NORTH ATLANTIC TREATY ORGANISATION
NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE
NMIOTC
SOUDA BAY
73200 CHANIA
GREECE

3000 NSC-74/NU: 120
TO: See distribution

SUBJECT:**3rd NMIOTC CYBER SECURITY CONFERENCE – 'Food for Thought'**

DATE: 02 August 2019

REFERENCE: NMIOTC 3000 NSC-71/ser.: NU 01, dated 10 January 2019

1. Having identified the need to enhance maritime security through better awareness of the Cyber Threat, the NATO Maritime Interdiction Operational Training Centre organized its 3rd Conference on Cyber Security ,from 10-11 April 2019 at its premises at Souda Bay, Crete.

2. A total of 32 speakers, both from NATO and non-NATO organizations, presented their ideas regarding Cyber Security issues and the conference was attended by a further 147 participants from a total of 24 Allied and Partner nations. The conference benefitted from representation from governmental and international organizations, agencies, standardization bodies, the military, academia, strategic think tanks and the private sector, including shipping companies. Such diverse attendance encouraged collaboration between different organizations and ensured that cyber defence was discussed in a holistic approach, comprehensively covering the most pressing issues across the whole maritime environment.

3. Discussions covered a wide breadth of Cyber Security challenges, including the following:

- Research Innovative Results in Maritime Cyber Security and Cyber Defence.
- Secure Maritime Logistics and Protection of Maritime Critical Infrastructures.
- NATO-EU Cyber Security Collaboration and Initiatives.
- The role of Cyber Security in maritime power, geopolitics-international cyber security legislation and policies.
- Latest Advanced Technology Solutions and Concepts.
- Cyber Security in Maritime Operations.

4. The above subjects are covered in more depth in the attached 'Food for Thought' (FFT) paper (Enclosure 1), which captures the salient points of the conference sessions. NMIOTC

considers that this document could serve to inform the development of strategic, operational and tactical products in relation to Cyber Security, leading to improved Allied Maritime Strategy to address the Cyber Threat. It also highlights how through enhanced engagement and transformation, the NMIOTC could provide training in support of the Alliance's goals and objectives relating to Cyber Security in the maritime domain.

5. The participation of so many experts and professionals from such varied organizations was certainly beneficial to this year's Cyber Security Conference. NMIOTC is committed to building on this success and is pleased to announce that next year's NMIOTC 2020 Cyber Security Conference will be held 30 September – 1 October 2020.

6. For further information please contact NMIOTC POC:

OPR: Lt Cdr Dimitrios Megas GRC (N)
Staff Officer of Transformation & Experimentation
Tel +30 28210 85716
Email NATO Unclass: megasd@nmiotc.nato.int

Stelios Kostalas
Commodore GRC(N)
Commandant NMIOTC

ENCLOSURES:

1: 3rd NMIOTC Cyber Security Conference - Food for thought Paper.
2. 3rd NMIOTC Cyber Security Conference Agenda

DISTRIBUTION:

External:

Action:

SHAPE REGISTRY	usershaperegistry@shape.nato.int
SHAPE NMR GRC	nmrgrc@shpae.nato.int
HQ SACT REGISTRY	hqsactregistry@ais.nato.int
IMS CENTRAL REGISTRY	imscentralregistry@hq.nato.int
MAIL BOXNSOFFICE	mailboxnsoffice@hq.nato.int
NCIA REGISTRY	nciaregistry@ncia.int
NCIA REGISTRY MONS	nciaregistrymons@ncia.nato.int
JFCBS CG REGISTRY	cgregistry@infcbs.nato.int
JFCNP CG REGISTRY-common mailbox	jfcnpncsregistryco@jfcnp.nato.int
JFC NAPLES NMI HQ MAILBOX	jfcnaplesnmihqmailbox@ais.nato.int
MC RECORDS CENTRE	recordscentere@mc.nato.int
JWC REGISTRY	jwc.jwccgreg@jwc.nato.int
HQ NATO HEL MILREP	(NSWAN: GR.milrep@hq.nato.int)
SHAPE NMR – GRC	(NSWAN: NMRGRC@shape.nato.int)
SHAPE COS	(NSWAN: COM.COS@shape.nato.int)
MARCOM DCOS OPS	(NSWAN: recordscentre@mc.nato.int)
MARCOM - ACOS N6 (CIS) and Cyber Deputy Senior National Representative	(NSWAN: J.DECHANET@mc.nato.int)
CCD COE	(NU: Periklis.Pantoleon@ccdcoe.org)
HNDGS Deputy Chief Defence Policy Branch Head / D´ Branch Strategic Plans and Policy Division Head / D4	

HNGS
Deputy Chief
Head A´ Branch
Head B´ Branch

Internal:

Action:

DIR TS
OPR

Info:
DCOM
COS
QA Manager

ENCLOSURE 1 TO:
NMIOTC NOTE: NU:120
NSC-74/ 02 AUG 2019

3rd NMIOTC Cyber Security Conference
FOOD FOR THOUGHT PAPER

1. BACKGROUND.

Cyber has changed our world. The ongoing digital revolution has fueled unprecedented prosperity and efficiency in our globalized economy and has become inextricably linked with all aspects of our modern life. These innovations will continue to drive global progress for the foreseeable future and are set to continue to evolve at astonishing speeds. In the wake of this progress, lies a growing number of challenges and risks that threaten the very core of the global security and prosperity.

The recognition of cyberspace as an operational domain, analogous to land, air, maritime and space by NATO, marks a new era. Cyberspace has become an operational domain that various sectors (industry, commercial, civilian, military) interact and operate on. Meanwhile Cyber criminals are becoming more and more intelligent with cybercrime similarly evolving at an astonishing pace. Collaborative actions are needed to effectively defend against advanced attacks and avoid catastrophic impacts to our nations and peoples. NATO assists its individual member states to become more cyber resilient and some members have offered NATO access to their cyber capabilities so that they can train and participate in exercises relating to this threat.

Cyber information sharing, collaborative incident handling and cyber situational awareness are the most essential areas that NATO collaboration will lead to successful civilian, industrial, commercial and military cyber defense strategies and operations. The impact of cyber security incidents on the conduct of future maritime operations may be catastrophic given that maritime operations are conducted by technology-intensive platforms, which rely heavily on information systems. The question was thus posed, ‘How will this dependence on information technologies affect the ability to maintain security at sea?’.

To operate effectively within the cyber domain, we must develop and leverage a diverse set of cyber capabilities and authorities. Cyberspace operations, information and communications networks and systems, can help detect, deter, disable, and defeat adversaries. Robust intelligence, law enforcement, and maritime and military cyber programmes are essential to enhancing the effectiveness of Maritime Operations, in deterring, preventing, and responding to malicious activity targeting critical maritime infrastructure. We should recognize that cyber capabilities are a critical enabler of success across all missions and ensure that these capabilities are leveraged by commanders and decision-makers at all levels.

Besides the challenges, there are opportunities for collaboration especially in the

maritime domain. NATO relies on strong and resilient cyber defence to fulfill the core tasks of collective defence, crisis management and cooperative security. Our Partners could be engaged as well. Building a secure, trusted and humane cyberspace that empowers individuals rather than enslaves them is needed. An eco-system driven by data and complexes must be governed by norms and codes of conduct. Cyber is the ultimate team sport where the larger the network and the more diverse the set of partnerships, the more successful you are likely to be. Therefore, it is key that international actors, governments, private sector and civil society cooperate effectively to deal with the emerging threats.

A focus should be followed to ensure a safe, secure and resilient cyber operating environment that allows for the execution of Maritime Security Operation including Maritime Interdiction Operations (MIO) and maritime safe transportation. The purpose of the mission regarding cyber security in the maritime domain is to enhance the cyber awareness of all the participating naval units and boarding teams conducting relevant operations.

2. PANEL SESSIONS AND KEYNOTE SPEAKERS.

Prior to the commencement of the panel presentations, NMIOTC Commandant Commodore Stelios Kostalas GRC(N), addressed and thanked all attendees for their presence and support of the event. He highlighted that to operate effectively within the cyber domain, we must develop and leverage a diverse set of cyber capabilities and authorities. Cyberspace operations, information and communications networks and systems, can help detect, deter, disable, and defeat adversaries. Robust intelligence, law enforcement, and maritime and military cyber programmes are essential to enhancing the effectiveness of Maritime Operations, and deterring, preventing, and responding to malicious activity targeting critical maritime infrastructure. Finally, he concluded by highlighting the fact that it should be recognized that cyber capabilities are a critical enabler of success across all missions and ensure that these capabilities are leveraged by commanders and decision-makers at all levels. Cyber is the ultimate team sport where the larger the network and the more diverse the set of partnerships, the more successful you are likely to be. International actors, governments, private sector and civil society need to effectively cooperate to deal with the emerging threats.

2.1 Session 1: “Cyber Security in Maritime Operations”.

Panel 1 aimed to promote discussions over how to improve awareness and address challenges of cyber threats with respect to Maritime Operations.

Panel Members

- **Key Note Speech Opening:** Fred S. Roberts, PhD Distinguished Professor of Mathematics, Rutgers University, Director of Department of Homeland Security University Center of Excellence CCICADA: Command, Control and Interoperability Center for Advanced Data Analysis - **“Combined Cyber and Physical Attacks on the Maritime Transportation System”**.

- **Moderator:** Capt (N) Phd Student eng. Sebastian Popescu, Head of Communication IT&AC Office of Romania Navy HQ.
- **Speaker:** Mr Emmanouil Christofis, SHAPE J6 Cyberspace, Strategic Plans and Policy - **"Chronicle of Maritime Cyber Attack"**.
- **Speaker:** MARCOM Captain Christophe Eugene - FRA N MARCOM - ACOS N6 Cyberspace - **"Operationalisation of the maritime cyberspace: MARCOM's vision"**.
- **Speaker:** CAPT Amy B. Grable, USCG, Deputy, Coast Guard Cyber Command (CGCYBER), - **"Building cyber resilient ports through partnerships".**
- **Speaker:** CJOS COE,Cdr. Neculai GRIGORE,- **"Maritime Cybersecurity Afloat"**.

Professor Roberts provided an initial setting for discussions about physical security in the Maritime Transportation System (MTS). He stated that in recent years, there has been an increasing interest in cyber security in the MTS that has led to discussions about best practices for cyber security. It is likely that many future attacks on the MTS (and other systems) will be multi-modal, including both a cyber and a physical component. As a simple example, hacking into security cameras at a port increases vulnerability to a physical intrusion. Thus, a cyber attack could be a precursor to a physical attack, and in fact the opposite could also be the case.

He demonstrated how maritime cyber threat is included among several threats in maritime security, by presenting scenarios of combined cyber and physical attacks, and discussing ways to understand their likelihood based on ease of attack and seriousness of potential consequences. For instance, computerized maritime systems are highly vulnerable to cyber threats. These systems are widely located: harbours and ports, navigation systems, rigs, offices, headquarters, maritime vessels.

He concluded that ultimately, the weak link in defense against combined cyber-physical attacks remains the human being. A successful attacker tries to influence behaviour, leading to bad decisions. He or she would aim to introduce doubt, for example through false aids to navigation showing up on an electronic chart, spoofing a vessel track that may not correlate with radar, and creating a chain of things initiated by influencing the thinking of the bridge operator. Fundamentally, there does not seem to be anything special one would do to prevent a cyber attack intended as a precursor to a physical attack that one wouldn't do to prevent any cyber attack.

Mr Emmanouil Christofis presented an emulation of a cyber-attack which provides a realistic assessment of actual threats against company's environment based on the latest Tactics, Techniques and Procedures (TTPs) noticed in recent attacks.

He highlighted that by emulating the attackers, experts tested multiple aspects of organizations' security controls, such as external and internal network security, web application security and employee security awareness providing absolutely the real situation of the organization's cyber security posture.

As an expert in Cyber Strategic Plans and Policy, he demonstrated a real case scenario of compromising two of the most common applications used in Shipping. As a result,

the Red Team of Ethical Hackers managed to gain access to the entire corporate IT environment and demonstrated that could successfully gain control of the corporate's Information Technology (IT) infrastructure, including Active Directory (AD), email servers, database servers, file servers, network devices, impersonating senior management that could potentially lead to gain access to Ship's IT environment.

Captain Eugene highlighted that the main MARCOM's role and responsibility regarding cyber threats is strengthening cyber defences and integrating cyber capabilities into NATO planning and operations.

He provided the framework of Maritime Cyber Situation Awareness (MCSA) and introduced the main pillars of it, namely the permanent cyber readiness**,** the cyberspace awareness and the cyber reaction. The permanent cyber readiness consists of cyber hygiene, training, certification, rapid response team and catalogue of cyber measures (cyber posture). He highlighted that the main cores of cyberspace awareness are threat intelligence, threat evaluation, advice / guidance and he stated that in terms of cyber reaction, active response should be adopted in case of aggression.

Captain Grable, introduced the US Coast Guard Cyber Strategy strategic priorities for the next ten years namely: Defending Cyberspace, Enabling Operations, Protecting Infrastructure. She presented the main goals for each strategic priority. Regarding Defending Cyberspace, the main goals are identification and hardening of systems and networks, understanding and countering cyber threats and increasing of operational resilience. As far as Enabling Operations the main goals are to incorporate cyberspace operations into mission planning / execution and to deliver cyber capabilities to enhance all missions.

Finally, she concluded that regarding the protection of infrastructure the main goals are the adoption of risk assessment through promotion of cyber risk awareness and management in conjunction with the prevention through the reduction of cyber security vulnerabilities in the MTS.

Cdr Necolai provided a presentation regarding maritime cyber threats and the recognized maritime picture. He mentioned that adopting increased degrees of automation, modern systems and technologies increases the pace of decision-making processes and the quality of support for MSA but, in the same time, the systems become more vulnerable to cyber-attacks and the crews are less equipped to deal with the after effects. These vulnerabilities come from the dependency on other systems that are rather vulnerable to cyber warfare such as GPS, AIS, land and space-based sensors and satellite. The result of these actions is an altered recognized maritime picture, one of the main tasks of MSA, which represents an essential contribution to effective naval warfare operations. Currently, the activities to address cyber vulnerabilities are largely focused on the resilience of information technology systems. Mitigation actions aiming to decrease the hostile effects over military systems afloat could be a challenge.

He demonstrated the way four systems that are intended for feeding and exchanging of RMP information are vulnerable to cyber attacks. More specifically these systems are GPS (as part of GNSS), AIS, SATCOM and Tactical Data Link (TDL).

He drew the conclusion that not all threats presented are specific to military equipment. A wide range of functions already implemented in military equipment and systems provide satisfactory protection now. Meanwhile, we must consider that not all military ships and nations have the latest technology. These limitations are not necessarily determined by the refusal to comply with interoperability requirements but because of limited resources availability. At first glance, one can draw the wrong conclusion that only these will be affected. The need for information, for making the best decisions, the execution of actions in an allied, combined, joint and integrated environment force the interconnection of systems, ships, forces and command structures. Thus, a threat to the least protected “entity” will "facilitate" its extension and implicitly affect all infrastructures and decision levels. Lastly, the training of personnel who exploit systems and use information must be a priority. Many of the effects of these threats can be eliminated if staff apply the available procedures and recognize, as from the first signs of manifestation, each type of threat. This allows time to be gained, distortion of information to support the command and control process can be avoided and erroneous decisions and disasters generated by a blurred Recognized Maritime Picture (RMP) can be avoided.

2.2 Session 2: “NATO-EU Cyber Security Collaboration and Initiatives”.

Panel 2 addressed issues regarding NATO-EU cyber security collaboration and initiatives.

Panel Members

- **Key Note Speech Opening:** Mr Michael Tsamaz, CEO OTE Group.
- **Moderator:** Dinos Kerigan-Kyrou PhD CMILT, Emerging Security Challenges Working Group.
- **Speaker:** Dr. Nineta Polemi, European Commission, DG CONNECT, H1, Programme Manager- E.U. Policies – **“Cybersecurity Challenges and EC initiatives”**.
- **Speaker:** Dr Gregor Schaffrath, EEAS/ESDC – **“ESDC Cyber ETEE Platform”**.
- **Speaker:** Mr Mario Beccia, PO Capability, Armament & Technology Cyber Defence, EDA – **“Cyber Defence Systems Engineering: A framework to identify requirements described into a dedicated Cyber Defence Architecture to inform Capability Development”**.
- **Speakers:** CDR Sérgio Rodrigues, Lt COL Diego Sirvent, SHAPE J6 Cyberspace **– “Framework development, Maritime implementation and Cyber Security Challenges’’**.

Mr Tsamaz initially stated that cyber security is not just a matter of the institutions. It requires preparation and wide collaboration between all stakeholders of the digital future. It is a shared responsibility amongst all actors throughout the entire value chain: NATO and the EU, the states, the public administration, the academia and the industry. As the Head of the OTE Group he provided the main two areas that they focus on: Creating state of the art telecommunications infrastructure and services and securing them and sharing their cyber security expertise by providing Managed Security Services to third parties.

He carried on explaining that telecommunications are not just a commodity. It is the “X” factor, in times of war and in times of peace. Therefore, they make sure that they design and implement resilient networks and that they have in place the right back up plans to ensure network availability under all circumstances. He highlighted that is more complex than someone can imagine, given the different network architectures.

Mr Tsamaz informed the audience for the lately projects that the OTE Group runs, namely:

- The biggest landline optical fiber network in the country – core and commercial.
- The best mobile network with the widest 4G coverage in Greece.
- Satellite communications – widely offered to the shipping industry. OTE Group also supplies all the frigates of the Hellenic Navy with satellite dishes for their communication around the globe.
- International interconnection - in fact, 99% of all international traffic, travels through optical cables inside seas and oceans. OTE Group subsidiary, OTE Globe owns such cables – 16,000 km of optical fiber passing through 15 countries. Therefore, we also depend on the safety of the maritime world. If someone was able to interfere with these cables, there would be no telecommunications.
- And finally, tailor made networks. OTE Group is responsible for the development, maintenance and management of the Unified National Defense Communications System, which consists of a private fiber optic network which unites all the critical military bases throughout Greece. This network is the backbone of our military’s communications.

He made clear, it is a number one priority to ensure the integrity and security of the networks. He mentioned *“We have prepared ourselves, having in mind that any investment in cyber security, is money well spent.”* To this end:

- OTE Group has set up a separate organizational unit, reporting directly to OTE CEO, to manage the cyber-security risk.
- A highly skilled team of cyber-security experts is working together with systems’ engineers to have security built into their systems and services from the design phase.
- They constantly review and strengthen their security rules and systems to ensure that they reflect the strategic importance of infrastructure, as well as the evolution of cyber-threats.
- And they operate a state-of-the-art Cyber Defense Center, analyzing in real-time, billions of events, trying to quickly spot cyber-attacks, so that they can respond as fast as possible and secure our networks and services.

Finally, he stated that as part of OTE Group Managed Security Services portfolio, together with Otesat-Maritel, their subsidiary for maritime communications systems, they have built a niche security solution, specially designed for the challenges and requirements of ship owners. Their IRIS platform allows their OTE Security Operations Center to monitor 24/7 the on-board communications for signs of abnormal activities, taking advantage of various data analytics software tools for cyber security, as well as real time threat intelligence collected from all Deutsche Telekom Group footprint.

Dr Polemi stated that cyber security is strategic priority for EU. Building EU resilience to cyber attacks can be achieved through capacity building in addition with prevention and response coordination. She mentioned that currently EU faces three challenges regarding cyber security. The first challenge is better and more EU Cyber security technologies, the second is the digital sovereignty with respect to privacy, accountability, duty of care and trustworthy and the last one is cyber security knowledge, skills and values.

She referred to the main actions should be followed to cope with these challenges, namely:

- Close the gap between cyber security education and EU industrial, business, operational, legislative and ethical requirements.
- Upgrade cyber security training by easily accessing and using new technologies (e.g. AI simulation platforms, HPCs, Cloud resources, Big Data).
- Align academic & certification programmes.
- Adopt a multidisciplinary approach to cyber security training.
- Utilise all expertise (military, industrial, law enforcement, financial, governmental).
- Match cyber security skills and workforce-Prepare people.

Finally, she introduced the cyber security Competence Centre and Network (CCCN). The Comptence Centre will contribute to the following functions:

- Facilitate and help coordinate the work of the Network.
- Implement cyber security parts of Digital Europe and Horizon Europe Programmes.
- Enhance cyber security capabilities, knowledge and infrastructures.
- Contribute to the wide deployment of state-of-the-art products and solutions.
- Contribute to reducing cyber security skills gaps.
- Support cyber security research and development.
- Enhance cooperation between the civilian and defence spheres regarding dual use technologies.
- Enhance synergies in relation to the European Defence Fund.

Dr Schaffrath presented the concept of the European Security Defence College (ESDC) Cyber Education, Training Exercise and Evaluation) ETEE Platform. The main task of the ETEE platform within the ESDC is the coordination of cyber training and education for EU Member States. The existing training will be standardized and new courses will close the gaps between training needs and training activities. These efforts will be jointly undertaken by various stakeholders, including several centres of excellence and partner organizations.

He mentioned that the Cyber ETEE Platform has two main aims. Firstly, to address cyber security and defence training among the civilian and military personnel, including for the Common Security Defence Planning (CSDP) requirements for all training levels as identified by the EU Military and Civilian Training Groups. Secondly at a later stage, and depending on the further development of the concept, the Cyber ETEE platform could advance ETEE opportunities for a wider cyber defence workforce.

In conclusion he stated that interoperability is paramount, interoperability requires collaboration, ESDC is open to collaboration and the Cyber ETEE Platform could potentially act as training related facilitator between NATO and domains beyond defence on the EU side.

Mr Beccia stated that EDA's mission regarding cyberspace is to achieve better cybersecurity resilience. Better cyber security resilience implies: Better preparedness (people), better organization of assets (process), better assets (technology). He depicted the cyber resilience goals, namely:

- Anticipate: Maintain a state of informed preparedness to forestall compromises of mission/business functions from adversary attacks.
- Withstand: Continue essential mission/business functions despite successful execution of an attack by an adversary.
- Recover: Restore mission/business functions to the maximum extent possible subsequent to successful execution of an attack by an adversary.
- Evolve: To change missions/business functions, to minimize adverse impacts from actual or predicted adversary attacks.

He summarized that despite the good progress in the last 10 years, Cyber security is a young domain, still in an embryonic phase of development. Cyber Defence is an essential element of any EU MS military strategy. Despite the efforts, further research and innovation must be brought in the field. The Permanent Structure Cooperation (PESCO) framework offers an excellent vehicle to speed up creation of multilateral initiatives, and to support projects and initiatives based on the "coalition of the willing" approach. Finally, he mentioned that the European Defence Fund will contribute greatly to multilateral initiatives and offers a powerful tool to bring together Member States (MSs) and industry partners and EDA will continue to serve MSs in their endeavor to develop capabilities and shape a more coherent Cyber Defence capability landscape in Europe.

CDR Rodrigues and Lt COL Sirvent presented the context of Federated Mission Networking (FMN). They defined that FMN is the interaction of people, processes and technology to exchange information and/or services among federated mission participants including but not limited to the use of a set of interconnected autonomous computer networks for the conduct of coalition operations and exercises. The primary goal of the FMN capability (mission networking in a federated environment) is to support Command and Control and decision-making in future operations through improved information-sharing. The implementation of this capability delivers a *toolset* of processes, organizations, training, technology, and standards provided, in a coordinated approach, by NATO, NATO Nations and non-NATO nations cooperating.

In conclusion they demonstrated the FMN Cyber Defence concept with respect to SACEUR's Direction & Guidance on Cyber Defence, namely:

- Maintain Situational Awareness (SA) of NATO Cyberspace and how it affects Alliance Operations and Missions.
- Conduct Alliance Operations and Mission in Cyber contested environments.
- Provide Consequence Management (CM) to issues affecting cyberspace.

2.3 Session 3: “Latest Advanced Technology Solutions and Concepts”.

Panel 3 addressed issues and concepts with regards to latest advanced technology in maritime domain.

Panel Members

- **Key Note Speech Opening:** Mr Dimitrios Koutsopoulos, CEO at Delloite Greece.
- **Moderator:** Prof Gritzalis Dimitrios, Professor & Associate Rector Athens University of Economics & Business.
- **Speakers:** Prof Barton P. Miller, Prof Elisa Heymann University of Wisconsin-Madison, - **“Maritime Software Security through In-Depth Assessment, Education and Recovery”**.
- **Speakers:** Dr. Stefan Schauer (AIT) and Mrs Eleni-Maria Kalogeraki (Dept. of Informatics, University of Pireaus) – **“SAURON: Physical and Cyber Situation Awareness Fusion Models”**.
- **Speaker:** Dr George Stergiopoulos, Athens University of Economics & Business, **– “Results on container ship route risk-based interdependency modeling”**.
- **Speaker:** Mr Ilias Chantzos, LLM, MBA, Senior Director EMEA & APJGlobal CIP and Privacy Advisor Government Affairs, Symantec Corporation, - “**Cyberattacks on critical infrastructure** – **“Modus operandi, examples and considerations”**.

Mr Koutsopoulos - CEO of Deloitte Greece, presented the latest advanced technology solutions and concepts in relation to the cyber domain. He outlined that over the past ten years, cyber has progressed from:

- focus on compliance and security to known threats,
- to risk compliance and resilience to address published threats,
- to what we see today being the next area of cyber everywhere where focus is on managing risks outside the organization’s control.

Mr. Koutsopoulos noted that cyber threats are an emerging risk that will affect the strategy of the maritime industry. The maritime industry is being driven by a need to become more cost effective, more efficient, more reliable and safer. To achieve that, the introduction of digital technologies in OT (operational technology) environments moving forward to the autonomous ship vision is required.

He concluded by highlighting the following outcomes:

- the industry’s limited view/control of OT environment,
- the lack of standard security measures on OT systems across the fleet,
- the challenges to maintain these measures appropriately and the need to increase education on cyber risks and procedures among vessel crew.

Professors Miller and Heymann presented their research with respect to the maritime software security through in-depth assessment. The maritime sector develops and deploys a large quantity of specific to their needs. They mentioned that software includes ship control systems, port community systems, terminal operating systems, navigation systems, and even the business websites that support maritime commerce. The security of this software is vital to the safe and effective maritime operations. Violations of this security can potentially disrupt operations, damage equipment, harm people, damage reputations, and even sink ships.

They highlighted that maritime industry must address the security of this software throughout its lifecycle. From first design, through coding, testing, and deployment, security must be a consideration. They noted note that investment in security early in a project can have significant payoffs in the later stages. Additionally, they described our experiences in the areas of education and training, and in performing in depth software vulnerability assessments. They shared their experiences included delivering professional training, developing an undergraduate software security course, and engaging with a top industrial team on an in-depth software assessment resulting in improvements in the security of software that controls major container shipping ports.

In conclusion they emphasized to the concept of a strategy for recovery. Attacks are a reality and our response to such attacks must be based on limiting the scope of such attacks and recovery those part of our systems that have successfully been exploited.

Dr Schauer and Dr Kalogeraki initially they stated that over the last years, the maritime sector has become an attractive target for cyber criminals. Port infrastructures as well as vessels have been at the centre of numerous highly sophisticated attacks causing severe damage to economic and social life. In most cases, such attacks are utilizing combined attack vectors from both the cyber and the physical domain to exploit existing vulnerabilities in one of those domains. The magnitude of the consequences is often increased by cascading effects in both domains, even further amplifying each other.

They provided an overview on a novel approach implementing a holistic framework for situational awareness in the maritime domain. This Hybrid Situational Awareness (HSA) combines information coming from the cyber as well as from the physical domain and can identify potential cascading effects of an incident. Therefore, data from classical Cyber Situational Awareness (CSA) and Physical Situational Awareness (PSA) are integrated to generate a holistic picture of the current condition of all relevant assets within a maritime port. Furthermore, by applying intelligent reasoning algorithms, potential future attack scenarios can also be identified.

Finally, they demonstrated how this HSA framework can be integrated into port infrastructures, either from scratch or by using existing situational awareness systems, and how it can also communicate with emergency organizations of a city in case of a crisis.

Dr Stergiopoulos discussed the issue that container ships are prone to delays and congestion, both due to route delays (e.g. bad weather) and port unavailability (e.g. delays, congestions) along the way. He mentioned that with the specific research paper they have proposed a risk-based interdependency analysis methodology capable to detect large-scale

route congestion and ship delays between interconnected ports of the maritime network using dependency risk chains.

In his presentation, he demonstrated the results from implementing this methodology on a constructed model of the entire maritime network. The model was constructed using container ship AIS route data to calculate the dependency risk of ship routes between interconnected ports using assessment of container ship route flow. The dataset was provided by the Marine Traffic company that maintains a comprehensive maritime database worldwide for more than 6M users monthly. It contained all historical entry and exit calls of container ships in ports of the maritime network recorded from 2015 until 2017 (Q2). Data used to create a global maritime model graph, where ports are nodes and ship routes are edges. They used the methodology to detect all n-order route-port dependencies and automatically flag ship routes and relevant ports for increased risk of cascading congestion.

He finished by stating that the output framework can calculate: the risk of congestion transmission in any ship route or for any container ship, and can pinpoint specific ports that are prone to initiate cascading traffic congestions.

Mr Chantzos presented the Symantec's concept regarding cyberattacks on critical infrastructure. Initially he provided a taxonomy of the potential actors and motivations and he provide examples of the value of information sold on Dark Web.

As far as for the targeted attacks he highlighted that for 2018 attack groups target an average of 55 organizations each. The number of attack groups using destructive malware which grew by 25% in 2018. Additionally, he demonstrated a targeted attack modus operandi with respect to all phases of the attack namely: Infiltration, Foothold, Exploit, Data Discovery and Exfiltration.

He closed his presentation by demonstrating an attack to critical infrastructure by implanting a piece of malware into an otherwise legitimate software package at its usual distribution location. This can occur during production at the software vendor, at a third-party storage location, or through redirection.

2.4 Session 4: "Research Innovative Results in Maritime Cyber Security and Cyber Defence".

Panel 4 discussed issues and concepts regarding research innovative results in maritime cyber security.

Panel Members

- **Key Note Speech Opening: Dr George Troulinos, CEO Intracom Defense Electronics**.
- **Moderator:** Prof Evangelos Markatos, Ph.D, Head Professor Computer Science Department, University of Crete, Head Distributed Computing Systems Lab FORTHS-ICS.

- **Speaker:** Dr Alessandro Garibbo Strategic Marketing, Security & Information Systems Division Leonardo Industry - **"Improving maritime security through an integrated approach"**.
- **Speaker:** Mr Kah Kin Ho, Senior Director Fireeye EMEA Public Sector – **"Applying lessons from maritime dispute to cyber deterrence"**.
- **Speaker:** Mr Christos Vidakis, Principal Risk Advisory, Cyber Risk Services,Deloitte – **"Maritime Cyber Threat Landscape and lessons learnt from the front line. Cyber Everywhere: The Bow-Tie and the real-life approaches"**.
- **Speaker:** Mr Isidoros Monogioudis, Principal Cyber Security Advisor to JV DIAPLOUS Maritime Services / FOCAL POINT Cyber Security, - **"How to Achieve Business Continuity through Effective Cyber Risk Mitigation and advance Crisis Response"**.
- **Speaker:** Mr Chris Pike, Cyber Threat Intelligence Advisor, CrowdStrike Inc, - **"How to Operationalize Cyber Threat Intelligence for Maritime Organizations"**.

Mr Troulinos as the CEO of Intracom Defence Electronics provided the maritime industry perspective regarding cyber security. He underlined that the maritime industry is moving fast towards full digitization and that modern vessels are now high-value complex ICT systems. Moreover, he highlighted that cyber security risks should be addressed in the same way as any other top risks that may affect the safe operation of a ship and the protection of the environment and that cyber attack consequences involve financial loss, physical loss/damage to ships, physical injury to crew, cargo loss, pollution, reputational damage and business interruption. In addition, he stated that regarding cyber attacks in the Maritime Industry: there is high impact and likelihood in conjunction with low preparation to address them.

After reviewing some noteworthy cyber attack incidents in maritime industry, he provided a proposed cyber security approach. More specifically he suggested the following:

- To establish organizational cyber security policies and practices and ensure the full compliance with them via regular and extensive audits.
- To secure the communications and IT infrastructure - located everywhere.
- Review and/or audit third-party cyber security status to reduce the risk of supply chain attacks.
- Standardize Maritime Industry specific cyber security procedures & mechanisms.
- Continuously training of the personnel.

Mr Garribo with his presentation provided Leonardo's perspective regarding improvement of maritime security through an integrated approach. He provided a taxonomy of emerging threats in maritime domain such as:

- EMP and Directed Energy Weapons.
- Electromagnetic spectrum as a warfighting domain and its convergence with cyber and Electronic Warfare (EW).
- Drone attacks.

- Hybrid threats, including cyber attacks, from hostile governments and non-state actors causing instability in Eastern Europe, the Middle East, and Africa.
- Surge of piracy affecting international shipping.
- Attacks from criminals and terrorists on ports, offshore installations and ships.
- Emerging threats to maritime energy infrastructure, including cyber attacks.

Then he referred to the issue of the technology convergence. He mentioned several aspects of technology conversion such as Information Technology (IT) and Operation Technology (OT) Convergence (Internet of Things and Industry 4.0), Radar-Communications Convergence: Coexistence, Cooperation, and Co-Design (Joint Radar and Communications Nodes, Phased-Array Antennas), Satellite Services Convergence (Satellites running multiple services for multiple customers at the same time, e.g. sensing, observation and communication for both the civil and the military), Artificial Intelligence (AI) and System Engineering Convergence (Cognitive Systems, Machine Learning).

Finally, he concluded by stating that towards an integrated approach for maritime security it is necessity to adopt cyber situational awareness and must be included in military doctrine.

Mr Kah Kin focused on the deterrence. He stated that deterrence is the primary strategy used by US, and by extension, NATO allies. Deterrence, by layman's definition, is really about drawing a line and communicating to our adversaries that they'd better not cross the line lest they suffer serious consequences. It is entirely reasonable for us to question the value of a deterrence strategy in the cyber domain, because, a successful deterrence would mean that our adversaries don't conduct cyber-attacks against us but yet the sheer amount of cyber breaches seem to suggest that deterrence has failed.

He also mentioned that we tend to gravitate toward a deterrence mindset in part because of the evolution of international law over time which gives rise to a security architecture which has "lines" drawn e.g. use of force, armed attack, etc. In other words the deterrence framework is being built into the security architecture. This security architecture with a built in deterrence framework has served us well since the end of world war two with some exceptions. It is important to recognize that this security architecture (with deterrence framework) only works well if two preconditions are in place: 1) attribution – knowing who did what to us and why, and 2) sovereignty recognition. On sovereignty recognition, if nobody recognizes that a territory belongs to a particular state, it is not hard to see why this will be contentious. The South China sea is a prime example of this. Sovereignty claims are made by coastal states now but in the past nobody bothered to make sovereignty claims as these islands were perceived as worthless. With the discovery of oil reserves, lucrative fisheries, and over time becoming an important shipping lane ($3 trillion of trade passes through every year), states have made attempts to claim what they believe is their sovereign territory on South China sea. Hence why this region has become one of most highly contested regions in the world.

In his words he explained that the cyber domain is no different: high value (we put everything in cyber) and the lack of sovereignty recognition again make this yet another highly contested domain. The cyber sovereignty issue is far from settled. One important reason for this has to do with states' freedom of action. The UK, for example, took the position in May

2018 that sovereignty as a rule does not exist. A rule that doesn't exist means there is no such thing as UK violating the sovereignty of other countries with their cyber operation that doesn't cross the use of force threshold. However because of sovereign equality, the UK can also be target of such cyber operations by other states. Another reason why sovereignty is not settled is when western liberal democracy deals with Russia and China, they are concerned that sovereignty is used as a cover to suppress their citizens' human rights. To achieve stability in the cyber domain it is imperative that states with differing positions on the issue of sovereignty find common ground to foster much needed consensus in shaping future norms of behavior.

Mr Vidakis initially discussed the business perspective of the maritime cyber threat landscape, digital and regulation challenges and Deloitte's value proposition to industry's cyber focus areas such as threat intelligence, situational awareness, and enforcement of risk-based approaches and implementation of agile and adaptive security controls. He addressed the importance of maritime organizations to understand the level of risk associated with the current cyber exposure and to enforce a cyber governance model to mitigate cyber risks and obtain benefits from cyber.

In addition, he 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 summed up by stating that 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) environments moving forward to the digital ship version.

Mr Monogioudis presentation provided guidelines how to achieve Business Continuity through effective Cyber Risk Mitigation and advanced Crisis Response. Initially he highlighted the added value of Cyber Risk Management. More specifically he mentioned that a proper adoption of Cyber Risk Management assists organizations in identifying risks both in systems (cyber) and processes and analyzes the attack surface and pinpoints the most critical threats. It explores the different mitigation strategies and highlights the next steps to be taken thus minimizing unnecessary expenses and promotes budget smart allocation whilst promoting the adaptation of a security-by-design framework in all aspects within an organization.

He numbered the common vulnerabilities to the maritime industry, namely:

- Obsolete and unsupported operating systems.
- Outdated or missing antivirus software and protection from malware.
- Inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords.
- Shipboard computer networks, which lack boundary protection measures and segmentation of networks.
- Safety critical equipment or systems always connected with the shore side.

- Inadequate access controls for third parties including contractors and service providers.

Additionally, he also referred to the threat impact. He stated that the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

In his words, Cyber Risk Management System can be enhanced through asset management, Cyber Risk Visualization, mapping vulnerabilities with critical business functions and by adopting continuous Cyber Risk Assessment.

Mr Pike with his presentation provided a concept of how to operationalize cyber threat intelligence for cyber stakeholders operating within the maritime industry vertical. Initially he stated that the purpose of threat intelligence is to achieve an understanding of our adversaries' intent, behaviors, capabilities, and infrastructure relative to our own business mission, our critical assets, and our own attack surface and then communicate that understanding to security-focused stakeholders.

He reviewed the most current cyber threats to the maritime industry, and he highlighted that the malware free attacks are capable to avoid detection by antivirus, IDS, next generation firewalls, to avoid exploiting vulnerabilities, can look like a typical IT admin, can leverage legitimate processes and to be stealthier and more effective.

Finally, he stated that ransomware has become a prevalent payload delivered by malicious actors globally. Sophisticated ransomware operators will make campaigns more targeted with larger ransom demands. In his words he highlighted that the understanding of cyber threats to the maritime industry is important and can leverage threat intelligence in order to mitigate cyber threats.

2.5 Session 5: "Secure maritime logistics and Protection of Maritime Critical Infrastructures".

Panel 5 addressed issues regarding secure maritime logistics and maritime critical infrastructure protection.

Panel Members

- **Moderator:** Mr Emmanouil Christofis, SHAPE J6 Cyberspace, Strategic Plans and Policy.
- **Speaker:** Dr Stavros Karamperidis, Lecturer in Maritime Economics, Plymouth Business School, - **"Cyber-security in the Maritime Sector: Previous cases and lessons learned from other sectors for commercial shipping"**.
- **Speaker:** Mr Quentin Drion IT Director of Infrastructure and Operations MSC Mediterranean Shipping Company SA, - **"Overview of The Cyber Security Threat Environment from The Perspective Of a Large Commercial**

Operator".

- **Speaker:** Dr Cerruti Franco, IT Security and Operation Director, Carnival Maritime - Costa Group, - **"Maritime Cybersecurity status of Carnival Corporation & PLC - March 2019"**.
- **Speaker:** Chronis Kapalidis, Hudson Analytix, PHDc, WMG, University of Warwick, Academy Fellow, Chatham House,- **"Cyber Risk Quantification: A Case-study from the Commercial Maritime Sector"**
- LTC Ret. Freddy Furulund Director of Security & Contingency Intelligence & Operations Centre (IOC) Den Norske Krigsforsikring for Skib Norwegian Shipowners' Mutual War Risks Insurance Association, - A Comprehensive Cyber Security Risk Management Strategy – **"A Norwegian shift from a defensive to a proactive and Intelligence driven approach of thinking about maritime OT and IT risks"**.

Dr Karamperidis with his presentation investigated who are the cyber threat actors, why they are targeting the shipping sector and how the sector could better defend against cyber-attacks. Initially he stated that there are four types of cyber-attacks, those are: activists, competitors, criminals, and terrorists. The motivations of those attacks range from economic to personal glory to political. The economic motivation for a cyber-attack is constantly increasing in terms of frequency. However, as cyber-attacks do not have any borders, the distinction between the specific cultural values and specific motives it is difficult to be observed. It is even harder to identify how cyber.

Dr Karamperidis also focused on the characteristics of shipping and the importance of human element for the sector. As the shipping sector is a late adopter of technology (specifically in terms of cybersecurity shipping is roughly 20 years behind equivalent sectors training in cyber-security has lagged behind other industries.

Finally, he stated that solid cyber-defences cannot be implemented in shipping due to a range of characteristics. Some of them include:

- Global presence so they could capture cargo movements (offices all over the world).
- Some of the offices are occupied by agents as cargo volume is not enough to justify the presence of a dedicated office. Agents have their own IT infrastructure.
- Most of the vessels are chartered, through that way shipping companies reduce the investment risk, but they increase the cyber risk as they cannot "fully" control the vessel and its IT which is integrated with the shipping company systems.
- Cyber defence of the shipping company is inland based while the on board systems marine operated by the on-board technical department which often has limited cyber defence background knowledge.
- Due to chartering of the vessel crew may not be directly trained by the company, thus human risk is increasing.
- Various visitors require access to IT systems on board the vessel (e.g. inspection), they could potentially affect the vessel.

- Various organizations (e.g. port) interact with the vessel and the vessel exchange information in various forms/environments. That increase the vulnerability of the vessel.

Mr Drion provided an overview of the cyber security threat environment from the perspective of a large commercial operator, namely the MSC Mediterranean Shipping Company SA. At the beginning he presented what MSC considers as a cyber security. In his words he stated that the cyber security comprises from OT security, IT security and physical security. OT security covers the protection of the hardware and software that manage physical devices such as valves, pumps, engines, balance systems, etc. It security has to do with the protection of computer systems, company and customer data from disruption while the physical security ensures protection from physical actions and events that could cause loss or damage to people and company assets.

He named some common risks for a cyber attack from a maritime industry perspective, namely:

- Manipulation of GPS system on board.
- Manipulation of data to get early notice on ETA of delivery.
- Gain physical access to terminals.
- Targeted attacks on automated terminal infrastructure.
- Customer contract breach.

Additionally, he stated that in order to achieve risk mitigation it is required to adopt global cyber security program approach to cover below topics:

- Governance: Operational model, Roles& Responsibilities, define resources needed.
- Risk management: measure risk financial, operational, compliance.
- Business Continuity& Disaster Recovery.
- Identity & acces management: Roles and rights on system management and review.
- Incident management: Dedicated skill persons.
- Third party services: Contract management, RACI definition.
- Create awareness: train all user to react properly.

Mr Drion summed up by stating that cyber security is a never-ending job, is seen as always excessive until something happens. It needs to be mandatory integrated in all business process.

Dr Cerruti from Carnival Corporation PLC provided an overview of maritime cyber security project. He mentioned that in 2016, Carnival Corporation engaged L3 TRL Technology to perform a cyber security review of 3 ships within the fleet, with a focus on maritime Operational Technology (OT). These ships were the Carnival Breeze, the Emerald Princess, and the P&O Britannia. As a result of this review, the company initiated a project to implement a comprehensive maritime cyber security framework. Later another vendor engaged to conduct an operational technology cyber discovery, draft policies and standards, develop training, and build a roadmap for the risk mitigation and implementation plan; based

on the past assessment and of multiple industry guidelines and standards. This vendor engagement focused on the following areas:

- Technology Discovery and Build Cyber Security Management Framework.
- Deliver OT Training and Awareness Campaign.
- OT Access Management Program.
- OT Change Management Board.
- OT Cyber Incident Response Program.

He also highlighted that as a result from the specific projects Carnival Corporation adopted the following measurements:

- OT Technical Training.
- General Awareness Training.
- Removable Media Policy – Scheduled for adoption in April 2019.
- USB Scanners – 20 scanners were purchased.
- Reporting Cyber Incidents – Carnival is developing a Cyber workflow to integrate onto the onboard systems.

Mr Chronis Kapalidis, the European representative of Hudson Analytix, presented how the commercial maritime industry is trying to deal with one of the major concerns of boardroom members and senior managers, which is risk quantification. Analyzing the findings of research conducted at Chatham House, the Royal Institute of International Affairs, and supported by Hudson Analytix, he tried to illustrate how risk can be assessed and therefore minimized, in order to consequently, minimize cost and maximize benefits for organizations in the commercial maritime sector specifically.

Highlighting the misunderstanding of cyber risk within the industry, he stated that the priority should be to understand how each organization can be affected from a cyber breach and therefore approach cybersecurity investment on a Return-on-Investment (ROI) basis. The research findings from CH indicated that ports and ships are not as vulnerable to cyber breaches as expected. The adoption of increased digitalization, though, is broadening the cyber-attack surface. Another interesting outcome was that cybersecurity cannot be isolated and dealt with independently since, in most cases, in both ports and ships, a cyber breach will have physical consequences to one or more of these ecosystems' sub-components.

Aligning with the IMO's guidelines on cybersecurity, Hudson's suggestion is the adoption of the Cybersecurity Capability Maturity Model (C2M2). The adoption of such a model on Hudson's cyber risk quantification tool, HACyberLogix, will lead, eventually, to technology and, consequently, insurance risk reduction. Empowering maritime stakeholders to rapidly deploy and economically assess, baseline and benchmark the cybersecurity capability maturity of their entire organization is the first step towards building and sustaining the organization's cyber resilience. This ongoing process requires the active participation of all staff, both in navy and commercial shipping entities.

Mr Furulund provided a briefing with theme "A Comprehensive Cyber Security Risk Management Strategy – A Norwegian shift from a defensive to a proactive and Intelligence driven approach of thinking about maritime OT and IT risks". He mentioned that merchant

vessels are continuously becoming bigger and getting more electronic systems. Seafarers often depend on technology data more than their own skills, knowledge, and senses. Crews are becoming smaller as computer systems are being used for navigation, as well as for rapid unloading, handling, and tracking of goods at ports. Unfortunately, these systems are also highly vulnerable to cyber threats.

He stated that the security risk is the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. In addition, he highlighted that in order to adopt a proper and efficient cyber and security risk management in terms of identification it is required a triad approach. More specifically it has to be continuously identified the physical and software assets, the threats to organizational resources and finally the asset vulnerabilities. Moreover, he said that an emphasis should be put on the threats as predictive, actionable intelligence on cyber threats.

Finally, he concluded that a cyber intelligence consists of three core levels. The technical cyber intelligence addresses the technical level protection, the operational cyber intelligence deals with the operational level in terms of advising, planning and coordination. Thirdly there is the strategic cyber intelligence in terms of strategic level direction and guidance.

2.6 Session 6: "The role of Cyber Security in Maritime Power, Geopolitics – International Cyber Security Legislation and Policies".

Panel 6 discussed issues regarding the role of Cyber Security in Maritime Power, Geopolitics – International Cyber Security Legislation and Policies.

Panel Members

- **Moderator:** Mr Chris Kremidas Courtney Multilateral Engagement Coordinator J9 Interagency Partnering Directorate US European Command (EUCOM).
- **Speaker:** Evangelos Markatos, Ph.D, Head Professor Computer Science Department, University of Crete, Head Distributed Computing Systems Lab FORTHS-ICS, - **"Fighting Propaganda in the era of fake news"**.
- **Speaker:** Camille E.Sailer, Esq., AEGIS Partner and President, European-American Chamber of Commerce (Princeton, NJ), - **"Transatlantic Maritime Cybersecurity: Prevailing Over Challenges; Creating Successful Safeguards"**.
- **Speaker:** Adv. Sonja Els (Lt Col) Faculty Military Science University of Stellenbosch, RSA,- **"For cyber security: does Africa Honour the International Legal Responsibility for Cyber-Related Activities?"**.
- **Speaker:** Mr Rory Hopcraft Royal Holloway, University of London, - **"The Importance of Information Sharing in the Creation and Enforcement of Maritime Cybersecurity Regulation"**.

Professor Markatos initially stated that over the past few years we have been witnessing the rise of misinformation on the Internet. Called under a variety of names, including disinformation, fake news, and propaganda, misinformation continues to increase

and propagate, placing psychological warfare in a new context and scale. Recent results, including revelations about Cambridge Analytica, suggest that misinformation has been used to influence the result of the most recent presidential elections in the United States as well as the result of the Brexit Referendum in the United Kingdom. In addition to influencing election results, misinformation has probably been used to increase the impact of (or prepare the ground for) military actions, including the recent events in Crimea. Although misinformation is initially orchestrated by well-trained agents, including state agents, it is unfortunately spread by ordinary people who are tricked to believe it and spread it among their connections online.

He presented his team project which aim is to fight disinformation using an automated approach. Their approach is inspired by the way we fight SPAM email messages. Indeed, to fight SPAM, computer scientists have developed SPAM filters: automated programs that scan all email messages of each user, categorize them as SPAM (trash email) or HAM (regular email) and filter the SPAM out of the users' mailboxes. In the specific project they follow the same approach: they process all information (e.g. tweets, posts, web documents, etc.) that users see online and characterize them as misinformation or not. If they find misinformation they clearly label it so that the user will be warned that he should be careful before believing this current piece of news.

Professor's Markatos team have developed their system as a plug in for the Chrome web Browser. The system combines in an intelligent way a variety of features to decide whether a piece of news is misinformation. Such features include: the reputation of the person (account) posting the news, the reputation of the web site where the news is hosted, natural language processing features that characterize a fake news article etc. Using a deep learning approach, they combine all these features towards providing a rating that is timely and accurate. It should be noted that the system is General Data Protection Regulation (GDPR) compliant since the plug in works locally on the user's browser without the need of external communication.

Finally, he concluded by stating that the initial results are very positive showing that the specific system is fast and effective at fighting misinformation and reducing the spread of propaganda.

Mrs Sailer initially highlighted the importance of the maritime transportation and she stated that given the critical horizontal nature of maritime shipping, nothing less than over-arching, integrated, tech-savvy systems, enforcement and information approaches are urgently required.

She analyzed the characteristics of current Maritime Security. In her mind modern day maritime cyberhackers have taken on the attributes of the pirates of past centuries, not only threatening cargo and finances but also putting crew and others on board in life and death situations.

In her words, geopolitical stressors such as Brexit and philosophical swings among global civil societies and the officials they elect exacerbate the accelerating potential of maritime cyber threats especially as the rewards for malfeasance are growing exponentially. Populist and inward-looking political trends that emphasize protecting national borders rather than cross-border collaboration and individual country decision-making rather than multilateral

cooperation serve to heighten the difficulty of effective maritime cybersecurity.

She discussed the EU's GDPR and the 2015 U.S. Cyber Information Sharing Act and she conclude that a positive element of GDPR is its requirement to enforce common data breach protection notification calling for a company to report any breach of its system within 72 hours. The additional benefit of this provision is that industry awareness almost by force will need to improve and implement better response time to potential vulnerabilities.

She finished by highlighting the requirement for an International Collaborative Strategy among major stakeholders and she focused on the improvement of training and exercises between NATO and the EU and yoking those two entities for training and exercises with the U.S. thereby forming a maritime cybersecurity triangle. Specific areas where this cooperation could be valuable include forensics training and judicial coordination in prosecuting cybercrimes.

Lt Col Els stated that effective global cyber governance demands a collective effort by sovereign states, international and regional organizations, and non-state actors.

The aim of her presentation was to investigate whether Africa, and more specifically the African Union (AU) can ensure that, with reference to cyber security, regional peace, security and stability are maintained in response to the international communities' collective responsibility of "due diligence". She focused on pro-active cyber related provisions of good practices by NATO and the EU in comparison with that of the AU. Then she investigated to which extent the AU encourages its member states to honor international law obligations *erga omnes* towards the international community in the open digital domain.

Finally, she stated that a comparative analysis of the scope of the Budapest Convention on Cyber crime and the African Union Convention on Security in Cyberspace and Personal Data Protection will disclose Africa's current position on cyber security. Safeguards and action are needed to protect the global cyber domain, both in the civilian and military environments. Africa needs to increase the continental ability to fight cyber threats and close the cyber security skills gap.

Mr Hopcraft discussed the importance of the maritime community in the understanding, and mitigation, of threats to the maritime domain. By using the example of piracy and shipping in the Polar regions, he highlighted that through an international forum, the maritime community can share vital information to mitigate maritime threats successfully. The community plays three important roles within the creation of maritime cybersecurity regulation.

The first role that this community plays is in understanding the threat. The diversity of the maritime community's membership allows discussions to include local, regional and international stakeholders, as well as the required technical expertise. Through this collaboration of stakeholders, it allows the maritime community to understand the threat from all perspectives internationally. The second role of the community understands the type of regulation that needs to be created. By the IMO engaging with the maritime community, it ensures that regulation and guidance that it creates is acceptable by the community. If the community does not accept the regulation or guidance, there will be little uptake, which will do

little to reduce the risks to cyber-enabled technology. The third and final role the community will play is through the enforcement of the regulation It is then through the compliance process that issues and concerns will be noted and fed back into the IMO, ensuring that amendments are made to safeguard the continued effectiveness of maritime cybersecurity regulation.

Finally, he stressed the importance that this international community, and its information-sharing capabilities, will have on the enforcement of regulation, assisting in the continued safety and security of all users of the maritime space.

2.7 Closing Remarks.

NMIOTC Commandant Commodore Stelios Kostalas GRC(N) highlighted that the most important outcome of the conference was the bridge building between public and private sectors, the fusion of different approaches, and the development of common understanding leading to productive co-operations and synergies.

He emphasized to the fact that cyber security challenges in the maritime spectrum (both military and commercial) demand a constant updating effort and a robust training framework. He concluded that the conference, along with the cyber security resident course 19000 and the Navy Cyber Defense Exercise “Cyber Gordian Knot” organized by NMIOTC, are the best proof of the NMIOTC steady commitment to be in the front line of capacity building in the Maritime Domain Cyber Security, an area and a topic that will dominate the efforts, at least for the next decade.

3. 2019 NMIOTC CYBER SECURITY CONFERENCE MAIN TAKEAWAYS

A. Maritime Cyber Security:

- Gray is the new color of war.
- Cyber is borderless by nature – and cannot address in isolation.
- More sophisticated attacks are multi-modal, not just cyber.
- Cyber involves a bilateral human-network engagement – humans are part of cyberspace.
- Maritime industry moving toward full digitization.
- We live in a dual-use overlap era.
- Are we prepared or even aware of convergent technology threats?

B. Risk Management:

- There are no useful tools for quantitative risk assessment for multi-modal attacks.
- The weakest link is human.
- Learning and evolving: Emulating cyber attacks to provide realistic assessment of security and response.
- The importance of red teaming and constantly testing our own readiness and vulnerabilities.

- Cyber risk management in an era of increasing complexity and with more expectation of remote access.

C. Resilience, Decision-making, and Response:

- Resilience: increasing operational resilience, capacity building, prevention and response coordination.
- A military commander needs to feel pain in an exercise in order to learn how to cope with a cyber attack (lose a vessel, etc).
- Leveraging AI to support decision-making.
- The challenge of attribution of cyber attacks – and reminder the rest of hybrid community sees cyber as having the easiest and fastest means to achieve attribution.
- Interoperability is paramount – not optional. Requires collaboration in entire supply chain.
- Disinformation and propaganda: AI + human judgment necessary for any effective detection engine.

D. Public-Private Issues:

- Public-private interface. Cyberspace infrastructure owned and controlled by private entities.
- Industry is the first to identify emerging cyber security threats – not governments.
- Only 6% of smaller companies feel comfortable with their level of cyber security – yet they are part of the larger supply chain. Thus, its in everyone's interest to cooperate.
- AI and Blockchain are of use to the private sector, however they are not as attractive to military or governing applications due to cost and technology latency of systems. Hence these innovations are not as connected to civil/military applications.

E. Remediation, Lessons Integrated, Training:

- Remediation. Importance of sharing vulnerabilities and lessons integrated.
- Continuity of operations – physical and cyber domains.
- Cyber situational awareness must be included in military doctrine.
- The cyber attack surface is larger than ever; entire economies, financial systems, maritime shipping and logistics systems, communications and media, etc.
- Quick wins are still possible if we apply known protections and updates; cyber security compliance.
- Cyber security as mission assurance.
- Different approaches to cyber risk quantification and its associated challenges.
- The cultural, organizational, and technological constraints to cyber security – culture eats strategy.

F. Political Challenges:

- Cyber deterrence – difficult since cyber sovereignty is still not defined. Without sovereignty, cannot deter.
- Rising populism as a challenge to the ever greater need for international cooperation.
- EU-US cooperation in cyber security – positive trends yet not well known.
- Cyber security in Africa; Malabo convention – the challenge of getting 55 sovereign states to agree to an overarching cyber security agreement. Points to the difficulty of establishing global norms.
- Global best practices are nonetheless valuable.
- Information sharing: until there is a major impact, little interest in improving. Estonia example.

ENCLOSURE 2 TO:
NMIOTC NOTE: NU: 120
NSC-74/ 02 Aug 2019

NMIOTC 3rd CYBER SECURITY CONFERENCE AGENDA

TIME	TOPIC	SPEAKER
10 Apr 19		
0830-0900	**Registration – Welcome Coffee - Networking**	
0900-0945	Welcome address • NMIOTC Brief • Admin Brief	Commodore Stelios Kostalas GRC N NMIOTC Commandant • LT CDR Christos Tasiopoulos GRC N • LT CDR Kostas Papanastasis GRC N
0945-1130	**SESSION 1 Cyber Security in Maritime Operations**	
	Key Note Speech Opening: Fred S. Roberts, PhD Distinguished Professor of Mathematics, Rutgers University, Director of Department of Homeland Security University Center of Excellence CCICADA: Command, Control and Interoperability Center for Advanced Data Analysis **Moderator:** Capt (N) Phd Student eng. Sebastian Popescu ,Head of Communication IT&AC Office of Romania Navy HQ • Chronicle of Maritime Cyber Attack • Operationalisation of the maritime cyberspace : MARCOM's vision	• Mr Emmanouil Christofis, SHAPE J6 Cyberspace , Strategic Plans and Policy • MARCOM Captain Christophe Eugene - FRA N MARCOM - ACOS N6 Cyberspace

	• Building cyber resilient ports through partnerships • Maritime Cybersecurity Afloat	• CAPT Amy B. Grable, USCG, Deputy, Coast Guard Cyber Command (CGCYBER) • CJOS COE,Cdr. Neculai GRIGORE
1130-1200	**Group Photo – Coffee Break**	
1200-1345	**SESSION 2 NATO-EU Cyber Security Collaboration and Initiatives**	
	Key Note Speech Opening: Mr Michael Tsamaz, CEO OTE Group **Moderator:** Dinos Kerigan-Kyrou PhD CMILT, Emerging Security Challenges Working Group	
	• Cybersecurity Challenges and EC initiatives	• Dr. Nineta Polemi, European Commission, DG CONNECT, H1, Programme Manager- E.U. Policies
	• ESDC Cyber ETEE Platform	• Dr Gregor SCHAFFRATH, EEAS/ESDC
	• Cyber Defence Systems Engineering: A framework to identify requirements described into a dedicated Cyber Defence Architecture to inform Capability Development	• Mr Mario Beccia,PO Capability, Armament & Technology Cyber Defence, EDA
	• FEDERATED MISSION NETWORKING (FMN) – Framework development, Maritime implementation and Cyber Security Challenges.	• CDR Sérgio Rodrigues, Lt COL Diego Sirvent, SHAPE J6 Cyberspace FEDERATED MISSION NETWORKING (FMN), Secretariat
1345-1445	Lunch Break - Networking	
1445-1615	**SESSION 3 Latest Advanced Technology Solutions and Concepts**	
	Key Note Speech Opening: Mr Dimitrios Koutsopoulos, CEO at Delloite Greece	

	Moderator: Prof Gritzalis Dimitrios, Professor & Associate Rector Athens University of Economics & Business • Maritime Software Security through In-Depth Assessment, Education and Recovery • SAURON: Physical and Cyber Situation Awareness Fusion Models • Results on container ship route risk-based interdependency modeling • Cyberattacks on critical infrastructure – Modus operandi, examples and considerations.	 • Prof Barton P. Miller, Prof Elisa Heymann University of Wisconsin-Madison • Dr. Stefan Schauer (AIT) and Mrs Eleni-Maria Kalogeraki (Dept. of Informatics, University of Pireaus) • Dr George Stergiopoulos, Dr Theodore Douskas, Athens University of Economics & Business • Mr Ilias Chantzos, LLM, MBA Senior Director EMEA & APJ Global CIP and Privacy Advisor Government Affairs, Symantec Corporation
1615-1620	Wrap up	Mr Chris Kremidas Courtney Multilateral Engagement Coordinator J9 Interagency Partnering Directorate US European Command (EUCOM)
	END OF FIRST DAY	
1930-2200	Ice Breaking Event	

TIME	TOPIC	SPEAKER
11 Apr 19		
0900-1045	**SESSION 4 Research Innovative Results in Maritime Cyber Security and Cyber Defence**	
	Key Note Speech Opening: **Dr George Troulinos, CEO Intracom Defense Electronics** **Moderator:** Evangelos Markatos, Ph.D, Head Professor Computer Science Department, University of Crete, Head Distributed Computing Systems Lab FORTHS-ICS	
	• Improving maritime security through an integrated approach	• Dr Alessandro Garibbo Strategic Marketing, Security & Information Systems Division Leonardo Industry
	• Applying lessons from maritime dispute to cyber deterrence.	• Mr Kah Kin Ho, Senior Director EMEA Public Sector
	• Maritime Cyber Threat Landscape and lessons leant from the front line. Cyber Everywhere: The Bow-Tie and the real-life approaches	• Mr Christos Vidakis, Principal Risk Advisory, Cyber Risk Services,Deloitte
	• How to Achieve Business Continuity through Effective Cyber Risk Mitigation and advance Crisis Response	• Mr Isidoros Monogioudis, Principal Cyber Security Advisor to JV DIAPLOUS Maritime Services / FOCAL POINT Cyber Security
	• How to Operationalize Cyber Threat Intelligence for Maritime Organizations	• Mr Chris Pike , Cyber Threat Intelligence Advisor ,CrowdStrike Inc

1045-1115	Coffee Break – Networking	
1115-1300	**SESSION 5 Secure maritime logistics and Protection of Maritime Critical Infrastructures**	
	Moderator: Mr Emmanouil Christofis, SHAPE J6 Cyberspace , Strategic Plans and Policy	
	• Cyber-security in the Maritime Sector: Previous cases and lessons learned from other sectors for commercial shipping	• Dr Stavros Karamperidis, Lecturer in Maritime Economics, Plymouth Business School
	• Overview Of The Cyber Security Threat Environment From The Perspective Of a Large Commercial Operator	• Mr Quentin Drion IT Director of Infrastructure and Operations MSC Mediterranean Shipping Company SA
	• Maritime Cybers ecurity status of Carnival Corporation & PLC - March 2019	• Dr Cerruti Franco, IT Security and Operation Director ,Carnival Maritime - Costa Group
	• Cyber Risk Quantification: A Case-study from the Commercial Maritime Sector	• Chronis Kapalidis, Hudson Analytix, PHDc, WMG, University of Warwick, Academy Fellow, Chatham House
	• A Comprehensive Cyber Security Risk Management Strategy – A Norwegian shift from a defensive to a proactive and Intelligence driven approach of thinking about maritime OT and IT risks.	• LTC Ret. Freddy Furulund Director of Security & Contingency Intelligence & Operations Centre (IOC) Den Norske Krigsforsikring for Skib Norwegian Shipowners' Mutual War Risks Insurance Association
1300-1400	Lunch Break – Networking	

1400-1530	**SESSION 6 The role of Cyber Security in Maritime Power , Geopolitics – International Cyber Security Legislation and Policies**	
	Moderator: Mr Chris Kremidas Courtney Multilateral Engagement Coordinator J9 Interagency Partnering Directorate US European Command (EUCOM)	
	• Fighting Propaganda in the era of fake news	• Evangelos Markatos, Ph.D, Head Professor Computer Science Department, University of Crete, Head Distributed Computing Systems Lab FORTHS-ICS
	• Transatlantic Maritime Cybersecurity: Prevailing Over Challenges; Creating Successful Safeguards	• Camille E.Sailer, Esq., AEGIS Partner and President, European-American Chamber of Commerce (Princeton, NJ)
	• For cyber security: does Africa Honour the International Legal Responsibility for Cyber-Related Activities?	• Adv. Sonja Els (Lt Col) Faculty Military Science University of Stellenbosch, RSA
	• The Importance of Information Sharing in the Creation and Enforcement of Maritime Cybersecurity Regulation	• Mr Rory Hopcraft Royal Holloway, University of London
1530-1545	Wrap up	Mr Chris Kremidas Courtney Multilateral Engagement Coordinator J9 Interagency Partnering Directorate US European Command (EUCOM)
1545-1600	Closing Remarks	Commodore Stelios Kostalas GRC N NMIOTC Commandant