military, such as industry or academia.

Finding 2.2. NATO policy regarding cyberspace has become obsolete. Currently it is restricted to a CIS Security Policy that needs an update.

- Recommendation 2.2.1. Update the Alliance policy regarding cyber, including new aspects as the delivery of effects and active defense, as well as the involvement of other stakeholders such as industry and academia.

Finding 3.1. Cyber risks and incidents on ships are growing steadily, thus increasing their vulnerability to cyberattacks.

- Recommendation 3.1.1. Increase awareness about the requirement to secure ships and vital harbor systems, as well as personnel awareness against these threats.
- Recommendation 3.1.2. Create CTI mechanisms and implement them at different levels (national, NATO, IMO) to ensure accurate information sharing amongst organizations.
- Recommendation 3.1.3. Enhance Civil-Military Cooperation (CIMIC) in Maritime Security activities.

Finding 3.2. Ships digitalization and automation is in progress. This favors efficiency but also makes them far more vulnerable to cyber threats.

- Recommendation 3.2.1. As per recommendation 3.1.1. Discuss in forthcoming MSR RT the pros and cons of automation vs higher vulnerability to cyberattacks.

Finding 3.3. Despite the importance of information sharing regarding cybersecurity, organizations and companies in the shipping industry are reluctant to share the required information when it comes to security breaches and cyberattacks, allegedly to protect their reputation.

- Recommendation 3.3.1. Educate security branches of organizations on the need to share all cybersecurity issues, as it will facilitate the necessary awareness to make the right decisions to prevent them from happening again.

Finding 4.1. Missions do not always go as planned and issues arise that can lead to legal proceedings. Historically, courts have sided with those enforcing UN resolutions.

- Recommendation 4.1.1. Share UN resolutions and lessons learned from missions that have led to legal proceedings to inform others in order to minimize legal ramifications from enforcing UN resolutions.

Finding 4.2. The role of law is an integral part in all aspects of MSA.

- Recommendation 4.2.1. All authorities, military or civilian, with responsibility in planning operations/activities related to maritime security should make sure to involve lawyers, integrating them in planning groups from the initial stages of the process and avoid concealing any information they should have access to.

Finding 4.3. Technology has led to a better understanding of the maritime environment, but are we may not be using technology appropriately and legally.

- Recommendation 4.3.1. Make it a habit to involve lawyers early and often from strategic policies to tactical employment in order to understand the legalities of new technologies within the maritime domain.

Finding 4.4. Registration and certificates are used to help maintain safety and security throughout the maritime environment; however, more and more certificates are found to be fraudulent.

- Recommendation 4.4.1. Build a database and share the knowledge of known fraudulent users and companies within the maritime environment.

Finding 4.5. Address the issue of suspicious ships flag hopping or states registering ships that was previously fraudulently registered.

- Recommendation 4.5.1. Develop standards to ascertain "ownership" and "control" of ships. Develop and share databases of ships that are known to switch flags from port to port.

Finding 4.6. When is it compulsory to report disruptions, cyber-attacks, ransomware from countries and private companies for the greater good of the maritime environment?

- Recommendation 4.6.1. Encourage countries and private companies to disclose as much as possible to help others prevent similar attacks and possible help gather information to find perpetrators.

4. CONCLUSION.

The MSR RT is CJOS COE's primary tool for discussing maritime security concerns with a focus on identifying gaps in global maritime situational awareness, facilitating better information exchange, increasing overall communication between stakeholders, and providing an interconnected network across all of them. Our process is based on identifying the key players (nations, NATO, IO, NGOs, etc.), developing an engagement matrix, and identifying what information exchange requirements and protocols should be established for the purpose of building MSA.

The following are the conclusions drawn from the discussions and subsequent CJOS COE team analysis, grouped attending to this MSR RT objectives:

Objective 1 – Identify the contemporary challenges with improved information sharing and collaboration among the MSRs from across the global maritime community of interest

- Maritime is too complex an environment due to vastness of sea spaces and the overwhelming amount of activities carried out therein.
- Illegal activities flourish in the maritime domain due to complexity of the maritime domain, thus making Maritime Security a demanding challenge.
- Tackling these threats in such a complex scenario can only be achieved through cooperation.

- Efficiency demands to focus efforts primarily on main sea lines of communications and choke points.
- Investigation and investments are required to achieve data integration systems capable of merging an increasingly huge amount of maritime security data.
- This increase in investments, though a reality, should be driven by an organizational effort to harmonize the multiple different networks and systems existing thus optimizing interoperability among them.

Objective 2 – Identify and share how all stakeholders can contribute to the security of the sea and its lines of communications

- There is a recognized need to enhance education of societies concerning the importance of maritime domain to their own well-being and prosperity.
- The need has been identified to create working groups to allow as many stakeholders as possible to contribute to building MSA on a permanent basis.
- Watchstanders and decision makers from national and NATO Maritime Operation Centers should attend further MSR RT to ensure exchange of views among these important actors in Maritime Security.
- Regional stakeholders should be invited to forthcoming MSR RTs, especially those from high-risk areas when it comes to security: Africa, Indian Ocean, and Southeast Asia.
- Shipping industry is an essential part of the maritime security solution, providing potential worldwide sensors for information sharing.
- The implementation of a unique unclassified system to share information on the maritime domain should be a priority to joint together as many stakeholders as possible is necessary.

Objective 3 – Examine the role of law to improve MSA, information sharing, and the timely response to evolving security threats.

- MSA has played an increasing role as demonstrated by the increasing number of UNSCRs concerning Maritime Security through the last decades.
- Contemporary focus on AIS in UNSCRs is evidence of the increasing importance of this tool.
- Due to complexity of legislation concerning maritime security, it is necessary to include lawyers in planning process of MSO and, in general terms, any other activity related with, and keep them aware of the situation to better advice the commander prior to making the appropriate decisions.
- Australia is an example of country with high implication with its maritime interests, having issued a wide breadth of legal regimes to protect those interests, including the use of force.
- The IMO, as global standard-setting authority for the safety, security and environmental performance of international shipping, can best suit the role of establishing a global structure for management of a common language and definitions for Maritime Security issues, through the IMB.
- A steady increase in fraudulent practices concerning registrations poses a threat as they provide concealment for illicit activities and this affects safety, security and can damage the marine environment.

Objective 4 – Underline the importance of cyber intelligence in maritime security, addressing its scope and challenges, including hybrid threats.

- There is a general shortfall in the education and training of staffs and crews concerning cyber defense, which underscores the need for comprehensive courses and exercises in this realm.
- NATO policy regarding cyber is obsolete and should be updated by including relationships with other sectors like industry and academia.
- Cyber vulnerabilities increase as risks and incidents grow steadily, being necessary to secure infrastructure as well as personnel awareness.
- Ships automation trend benefits efficiency, but makes them more vulnerable to cyberattacks

The Way Forward

There is a widespread reluctance in industry to share information on cyber vulnerabilities for prestige and competition reasons. Most of these conclusions imply actions that can be found amongst the recommendations included in this report. However, experience shows that the annual MSR RT alone does not provide sufficient engagement to keep the necessary momentum toward accomplishment of these goals. To facilitate this objective, we will engage the maritime community in a series of working groups aimed at maintaining the required effort in three areas considered key to maritime security:

- Maritime Situational Awareness.
- Information Sharing, Interoperability and Integration.
- Cyber defense in the Maritime Domain.

A Terms of Reference for such groups, including composition, objectives and battle rhythm is being tailored to better support the fulfillment of activities and will be submitted to maritime community members to encourage them join this initiative, thus seeking to attain the second of the objectives of this MSR RT: ”Identify and share how all stakeholders can contribute to the security of the sea and its lines of communications”.

On behalf of the leadership of CSW COE, NMIOTC and MARSEC COE, CJOS COE would like to thank all participants and contributors who made the MSR RT 19 such as success. We look forward to seeing your participation in the Working Groups and at future Maritime Security Regime Roundtables wherever they are held around the globe!

Norfolk, June 2019