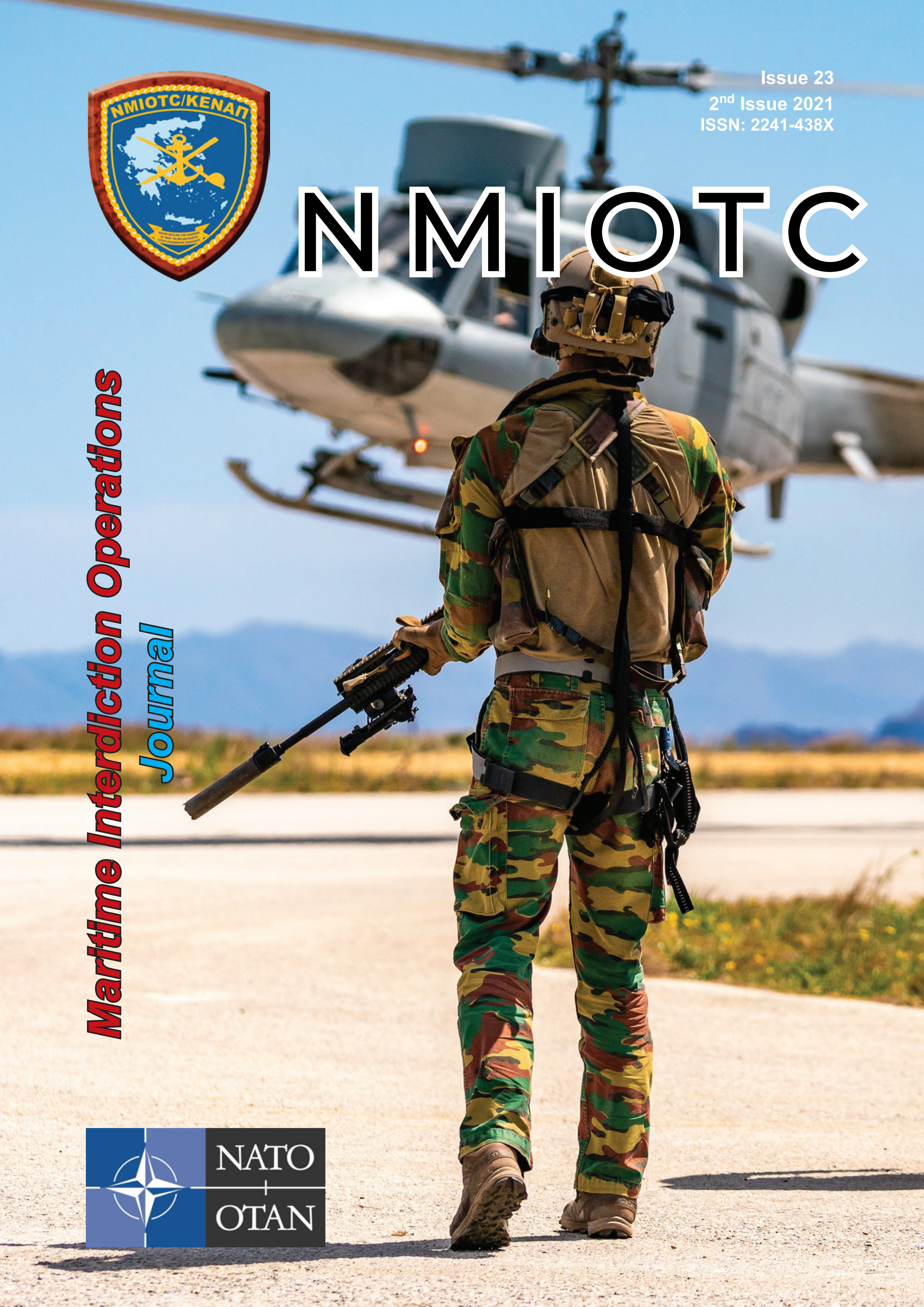


Issue 23
2nd Issue 2021
ISSN: 2241-438X

NMIOTC

Maritime Interdiction Operations Journal

NATO
OTAN

NATO
Maritime Interdiction Operational Training Centre

13th NMIOTC
ANNUAL CONFERENCE
7th and 8th of June 2022

SAVE THE DATE

"Countering Terrorism Threats in Maritime Domain:
How effective Interdiction strengthens
Alliance's Deterrence and Defence Objectives"

6th NMIOTC CONFERENCE
ON CYBER SECURITY IN MARITIME DOMAIN

27th – 28th September 2022
Souda Bay, Crete

CONTENTS

COMMANDANT'S EDITORIAL

MARITIME SECURITY

CYBER SECURITY IN THE MARITIME DOMAIN

NMIOTC COURSES & ACTIVITIES

NMIOTC TRAINING

HIGH VISIBILITY EVENTS

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Commodore Ch. Thymis GRC (N)
Commandant NMIOTC

Executive Director
Commander G. Finamore ITA (N)
Director of Training Support

Editor
Commander P. Pantoleon GRC (N)
Head of Transformation Section

Layout Production
Lieutenant I. Giannelis GRC (N)
Journal Assistant Editor

Cover Photo: Evan Possley

The views expressed in this issue reflect the opinions of the authors, and do not necessarily represent NMIOTC's or NATO's official positions.

You may send your comments to:
pantoleonp@nmiotc.nato.int

NMIOTC Commandant's Editorial

NMIOTC, located in this beautiful but also highly strategic location in Souda Bay, stands as the only NATO quality assured educational and training facility, dedicated to training and research in the maritime domain. Our core aim and endeavors correspond to the need of the alliance for enhancing both capabilities and awareness in maritime interdiction, which is the key enabler to maritime security, and as by definition aims to 4Ds: Detect-Delay-Disrupt-Destroy all asymmetric and hybrid threats including cyber ones, before they become a threat to ourselves or to our friendly forces.

This autumn NMIOTC organized its 5th NMIOTC Conference on Cyber Security in the Maritime Domain. It is well known that our strategic situation is characterized by complexity. We used to say it was complicated when we had to interact with many factors, but we could analyze them in order to draw reasonable conclusions to drive our decisions. Now, our world is complex, we have to deal with so many interconnected and transnational factors that it is impossible to comprehend all possible outcomes, thereby making surprise more possible, decision-making based on imperfect information norm and failure an increased possibility.

We recognize complexity is the new norm and cyber has undeniably been a significant factor by having changed our world. The ongoing digital revolution has fueled prosperity and efficiency in our globalized economy and has become inextricably linked with all aspects of our modern life and all areas of society, including industry and economy, as well as governmental domains, such as defense and security. These innovations will continue to drive global changes for the foreseeable future, and from most perspectives, will continue to evolve at astonishing speeds.

Data seems to be the driving force in

this brave new world of communication networks, artificial intelligent led technologies, and remotely connected robotics. I cannot avoid mentioning that the current unprecedented situation that we all face with the covid-19 pandemic has demonstrated this paramount need for a holistic international and interagency approach and cyber resilience to cope with such large-scale challenges. Yet, in the wake of this progress, lie a growing number of challenges and risks that threaten the very core of global security and prosperity. The sea was always the guarantee for the wellbeing and prosperity of our nations and their people. And unfortunately, the size and scale of the maritime environment and the various sectors (industry, commercial, civilian, military) interacting and operating within, makes it a particularly advantageous environment for potential cyber offenders who become more and more sophisticated and seek to undermine the authority of these actors and their actions.

In December 2018 the U.S. Navy reported that hackers had repeatedly stolen information from navy contractors including ship maintenance data and missile plans. In May 2021 the Norwegian energy technology company Volue was the victim of a ransomware attack that resulted in the shutdown of water and water treatment facilities in 200 municipalities, affecting approximately 85% of the Norwegian population. In the same month the colonial pipeline, the largest fuel pipeline in the United States, was also the target of a ransomware attack. the energy company shut down the pipeline and later paid a $5 million ransom. A few years ago, nobody could imagine that all these incidents could happen, and these are some typical examples of what the chameleon face of cyber threats can be. We have acknowledged the need for synergies among all stakeholders which are more than ever before required, in order to effectively deter and defend against advanced attacks and to avoid or at least decrease any catastrophic impacts to our nations, industries, and peoples. Countering hybrid cyber threats calls for a holistic and collaborative approach but also with the ability to join the dots between seemingly separate, but effectively interconnected events. Cyber information sharing, collaborative incident handling, cyber situational awareness, and finally resilience are therefore considered paramount and require a coherent network of civilian, industrial, commercial and military cyber defense strategies and operations. Bringing all this to our domain of expertise, the maritime domain, I would like to emphasize that maritime operations are conducted by technology-intensive platforms, which today rely heavily on information systems, and that the impact of cyber security incidents on the conduct of current and future maritime operations could be devastating.

We strongly believe that cyber capabilities are a critical enabler of success across all missions, and by ensuring that these capabilities are leveraged by commanders and decision-makers at all levels in order to operate effectively, we must develop and constantly update a diverse set of cyber capabilities and authorities, therefore NMIOTC has endorsed the integration of Cyber Security aspects in all its training products and activities.

Charalampos Thymis
Commodore GRC (N)
Commadant NMIOTC

5th NMIOTC Conference on Cyber Security in the Maritime Domain

by Wendi Brown (1wendibrown@gmail.com)
Lieutenant Colonel U.S. Army Reserve

Our 5th NMIOTC Conference on Cyber Security in Maritime Domain was held on September 29-30, 2021 at the NMIOTC's premises in Souda Bay, Crete, Greece. Commodore Charalampos Thymis, the NMIOTC Commandant, invited speakers that provided new and updated knowledge and information about maritime cybersecurity. Wendi O. Brown, Lieutenant Colonel U.S. Army Reserve, provided this report.

1st DAY

Keynote Speaker: Brigadier General Dimitrios Kesopoulos GRC (A), ACOS SHAPE J6 Cyberspace

I am Brigadier General Dimitrios KESSOPOULOS, Assistant Chief of Staff J6 CYBER at SHAPE.

In my role of ACO's CIS Operational Authority I have been often witnessed and prime subject to the nowadays more and more frequent cyber security challenges (including the ones within the maritime domain) which NATO has to face every day, and this initiative from NMIOTC is definitely on the right "course", to use a navy term.

These emerging cyber security challenges pose a serious threat also for the maritime environment, as shown in many cases during the last 3-4 years, and should be handled collectively inside the NATO Cyberspace Operations community and under the solid foundation of information sharing and situational awareness. That's exactly the reason why SHAPE encourages this endeavor at NMIOTC and will support with Subject Matter Experts as well.

This Conference is a great opportunity to bring together all the key stakeholders belonging to the Maritime community in order to make clear that cyber defense is not only about technical issues or merely ensuring C2, but it has very deep and DIRECT operational implications, with adverse effects on the commanders' ability to freely conduct military and security operations.

Let me start with "The History and Evolution of Cyberspace as a NATO Domain of Operations" has taken some time. While there was obviously prior thought, the journey itself commenced in 2002, with the recognition of cyber threats to NATO networks.

Following the cyber attack on Estonia in 2007, in 2008 NATO Cyber Defence Policy 1.0 was formulated, which was updated in 2010, again in 2012, and again in 2014 as NATO's understanding of the potential operating environment, and the potential threats, increased. 2016 brought the Cyber Defence Pledge from Nations, and recognition of cyberspace as a Domain of Operations. Leading in 2018 to the founding of the Cyberspace Operations Centre on 31 August 2018 with the intent to integrate cyber effects and provide Domain advice to SACEUR. All of which can be summarized as a series of political decisions and guidance, leading to actions in the military sphere.

I would like now to tackle some main areas in Cyberspace that have a significant role. I will start with the Hybrid Warfare.

Hybrid Warfare

What I just said about the military, however, should not mistake you into thinking that cyber warfare is or will be a type of warfare in and of itself. More likely, cyber will be a fundamental component, to varying degrees, of future conflicts along with other domains of warfare, capable even to act as a sort of "force multiplier" to re balance or increase the performances of military actions on the modern battlefields.

A big example of this is the so-called Hybrid Warfare, a type of warfare suing a wide range of overt and covert military and civilian measures are employed in a highly integrated fashion. We have seen examples of Hybrid Warfare employed in many small and large conflicts around the world in the past 25 years, It seems that cyber's role in Hybrid Warfare is constantly growing in importance and application. It is in fact the perfect tool for any actor waging Hybrid Warfare tactics due to its low cost of entry, easily replicability of the cyber-weapons, the difficulties related to a clear attribution by State Actors and the potential large scale impacts on the military and civilian societies.

This is already proved by the published strategies and proven tactics of historical NATO, competitors such as Russia, China, terrorist groups, which aim to challenge our Alliance and already have demonstrated their intentions in Hybrid warfare using their Cyber offensive capabilities as their weapon of choice.

Emerging and Disruptive Technologies (EDTs)

At their meeting in London (2019), NATO Leaders endorsed the "Emerging and Disruptive Technologies Roadmap" (EDT Roadmap), highlighting that Allies and NATO should address the potential opportunities, security risks and ramifications of these new technologies in a collective effort to maintain NATO's technological edge.

As outlined in the EDT Roadmap, the DEFENCE POLICY AND PLANNING COMMITTEE DPPC (R) "should consider potential implications for NATO's strengthened "deterrence and defence" posture across various domains, and integrate these into the ongoing work at the appropriate juncture.

From the deterrence and defence perspective, practical EDT applications span across multiple areas. EDTs are expected to play a critical role in future warfighting and building preeminent forces that can decisively operate across domains and deliver joint effects. Imagine how Artificial Intelligence (AI), Big Data Analytics, Quantum Computing could have a huge impact on Alliance Operations and Missions (AOM).

Certain technologies are expected to have a particularly revolutionary and transformative effect, such as quantum technology and AI which has the potential to become a game changer in many areas, including sensing, cryptology and analytics, providing unprecedented computing capability and highly secure communications

Key application areas and the benefits of many EDTs will be available to both NATO

BUT ALSO to its potential adversaries, who will seek to exploit such technologies for asymmetric advantage. The advantages enabled by EDTs can become vulnerability, as many technologies have both defensive and offensive applications. Given the wide range of applications stemming from EDTs, they have the potential to substantially impact NATO's security, including across the "3Rs" – Readiness, Responsiveness and Reinforcement.

EDTs are expected to have a substantial impact on future warfighting. High operational tempo will be the main characteristic of future warfare. Speed will be required for operations planning, deployment and sustainment, collecting and processing intelligence, and delivering the required effects. These elements will need to feature in training and exercises to ensure that NATO adapts accordingly.

Next topic is the NATO's Comprehensive Cyber Defence Policy

NATO's Comprehensive Cyber Defence Policy

What is, then, NATO's approach to cyber defence in front of such challenging and fast-moving cyber landscape?

As NATO's essential purpose is to safeguard the freedom and security of its members through political and military means, its fundamental cyber defence responsibility is to defend its own networks. Also, NATO recognises that international law, including international humanitarian law and the UN Charter, applies in cyberspace.

Malicious cyber actors also increasingly seek to exploit the "trust" which users put in providers, products and processes in order to carry out malicious activities. This includes seeking to exploit weaknesses in hardware and software supply chains, as well as targeting services outsourced to managed service providers. Apart from the direct economic and reputational costs, trust in an open and free cyberspace governed through a multi-stakeholder model is being eroded.

To this end NATO will,

- defend its CIS and networks against current and future cyber- and cyber enabled threats, and ensure swift mitigation and recovery;
- continue implementing cyberspace as a domain of operations in a multi-domain environment, mainstream

cyber aspects across all domains, and leverage cyberspace in line with the Concept for Deterrence and Defence in the Euro-Atlantic Area;

- provide a platform for:
  - enhancing and contributing to Allied national cyber defence and resilience;
  - deterring and responding to the full spectrum of cyber threats;
  - harnessing mutually beneficial partnerships;
  - leveraging innovation and knowledge;
  - information sharing and consultations.

NATO's Comprehensive Approach To Cyber Defence

In support of its three core tasks, NATO cyber efforts are three-tiered:

- At the political level, Allies set policy to articulate political oversight, including direction and guidance on Alliance political and public messaging, and on how NATO's cyber related objectives contribute to the overall deterrence and defence posture of the Alliance, and promote stability in cyberspace.
- At the military level, the Alliance conducts activities in- or enabled through cyberspace in support of military objectives and operations across all domains – cyberspace, land, sea, air and space – through crisis management, Alliance Operations and Missions (AOM) and, if necessary, collective defence.
- At the technical level, persistent efforts focus on all aspects related to protecting and defending communication and information systems (CIS) and networks to ensure mission assurance and business continuity at all times. NATO's ability to credibly defend its own CIS and networks relies on a mature governance structure for cyber defence.

Cyberspace Operations Centre (CyOC)

The NAC tasked ACO with the challenging task of operationalizing cyber space as the 5th Domain, by building up cyber resilience and situational awareness and warning within ACO.

The CyOC is seen as a key factor in this operationalising the cyberspace domain, and it was presented as a major feature of the NATO Command Structure (NCS) Adaptation (NCS-A) in the cyberspace functional area in 2018.

CyOC's Concept of Operations is very briefly:

- Designed to function as the theatre component for cyberspace
- Full spectrum cyberspace situational awareness across the Alliance
- Immediate decision support for response options to cyberspace events/incidents/attacks with mission assurance as the goal
- Focal point for coordination of voluntary National effects
- Coordinating Authority for cyberspace operational planning

Success of Cyberspace Domain Roadmap is therefore, to a great extent, dependent on the CyOC. It is essential to foster the relationships between CyOC and all relevant stakeholders, within and outside the NCS, including NCIA and the newly-established Chief Information Officer function for the NATO Enterprise. This should be continued as a priority for 2022, in alignment with the NCS adaptation, focusing on the cyberspace C2 concept of operations and the unrestricted full operational capability of CyOC.

Consequence Management/Continuity of Operations

If and when NATO's military structure is asked to go into a real fight, despite our best efforts, it is unlikely we will be able to defend against all the anticipated and unanticipated cyber-attacks, exactly due to the reasons I mentioned at the beginning of this speech.

So, ACO's challenge is to prepare our field commanders and units to be able to operate in a degraded or contested cyber environment where the information at their disposal might be unavailable, partial or even unreliable due to integrity concerns following network breaches.

But how do we do that? The answer is multifaceted:

- First and most important, we need to develop our operational plans taking into account that portions of cyberspace may be unavailable to us during combat operations as well as many important C2 functions. To take a very simple example, if the Maritime Command and Control System (MCCIS military system) or the Vessels Traffic Management System (civilian system) experiences a cyber-attack which disrupts the Recognised Maritime Picture (RMP).
  - In one of a past SteadFast COBALT Exercise, the Red Team ended up putting more of their focus on the maritime scenario. The start of the scenario was network access with a dropbox and the end goal was the injection of a hostile submarine in the MCCIS Recognized Maritime Picture (RMP) in close proximity to allied ships in the Baltic Sea. (Slide). This RMP could create a very tense situation, until it could be validated by the supposed source to be an error. Furthermore, once validated by the source to be an error, the reliability of the RMP would be questionable while the root cause of the glitch is unknown.
  - Our operational plans would state how to execute 'Impact Analysis'' and 'Consequences Management'' processes in order to keep combat Maritime operations going on. Restoral of the actual systems would be a secondary concern. And that's was exactly the aim of the maritime scenario I mentioned before, to force the Operational Staffs to assess the operational impact and provide Consequence Management to the Commander.

- Second, we develop REALISTIC exercise scenarios which test the operational plans, how well our CyOC is able to keep operations going despite cyber-attacks and how well our commanders are able to execute the plans in a degraded information environment.
- Third, and perhaps the most challenging to implement, is that throughout the military command structure, cyber needs to be considered a proper operational domain and not just a support function, despite its "gluing" role I mentioned few minutes ago. This underlying foundation is critical in developing a modern military and in conducting modern warfare with modern means.

Senior leadership needs the higher and levels of awareness to understand the impact of a situation on their organization's ability to execute its operations and missions. A tremendous tool in achieving this goal will be the cooperation with the Industrial part of the society, which is always looking for cutting-edge technologies and best practices to counteract the actions of malicious actors in and through cyberspace.

Not only, in fact this information should have a scope! It must be correlated to the context of the mission or operations, thus exposing the real impact to its operations in order to support.

Decision making process on consequence management will be the founding bases for MISSION ASSURANCE.

I hope that I managed to tackle briefly all the main topics that are working at SHAPE regarding cyberspace operations. My SME is here as well to provide further insight and clarifications.

Ladies and gentlemen. Thank you for your patience and your attention.

SESSION 1: "The impact of emerging cyber risks in maritime security"
Moderator: Professor Nineta Polemi, University of Piraeus

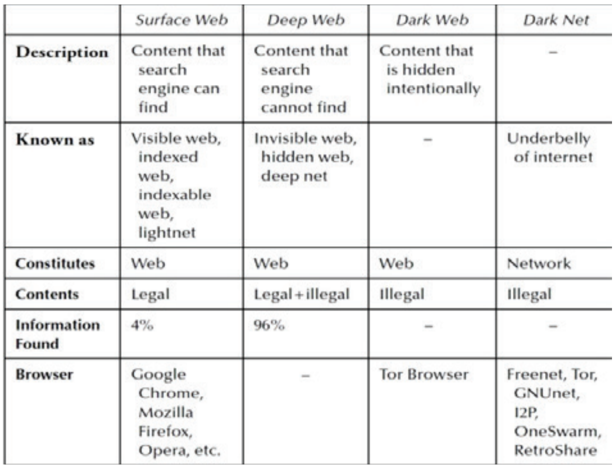
Lecture: "Unknown Field of Dark Web" Professor Nikitas Nikitakos, University of the Aegean

Professor Nikitakos described the following different types of Web below Surface Web:

- The Deep Web which includes financial records, medical records, military records, leaked documents, and the Dark Web
- The Dark Web which is the hidden collective of internet sites and only accessible by a specialized web browser like TOR (The Onion Router) is a software that is a key enabler of anonymity in communications
- It is used for people concerned with privacy, along with activists/whistleblowers and for keeping internet activity anonymous and private which make it suitable to be used for illegal activities. Contains 1000 times more sites than general sites of World Wide Web. It is the marketplace for drugs, guns, weapons, child pornography, hacked credit cards etc.
- The Dark Net which is a part of dark deep web, and it is a collection of networks and technologies used to share digital content.

The differences among surface, deep web, dark web, and darknet are shown in table 1 below:

Cybercrime in the Dark Web can be in individual, property or government level where criminals hack government or military websites, or by using social networks to enable their illegal activity.



	Surface Web	Deep Web	Dark Web	Dark Net
Description	Content that search engine can find	Content that search engine cannot find	Content that is hidden intentionally	–
Known as	Visible web, indexed web, indexable web, lightnet	Invisible web, hidden web, deep net	–	Underbelly of internet
Constitutes	Web	Web	Web	Network
Contents	Legal	Legal+illegal	Illegal	Illegal
Information Found	4%	96%	–	–
Browser	Google Chrome, Mozilla Firefox, Opera, etc.	–	Tor Browser	Freenet, Tor, GNUnet, I2P, OneSwarm, RetroShare

The key takeaway was that Dark Web crime prevention can be achieved by monitoring the kits and services attackers use, the changes in attacker monetization strategies, collecting cybercriminal tradecraft, and by monitoring intel on vulnerabilities as they go through their three phases.

Lecture: TRESSPASS (robust Risk based Screening and alert system for PASSengers and luggage) Ioannis Papagiannopoulos, Port Facility Security Officer - Deputy Port Security Officer in Piraeus Port Authority

TRESSPASS (robust Risk based Screening and alert system for PASSengers and luggage), is a European research project in the H2020 framework and Border and External Security thematic area, receiving EU funding. The scope of the project is to modernize the way the security checks at border crossing points are operated on land, air, and sea. TRESSPASS imports the concept of "risk-based" security checks and proposes an analytic framework for modeling risk as well as a systematic approach of quantifying risk, based on a set of indicators ranging from real-time behavior analytics to intelligent information extraction and sharing that can accurately be measured across all four tiers of the EU Integrated Border Management. The 6 main objectives for TRESSPASS are to:

- Develop a single cohesive risk-based border management concept that covers the entire scope, i.e. a four-tier trans-national, multi-modal security tunnel, including concept of operations.
- Apply an ethics and data protection "by design" approach to ensure legal and ethical compliance of the risk-based screening solutions at borders.
- Include passenger trust in risk management model and perform sensitivity analysis and optimization.
- Develop three pivoting pilot demonstrators for demonstration of key conceptual, operational and technical aspects of this concept.
- Demonstrate the validity of the single cohesive risk-based border management concept by using the developed pilot demonstrators, red teaming and simulations.
- Prepare for the further development of this concept beyond this project by linking to other known risk-based border management projects.

Lecture: "Maritime Cyber Risk and Global Security" Mr David Nordell, Synapse Cyber Strategy, Israel

Mr David Nordell' paper that was presented is included in the current Journal issue on page 40.

SESSION 2: "Maritime Cybersecurity technologies and industrial products"

Moderator: Dinos Kerigan-Kyrou PhDC-MILT, Emerging Security Challenges Working Group

Lecture: "Safeguarding the Cyber Borders in Maritime" Mr Ewan Robinson Yango Satellite Communications

The new cyber requirements mean that we have to be able to understand, control, and be responsible for all the equipment and systems within our IT/OT environment on-board. The legacy hardware and software, underpinning the communications and connectivity and used by the providers, resellers, and their agents, is riddled with such poor architecture, procedures, and methodologies, that its inclusion makes it inherently untrustworthy and unable to be directly controlled or monitored.

The borders for communication are used by Satellite Operators, Wholesale Chain/Service providers, and Resellers/Agents may be obsolete and we need to embrace, Starlink, OneWeb, 5G, and other technologies which will become the new mainstream.

Mr. Robinson during his research conducted a proof of concept cyber-attack scenario against commercially available maritime hardware and he was able to identify and infiltrate connection ports, eavesdrop on available data, access webcams, access to the onboard antenna, access to the firewall to change firewall configurations, and check for unencrypted passwords.

Lecture: "Artificial Intelligence and Cybersecurity in 2030 – possible implications for the maritime sector" Dr. Swantje Westpfahl, Mr Tim Dalhoefer, Institute for Security and Safety at the Brandenburg University of Applied Sciences

Dr. Swantje Westpfahl's and Mr Tim Dalhoefer's paper that was presented is included in current Journal issue on page 25.

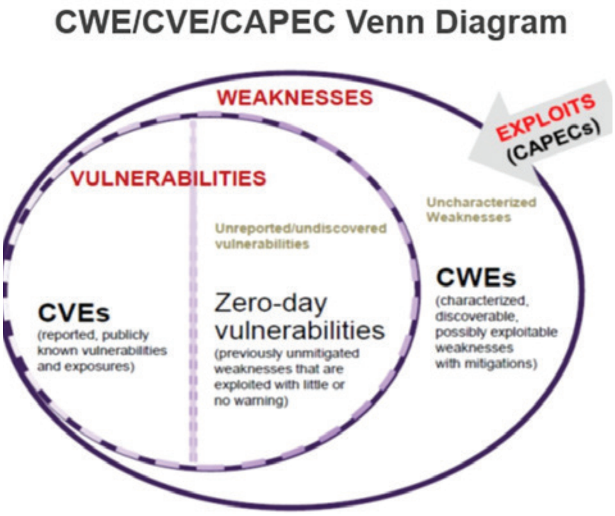
Lecture: "Securing the Software Supply Chain for Naval Warfare Systems", Eric Hill, Technical Account Manager, Synopsys

Mr. Eric Hill's paper that was presented is included in the current Journal issue on page 33.

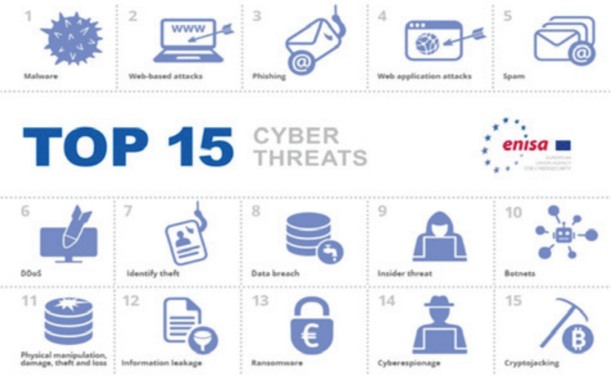
SESSION 3: Assessment, Certification and Training in Maritime Cyber Security

Moderator: Professor Christos Douligeris, Department of Informatics University of Piraeus

Lecture: "CYRENE-EUSCS: Cybersecurity Certification Scheme for Supply Chain Services", Professor Nineta Polemi, University of Piraeus


CWE/CVE/CAPEC Venn Diagram
WEAKNESSES
EXPLOITS (CAPECs)
VULNERABILITIES
Unreported/undiscovered vulnerabilities
Uncharacterized Weaknesses
CWEs (characterized, discoverable, possibly exploitable weaknesses with mitigations)
CVEs (reported, publicly known vulnerabilities and exposures)
Zero-day vulnerabilities (previously unmitigated weaknesses that are exploited with little or no warning)

The research paper that was presented by Professor Polemi is included in the current Journal issue on page 50.



Sources:
ENISA Threat Landscape 2020
ENISA Sectroral thematic threat analysis, 2020

Lecture: First Results on the use of cyber ranges to enhance awareness in the maritime sector, Olivier JACQ, PhD, CTO France Cyber Maritime

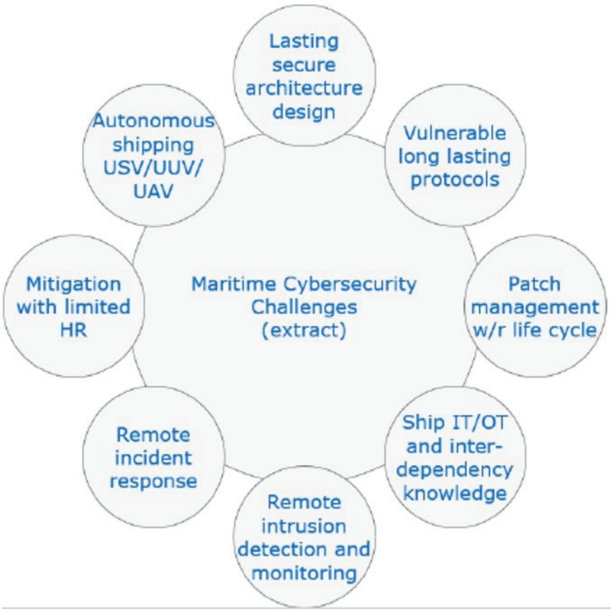
The maritime sector has been involved in an unprecedented digital transformation over the last years: Information Technology (IT) and Operation Technology (OT) systems are developing and interconnecting to achieve a safer and more competitive maritime economy. The attack surface of the sector is widening, leading to potential real-world risks in a sector operating many cyber-physical systems. However, operatives from the maritime sector know that securing a ship or a smart port is not an easy task but a long-haul objective.

Indeed, the sector has some characteristics which can hamper the deployment of traditional technical or organizational mitigation measures on board. To tackle those risks, the French public & private sectors created in November 2020 a non-profit organization, with over 40 members from public & private sectors, France Cyber Maritime, bringing together the maritime community and the cybersecurity sector. France Cyber Maritime's missions are to operate a Maritime Computer Emergency Response Team (M-CERT), to analyze and share specific threats, and to be a focal point for incident coordination as well as to provide tailored services, in full interaction and cooperation with maritime CSOs, CISOs, and public organizations.

France Cyber Maritime backed by the French Secretary of the Sea (SGMer) and the French Information Security Agency (ANSSI). There are three membership boards:

- Public actors (administrations, state agencies and regional/local authorities)
- End users (operators of the maritime and port sectors)
- Qualified providers of cyber security solutions

France Cyber Maritime tries to better prepare operators for maritime cybersecurity challenges through the use of Cyber ranges, where interactive, simulated platforms and representations of networks, systems, tools, and applications are used. Cyber ranges typically provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security-posture testing


Maritime Cybersecurity Challenges (extract)
Lasting secure architecture design
Vulnerable long lasting protocols
Patch management w/r life cycle
Ship IT/OT and inter-dependency knowledge
Remote intrusion detection and monitoring
Remote incident response
Mitigation with limited HR
Autonomous shipping USV/UUV/UAV

Maritime Cybersecurity Challenges

The full operational capability of the organization is planned for 2023

Lecture: "Adaptive and risk-driven security training for the maritime sector", Professor Sotiris Ioannidis, Technical University of Crete

Malware can infiltrate through a wide range of attack points. To mitigate this threat, maritime must provide cyber-range adaptable in modern delivery models with a dedicated cloud-provider.

The THREAT-ARREST platform offers training on:

- Known advanced cyber-attack scenarios
- New cyber-attack scenarios
- The way to make effective and systematic use of different security tools developed to detect and/or respond to cyber-attacks in all the different layers of the implementation stack of cyber systems; and
- Taking different types of actions against cyber-attacks including preparedness, detection and analysis, incident response and post-incident response actions.

In addition, a model-driven solution is developed, called Cyber Threat and Training Preparation (CTTP), that allows the continuous security assurance of the actual operating system, and the dynamic adaptation of the training procedures in the virtual cyber range's environment. As a result, a Smart Shipping Virtual Lab was created for:

- Emulation of the backend infrastructure and captain's on-board PC infrastructure
- Simulation of the smart vessels IoT ecosystem and the on-deck navigation equipment

Three CTTP complete training programs have been developed for the needs of the maritime sector:

- Security awareness – For staff with no or low-security knowledge
- Edge System security administrator – For personnel that require main security knowledge concerning the setting and usage of edge systems in the smart vessel
- Backend security manager – For security and privacy experts

Several training services are offered during the forementioned training programs like:

- Automated security vulnerability analysis
- CTTP modeling of the overall process
- Post-training evaluation
- Continuous security assurance and program adaptation
- Realistic virtual labs
- Multi-layer simulation and modeling
- Incorporation of Serious gaming
- Alignment with professional certification programs

2nd DAY

Keynote Speaker: Mrs Despina Spanou (virtually), Head of Cabinet of the Vice-President of, the European Commission Margaritis Schinas

Good morning to everyone to those who are lucky enough to be in Souda Bay and those who are following online. I am extremely sorry not to be there. As you know, I was supposed to visit the base and together with the European Commission Vice President Schinas, who is in charge of the Security Union. However, due to the recent events linked to the unfortunate earthquake on the island, we needed to allow the authorities the time to deal with that rather than our own visit. And we decided to join you online. But I make a promise we will be with you next time for sure. I thank you for inviting us at this critical time in the area of security and especially in the cyber world. And I am deeply honored to speak to such a distinguished audience, to speak to people who live and breathe security on a daily basis and to whom we all owe a lot. So, I have full recognition and gratitude for the work that you do for all of us, dealing with security from your actual posts.

During the days of the conference, you have already heard a lot about the work of NATO in the area of cybersecurity and especially in the maritime sector. Through my intervention today I will focus on what we do on the European Union side. And of course, on the European Union side, the maritime sector has its own legislation, but at the same time, it is treated as one of the critical infrastructures and therefore is captured by all relevant rules about cybersecurity and security in general.

Now, when it comes to cybersecurity, I think that the last year taught us a lot. First of all, the COVID-19 pandemic showed how vulnerable we can be when we all depend on digital systems to carry out even basic needs in life, schooling, working, so not just the traditional services offered by digital means but also our regular social, and economic life was all carried out by digital systems, relying on digital technology and we saw how vulnerable we are because data breaches, cybercrime, grew exponentially. And we have a lot of reports also from Europol, demonstrating how cybercrime evolved tremendously during the pandemic. Moreover, we had critical ransomware attacks in infrastructures that were unprecedented. I know that yesterday in his speech, Brigadier General Kesopoulos, referred to the Colonial Pipeline example. An example we also quote because it demonstrated if you allow me the big difference between the European Union and the rest of the world. What happened in the United States was unprecedented, a simple ransomware attack, not particularly sophisticated, paralyzed the provision of energy services to half of the territory of the United States, but also had an impact on physical systems. We had queues and fuel stations; we had the lack of provision of energy at all levels of the economy. And this was also because the incident was not necessarily reported early enough for measures to be taken. In Europe, we have already existing rules that would have allowed, first of all, the authorities to be more aware of the incident and possibly to allow for a more coordinated response. And it is likely to see that now in the United States. Last week the cybersecurity authorities in the US have proposed to the Senate to adopt the same type of rules that we have in the European Union. Rules that would require critical infrastructure entities to respect cybersecurity standards, to meet actually the highest cybersecurity standards, to report and notify the authorities of major incidents, and of course, a system of sanctions that would impose fines to those companies that did not comply with these principles.

But why is it important to share information? First of all, because this way the authorities can assist critical entities, but at the same time, it allows to prevent the spreading, of such types of cyberattacks and better situational awareness and coordination between the key actors. In the European Union of 27 independent member states, we rely on the concept of what we call a Security Union, which encompasses cybersecurity. The Security Union was a concept that came into place following the unfortunate terrorist attacks of 2016. When Europe realized that each EU country working alone, which was a traditional method for governments in the area of security, was not going to work in a Europe where there are no borders, where we have a true internal single market, where everything is interconnected. We started in a very step by step approach working together at EU level in creating a genuine security, and in my opinion in a very slow pace. For example, in the area of cybersecurity a key area for our overall security, we introduced rules to protect our critical infrastructures, but also to allow more information and more cooperation at EU level. Today, thanks to the so-called NIS directive, not only we have cybersecurity rules and standards that entities critical for our economy and society have to meet, as I mentioned earlier, we also have European networks bringing together the key cybersecurity actors across the EU. First of all the network of the regulatory authorities dealing with cybersecurity, the so-called NIS cooperation group, where all 27 government authorities gather and make decisions on how to go about the implementation of the existing cybersecurity. Also the CSIRTs Network, the network of the national emergency response teams, the so-called CERTS, that work together whenever we have cyber-attacks that could also have a very large impact across the European Union and across the world.

In July 2020, under the leadership of Vice President Margaritis Schinas, who is responsible for bringing together all security union the various European Commission departments working on security and coordinate and oversee the implementation of the Security Union Strategy, the EU adopted the first ever Security Union strategy. Why is it important to have a Strategy? Because Strategies in the European Union ecosystem are our contract. The contracts upon which we agree on the policies and actions we will take in a specific policy area.

In this Security Union Strategy, we decided something very important. We made clear that we are going to continue working on advancing our cybersecurity preparedness and resilience and reinforcing our legal framework. But we also decided that we are going to stop looking at cybersecurity separately from the rest areas of security. Cybersecurity is about security. After all, there is nothing anymore, especially in critical infrastructures that is not interconnected. Nowadays, any attack becomes automatically a cyber-attack and vice versa. or simply takes the form of a hybrid attack. Thus, we need to break the silos of treating cybersecurity separately. Let me give you an example to illustrate this new approach. We have the existing rules for a high common level of cybersecurity for critical sectors for our economy and society across the EU. This covers the transport sector, it covers energy, banking, health, etc. This is the so-called NIS directive that has been in place since 2018 and fully implemented by all member states of the European Union. We have now proposed the revision of this European directive, stepping up the sanctions part but also enlarging its scope to public administration, but also to additional certain critical industries. For instance, the healthcare industry, we saw that with a pandemic, how vulnerable the pharmaceutical sector can be, the food industry, because again, this is the heart of our society, the provision of food, and it's very important that these large actors also meet high cybersecurity standards. And of course, we reinforced the similarity of rules across the European Union to avoid having weak links, meaning countries where the systems meet lower standards and therefore they become a system of entry for attackers in the European Union. In addition to our legal framework, we also have a playbook at EU level to respond to large cross border cybersecurity incidents in the European Union. We are the first part in the whole world, I would say the first jurisdiction bringing together 27 countries that have a playbook in case of a large-scale cyber incident that allows us to coordinate and respond all together united.

For the full implementation of the Security Union we count on the European Union security ecosystem, which comprises of the EU institutions, Bodies and Agencies, the EU Member States but also the industry and the civil society. I would like today to make a special reference to the European Union Agencies working on security. What are these Agencies? They are structures outside the main European institutions, like the European Commission or the European Parliament, which I am sure you know well. The European Union Agencies are run basically in close cooperation with the EU member states. Their executive boards consist of the European Commission and representatives, usually national authorities, from the EU Member States. And we have a number of such Agencies that specialize in particular areas of cybersecurity too. For example, we have Europol that deals with law enforcement including in the cyber world; its department called EC3 (the European Cybercrime Centre) is a department that has taken down very big cybercrime networks and is fighting against cybercrime. We have also ENISA, the European Union Agency for cybersecurity, which contributes to EU's cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU Institutions, and helps Europe prepare for the cyber challenges of tomorrow. It is a hub of cybersecurity expertise. And we have the recently established European Cybersecurity Competence Centre, which will be responsible for managing the available EU funding in the area of cybersecurity. And this Competence Centre will bring together all the ecosystems across Europe, either private or public that deals with cybersecurity through the funding of research and innovation programs that can lead to improving EU's cybersecurity capabilities.

So we have this security ecosystem that is based on rules and regulations. And now what's next for the EU? It is time that we pass from law to practice. It is time that we pass from theory to operation, from preparedness to resilience and ability to defend against an attack. First of all, we have made a recommendation for the first-ever creation of a joint cyber operational unit, a unit that will bring together experts from all EU governments that can work on the response to large scale incidents. So not just to have a blueprint, that I mentioned earlier, for the theory, but also to have the practical tools for response.

A few days ago, the European Commission's President Ursula von der Leyen announced that we will continue to work and step up our cybersecurity capabilities. And she created and proposed for the first time the concept of cyber defense. It is the first time that in the European Union, we speak of defense, a union of defense, and where the focus of cybersecurity borrows all the elements from defense. This is very important for our cooperation also with NATO that has a lot of experience in this respect. And this is the future of our policymaking. The President also announced a new piece of legislation, the so-called Cyber Resilience Act, an act that will regulate all interconnected systems and products in the European Union with regard to their security.

There is therefore a lot to come in the coming years. This is an area that is only growing in the European ecosystem, again, passing from preparedness, now to operational and to response. And this will certainly be one of the areas where the EU NATO bond will grow even fonder, and it will pave a way for an ever-closer cooperation between the European Commission and NATO systems. And of course, now that we will work on the new EU-NATO joint declaration to be presented soon, we can certainly expect the area of cybersecurity to be central. I hope that this has been useful for the purposes of the conference. Once again, I am really truly sorry not to be there not only because it is much better to be in Crete than in Brussels between us, but also because I would have liked the opportunity to exchange more ideas with you and to borrow between the experience that you have in practice and our intentions to address cybersecurity the best way we can in the European Union. Thank you.

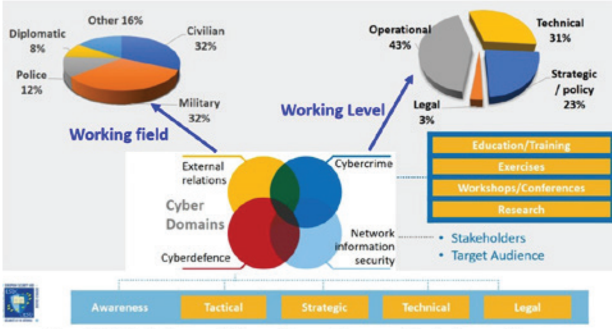
SESSION 4: NATO-EU Cyber Security Collaboration and Initiatives

Moderator: Iosif Progoulakis Department of Shipping, Trade and Transport - University of the Aegean, Chios, Hellas-Greece

Lecture: "European Security and Defense College – Training Cyber Security Professionals", Dr Gregor Schaffrath, Training Manager at the European, Security and Defense College (ESDC)

ESDC Objectives:

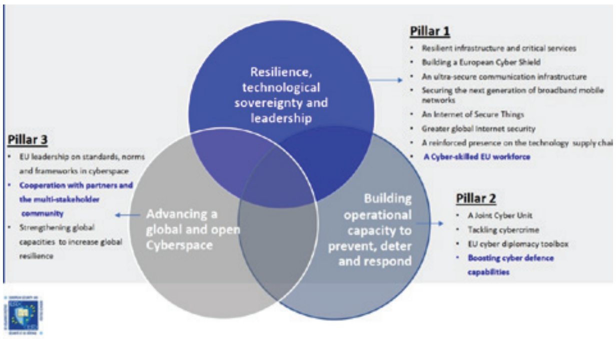
- Enhance common European security defense culture within CSDP
    - Promote a better understanding of CSDP as an essential part of CFSP
    - Provide Union and MS with knowledgeable personnel (EU policies, institutions and procedures in CFSP)
    - Promoting professional relations & contacts
- Support crisis management
    - Training CSDP Missions & Operations personnel
- ESDC Cyber Education, Training, Exercise and Evaluation Platform
    - To address cyber security and defense training among the civilian and military personnel, including for the CSDP requirements for all training levels as identified by he EU Military and Civilian Training Groups.
    - 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 defense workforce.



The ESDC Cyber activities, Ecosystem and Training audience

ESDC's Role in the EU Cybersecurity Strategy Context - 3 pillars:

- Resilience technological sovereignty and leadership
- Building operational capacity to prevent, deter, and respond
- Advancing a global and open cyberspace



Resilience, technological sovereignty and leadership

Pillar 1
- Resilient infrastructure and critical services
- Building a European Cyber Shield
- An ultra-secure communication infrastructure
- Securing the next generation of broadband mobile networks
- An Internet of Secure Things
- Greater global Internet security
- A reinforced presence on the technology supply chai
- A Cyber-skilled EU workforce

Building operational capacity to prevent, deter and respond

Pillar 2
- A Joint Cyber Unit
- Tackling cybercrime
- EU cyber diplomacy toolbox
- Boosting cyber defence capabilities

Advancing a global and open Cyberspace

Pillar 3
- EU leadership on standards, norms and frameworks in cyberspace
- Cooperation with partners and the multi-stakeholder community
- Strengthening global capacities to increase global resilience

ESDC's role in the EU Cybersecurity Strategy context

Lecture: "Data Centric Security (DCS) in Maritime Operations", Mr. Konrad Wrona, Principal Scientist NATO Cyber Security Centre (NCSC)

- Providing efficient data protection and information sharing capability across different security domains, belonging to NATO, the Nations, and specific Communities of Interest (COI), is of paramount importance for effective execution of NATO maritime operations.
- Current information protection practices rely to a large extent on a network-layer mechanism for compartmentalization of information and separation between different COIs. This leads to the segregation of networks into separate network domains and the implementation of perimeter defense at the boundaries of these domains. Such approach is inefficient in respect to the use of CIS resources and usually requires operating separated network environments, which is challenging when considering confined space, limited personnel and a variety of systems that need to be hosted in modern ships.
- Moreover, modern maritime operations require increasingly intensive information sharing with various external systems, both commercial and operated by non-NATO entities.
- Data-centric security rather than focusing on network perimeter defense focuses on securing access to the data itself. It introduces a comprehensive set of security measures, involving both passive and reactive measures, which can be configured to address various data protection and information sharing scenarios relevant to NATO.
- The DCS approach facilitates, at its core, the labeling of data with trusted metadata; access management; automation for sharing information cross-domain; and, latterly, cryptographic object-level protection to deliver enhanced post-release control and data leak protection.
- DCS capability development in the maritime domain has the potential to enhance the collective defense, crisis management activities, cooperative security and maritime security of nations and the Alliance as a whole.
- Vision of DCS – To enhance the ability to share, protect, and control data in accordance with evolving operational requirements strengthening Information superiority of the NATO Enterprise and Alliance Federation – to deliver shareable alliance information protected at source, controlled for life.
- Some of DCS Main principles and goals:

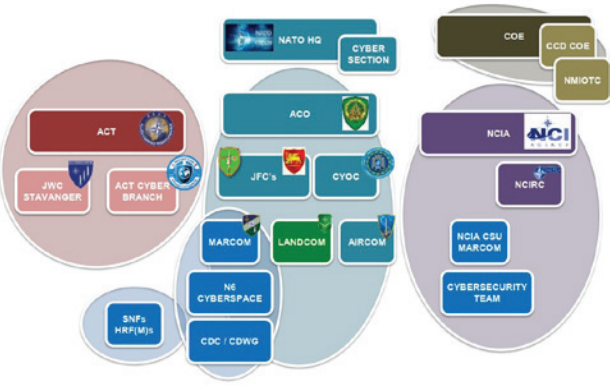
  - Focus on protecting data objects rather than domains
  - Meta-data to facilitate protection
  - Protection includes any combination of CIA Confidentiality, Integrity, and Availability
  - Facilitates various solutions for access management at the object level

Lecture: "Operationalizing the maritime cyberspace: Continuing the conversation", Cpt Antonie Colombier FRA (N), ACOS MARCOM/N6/Cyberspace

NATO Cyber Evolution:

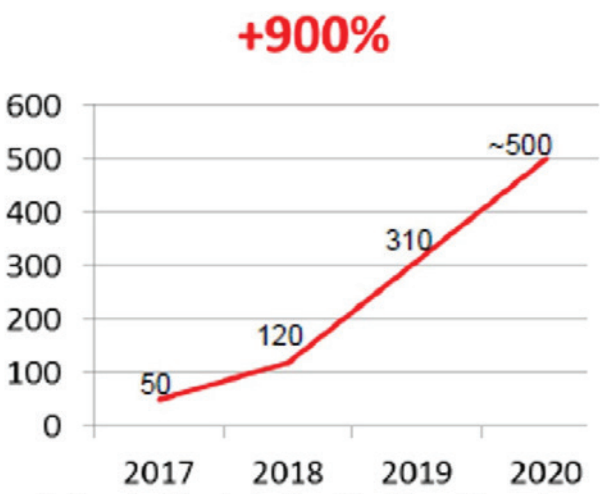
- 2014 in Wales Enhancing
- 2016 in Warsaw Adapting
- 2018 in Brussels Operating
- 2019-2020 in OPERATIONALIZING

- MARCOM's responsibilities
  - Ensuring that sea lines of communication between Europe and North America remain free and secure
  - Improving the movement of troops and equipment within Europe
  - Reinforcing logistics elements across the NCS in Europe
  - Strengthening Cyber Defenses and integrating cyber capabilities into NATO planning and operations



The NATO Cyber Community

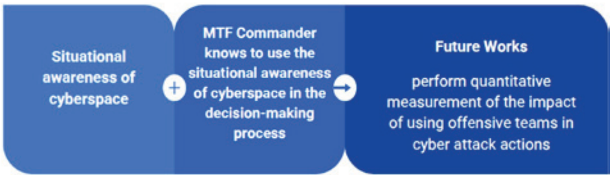
- Increased of Cyber Incidents in the Maritime Domain is 900%



Cyber Incidents in the Maritime Domain

Lecture: "Situational awareness of cyberspace on maritime military operations", Cdr Salvador Mota, BRA (N), Head of Cyber Defense Division, Brazilian Navy, Lt Françoa Taffarel BRA (N), Cyber Security Specialist, Brazilian Navy

The relevant paper that was presented is included in the current Journal issue on page 57.



Situational awareness of cyberspace + MTF Commander knows to use the situational awareness of cyberspace in the decision-making process → Future Works perform quantitative measurement of the impact of using offensive teams in cyber attack actions

SESSION 5: Secure Maritime Value and Supply Chains, Infrastructures & Services

Moderator: Professor Nikitas Nikitakos, University of the Aegean

Lecture: "Machine Learning-based Attacks on Safe Container Ship Loading", Dr Barton P. Miller, Professor in Computer Sciences, NSF Cybersecurity Center of Excellence, University of Wisconsin-Madison, **Dr Elisa Heymann**, Senior Scientist – Associate Professor, NSF Cybersecurity Center of Excellence, University of Wisconsin-Madison

The mission during research on Machine Learning-based Attacks on Safe Container Ship Loading is to:

- Anticipate threats to maritime cybersecurity
- Demonstrate the feasibility of these threats
- Defend against these strategies

The main research accomplishments so far are:

- 7 identified serious security vulnerabilities
- Designed remediations for these vulnerabilities
- An in-depth class in security software designed at Total Soft Bank

The major security problems:

- An attacker can manipulate the database holding the manifest container weight.
- The attack is limited by errors detected at the weighbridge and by some scales
- Can an attacker falsify the weights such that a ship would be loaded dangerously off balance?

The approach used to solve the identified security problems:

- Use adversarial machine learning to generate false weights for the container load that would result in an off-balance ship.
- To counter such attacks, is to develop detection strategies and more robust load planning algorithms.

Lecture: "Cybersecurity challenges in DDIL", Eduardo Bolas, Principal Scientist, NCI Agency,

Sophisticated Maritime Situation Awareness (MSA) systems extensively depend on data-savvy Internet Protocol (IP) based services. Obviously, this presumes the existence of reliant, stable and high-bandwidth communication systems, such as SATCOM, which cannot be taken for granted - vide the example of 2007, when China shot down a weather satellite. As a result, MSA communities have increased interest in alternative technologies for scenarios where SATCOM is unavailable – the so-called Denied, Degraded, Intermittent or Limited (DDIL) environments. An adaptation of services is required to manage throughput and cope with delay and jitter challenges, but maintaining support to critical business processes and information transfer. Such adaptations aim to improve data transfer efficiency, while not undermining cyber defense.

Military systems rely on high-grade encryption, which provides implicit security features that save bandwidth, but, unfortunately, are not adequate for ubiquitous civil-military networks. Moreover, modern cyber threats force the deployment of defense measures that contribute to inefficiencies and self-inflicted operational impairments that affect the overall systems' performance. It is important to invest in smart approaches to operate in DDIL environments: not only at the lower layers of OSI model, but also at the application, business processes, and knowledge management levels.

An analysis of cybersecurity challenges in DDIL environments was proposed, focusing on approaches to optimize MSA exchanges and maximize their effectiveness. The discussion included aspects of information diversity, independency, and granularity to optimize security processes and network efficiency.

Lecture: AI4HEALTHSEC – A Dynamic and

Self-Organized Artificial Swarm Intelligence Solution for Security and Privacy Threats in Healthcare ICT Infrastructures, Eleni Maria Kalogeraki PhDc, Focal Point, Dr. Spyridon Papastergiou, Focal Point

Are healthcare services important in the maritime sector?
Healthcare services on board:

- Highly Specialist diagnostics engaging new developments of science
- Advanced medical devices and equipment
- Comprehensive medical management system
- Highly competent doctors
- Medical training
- Medical remote assistance
- Effective treatment
- Follow best practices to address COVID-19 challenges (e.g. IMO webinars)

Nowadays there are daily headlines on cyber-attacks in Healthcare and Maritime sector.

AI4HEALTHSEC proposes a state-of-the-art solution that:

- improves the detection and analysis of cyber-attacks and threats on HCIIs and increases the knowledge on the current cyber security and privacy risks;
- builds risk awareness, within the digital Healthcare ecosystem and among the involved Health operators, to enhance their insight into their Healthcare ICT infrastructures and provides them with the capability to react in case of security and privacy breaches; And
- fosters the exchange of reliable and trusted incident-related information among ICT systems and entities composing the HCIIs without revealing sensitive corporate details

A main AI4HEALTHSEC solution outcome is the Dynamic Situational Awareness Framework (DSAF) that helps the operators to:

- thoroughly assess the vulnerabilities of all cyber assets;
- evaluate the probability of cyber-attacks;
- identify the relationships between indicators of compromise, threats, and adversaries
- estimate the cascading effects of attacks in the **Interdependent HCIIs** and identify how these attacks propagate across the **HCSCS**;
- provide technical assistance and guidance on investigating and handling complex, interrelated cyber security incidents and data breaches and extracting all relevant information; and
- combine and analyze all security incident-related information in an effective and accurate manner.

SESSION 6: Innovative Research in Maritime Cyber Security and Cyber Defense

Moderator: Mr Emmanouil Christofis,SHAPE J6 Cyberspace – Plans and Policy

Lecture: "Multi-Purpose Cyber Environment for Maritime Sector", Gabor Visky, Researcher, NATO Cooperative Cyber Defense Centre of Excellence (CCDCOE)

1.5 tons of goods are transported for every people around the globe by ship in a year. Recent cyber security incidents like A.P. Møller-Maersk NotPetya malware in June 2017, China Ocean Shipping Company (COSCO) in July 2018, and Norsk Hydro in March 2019 proved that the maritime sector's cyber security needs attention.
Cybersecurity Aspect

- 7 Types of Cyber Security to consider: Cloud Security, Network Security, Disaster Recovery, Application Security, Operational Security, Information or Data Security, and Business Continuity.
- People
- Technology
- Regulatory Framework

The People aspect of Cyber Security:

- Maritime becomes ICT expertise dependent
- Education focuses on operations
- Cyber education – usually out of the curriculum
- Special environment needed for industry-specific cyber education

The Technology aspect of Cyber Security:

- IT and OT needs a different approach
- Legacy devices (not meant to be cyber secure)
- Mixed technology (Compatibility, Partially renewed systems)
- Vendor-specific devices/protocol
- Confidentiality, Integrity, Availability of data and services
- Safety, Reliability, Security of processes

A Multi-Purpose Cyber Environment for Maritime Sector was built which includes a Transas NT Pro 5000 Navigational Simulator with additional cyber security research specific components that can be used as vulnerability

Multi-Purpose Cyber Environment for Maritime Sector testing environment for research, Cyber security experts' education, Maritime enterprise experts' education and Cyber security exercises.

Lecture: "Secure Software Development Techniques for mixed-criticality systems: Enhancing current system engineering frameworks for cyber operations",
Dr. Emmanouil Serrelis, Information Security Department Manager, Intrasoft International

Mixed Critically Systems include a combination of hardware and software that serve several purposes of different criticalities, such as power, safety or navigation systems.
Needs for Mixed-Criticality Systems:

- Non safety critical systems
  - Adaptability
  - Dynamic system structures
- Safety critical systems
  - Certification standards
  - Static configurations

Typical Software Development Lifecycles

- Waterfall, Agile, DevOPS

Challenges while applying Secure Software Development Lifecycle (SSDLC) for mixed critical system:

- Ensure each component security requirements
- Do not mix resources and requirements of components of different critically
- Keep total cost of development and service provision to a minimum
- Minimize technical debt

SSDLC key points are:

- A SSDLC maturity growth journey has direction but no need for a "finish line"
- SSDLC journey would benefit from a prescriptive approach (e.g. OWASP SAMM)
- Mixed criticality systems, platforms and environments are to be identified and managed within the early stages of the development lifecycle
- Build a standardized Secure SW development toolkit for applicable for any development process
- When choosing the right method/tool:
  - Take into account the risk appetite for each individual subsystem
  - Introduce cost-effective security controls and
  - Go for trusted, recently supported solutions and methods
- Request SSDLC assurance from your development vendors

Lecture: "Initial Results from the CyberSec4Europe Maritime Cybersecurity Demonstrator", Dr Christos Douligeris, Professor Department of Informatics, University of Piraeus, **Mr Christos Grigoriadis**, PhD student Department of Informatics, University of Piraeus

The CyberSec4Europe Maritime Cybersecurity Demonstrator project has identified 7 key demonstration cases in different domains addressing prominent research areas in the public and private sectors.

- Ecommerce with security consideration
- Security and integrity of the supply chain
- Privacy-presenting identity management
- Incident reporting
- Maritime transport security
- Secure medial data exchange
- Secure smart cities

Security Services for Maritime Transport Infrastructures:

- Service 1: Threat Modeling & Risk Analysis for the Maritime Transport Services
- Service 2: Maritime System Software Hardening
- Service 3: Secure Maritime Communications
- Service 4: Trust Infrastructure for Secure Maritime Communication

Maritime Transport – Roadmap and Research Goals

- Existing Taxonomies were researched and adjusted in order to map:
  - Maritime Threat Agents
  - Maritime Cybersecurity Threats
  - Maritime Cybersecurity Threat Impacts
- Maritime security services were developed:
  - To secure maritime infrastructures against existing threats
  - To predict uprising cybersecurity threats
  - To enhance communication security in the maritime sector
- Demonstrators were designed based on the services and will be presented in the context of:
  - A web-based risk assessment tool
  - A software recompilation/ hardening tool
  - A PKI solution along with VHF Data Exchange System (VDES) radio

Conclusion and Future Goals:

- Identification of threats and threat agents for the maritime sector
- Extension, integration, and initial validation of targeted security services such as risk assessment, system hardening, PKI, and secure maritime communications
- Next steps:
  - Integration of selected security services

in an adaptive security model, to provide real-time and (semi) autonomous risk assessment and mitigation of threats.

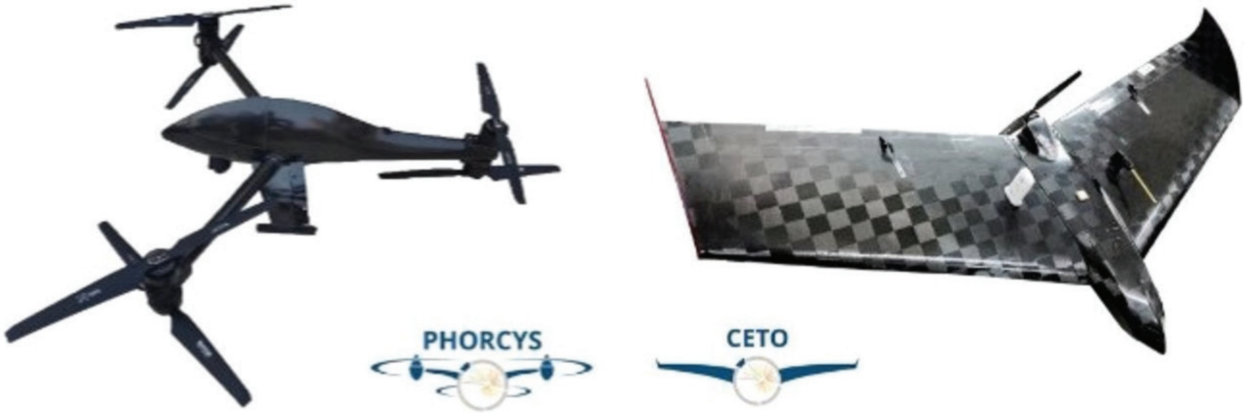
- Enrich maritime RA/RM tool (MITIGATE) with the software hardening techniques as part of the mitigation controls and policies for various critical maritime components.
- Extend the maritime PKI tool (CySiMS) into a VDES-ready solution, applicable to real maritime communication systems.

CLOSING REMARKS

With over 20 lectures from established cybersecurity professionals, this conference covered every critical maritime cybersecurity area. From military to non-military operations, we discussed the modernization progression to improve maritime cybersecurity. As discussed in previous cybersecurity conferences, the solution to effective and efficient maritime cybersecurity is a synergy of the government, military, legal, technology, intelligence, and academia sectors. This NATO maritime synergy will develop into a global interactive collaboration to ensure maritime security at the tactical, operation, and strategic levels.

As a young captain in the U.S. Army Reserves, Lieutenant Colonel Brown was called up to work at the Pentagon on the Crisis Action Team after 9/11. For her outstanding efforts, she received Army Staff Identification Badge and Global War on Terrorism Service Medal. As a major, Wendi Brown completed two consecutive combat tours in Afghanistan, which lasted for 18 long months. For her exceptional efforts in combat, she received the Bronze Star Medal, Defense Meritorious Service Medal, Non-Article 5 NATO Medal, Global War on Terrorism Expeditionary Medal, Afghanistan Campaign Medal, and NATO Afghanistan Service Medal (ISAF-International Security Assistance Force). As a lieutenant colonel, she worked at the U.S. European Command in Germany, joint operations environment, to monitor terrorist activities for 51 countries and territories to ensure stability throughout NATO and European Union. Also, Lieutenant Colonel Brown, completed logistical support to a global NATO communication network contingency operation to ensure computer and internet interoperability among NATO countries in case of terrorist or enemy network attacks against critical infrastructure. In the following assignment, Lieutenant Colonel Wendi Brown worked at the U.S. Africa Command, another joint operations environment, to monitor terrorist activities on the African continent. While working full-time, Lieutenant Colonel Brown earned her first Master of Science in Cybersecurity, graduating summa cum laude; an educational curriculum coordinated and endorsed by the U.S. Department of Defense. Four years later, she earned her second Master of Science in Cybersecurity. The graduate degree was Master of Science in Cybersecurity with Specialization in Cyber Intelligence, graduating summa cum laude; an educational curriculum coordinated and endorsed by the U.S. National Security Agency and U.S. Homeland Defense.

ARSx2
A marine area surveillance system using UAS, assisting anti-piracy measures and contributing to hostages and/or vessels recovery



by Christodoulou E., Charvalis G.*, Melas G.*, Poulakis O.*, Papakonstantinou A.**, Moustakas A.**, Doukari M.**, Moutzouris I.**, Topouzelis K. ***

**A.S. Prote Maritime Ltd personnel **Marine Remote Sensing Group personnel*

Abstract

The innovative project ARSx2 deals with the development of a maritime surveillance system, consisting of two UAVs, for the prevention of piracy or other illegal activities as well as the monitoring of pirate incidents in progress, and search and rescue cases at sea. The first UAV, called "Phorcys", is a VTOL hexacopter on a Y6 configuration. Equipped with a powerful hybrid EO/IR stabilized camera with object tracking capabilities, humans and items such as guns, canisters, etc. can be identified from a safe distance. The second small, flexible and easy to use by non-specialists fixed-wing UAV, called "Ceto" is used in emergency cases as a "rescue beacon". It is deployed when a vessel is already or will be occupied by pirates, while real-time position, images or video are transmitted to the patrolling authorities and rescue organizations.

In this paper, the project's followed methodology will be presented. The approach consists of the definition of operational and technical specifications, design and manufacture of the UAVs. The process of capture and analysis of data will be also presented, providing real-time high precision intelligence to operators and rescue authorities, indicating the interoperability, robustness and reliability of our aerial system. Additional system's uses such as ship inspection, mail transport, lighting of dark areas, rescuing people at sea, patrolling sea and inland areas etc., of the UAVs will be also referenced. Aspects that concerned the research team during the project implementation are presented in the conclusions with useful insights on piracy. Future concepts, directions and improvements of the ARSx2 system that have been explored, are introduced in the last chapter of this paper.

The ARSx2 project

The whole project is Co-financed by the European Regional Development Fund of the European Union and Greek national funds through the Operational Program Competitiveness, Entrepreneurship and Innovation, under the call RESEARCH - CREATE - INNOVATE (project code: T1EDK-04993) under the name: ARSx2 (AeRial System and Anti-piRacy System) Marine area surveillance system, using Unmanned Aircraft Systems (UAS) to avoid and prevent merchant ships from piracy. Main objective of the call "RESEARCH - CREATE - INNOVATE" is the connection of innovative business with research and enhancing of competitiveness, productivity and accessibility of hellenic companies in international market. Hellenic businesses join forces with R&D partners aiming to create competitive applications and services, able to cover the modern demands of the international market.

Our company's, partner for this project is Marine Remote Sensing Group (MRSG) of the Department of Oceanography and Marine Life Sciences of the University of the Aegean. Relevant subcontractors are: Ev Aetheria Ltd, B.I.MA S.A., Ucandrone PC and Fible Technologies PC. After successful laboratory tests, project is in the process of field testing of the two UAVs in land and marine environment.

Project's reasoning

Two key factors drove our involvement in this project. Initially, the previous experience of the company owners in Hellenic Navy, cultural informatics, University education field, R&D of new technologies, and in the field of Private Maritime Security.

Second factor is that all previous attempts regarding UAV utilization against piracy either remained only in a theoretical field, or were costly, large-scale solutions deploying UAVs (HALE and MALE type) purely of military nature, or were totally failed attempts based on the wrong assumption that "anyone can be a drone pilot/operator"!

All the above-mentioned reasons convinced us that we should be directed at developing a system which would be operated in situ, where the danger occurs, that is, on the ship that could be threatened by pirates! The innovative project ARSx2 deals with the development of a maritime surveillance system, consisting of two UAVs, for the prevention of piracy or other illegal activities as well as the monitoring of pirate incidents in progress, and search and rescue cases at sea.

Methodology

The methodological approach of the project follows six main stages. In the first one the existing functional framework is defined. This stage includes studies of piracy's operational environment, tactical counter piracy measures, UAV legal framework and maritime and aerospace communications study. In the second stage the analysis of operational and technical specifications take place. This leads to a better technical specifications definition followed by a certification step. Stages three and four correspond to Phase A and Phase B respectively. Phase A consists of the design, construction, parameterization and laboratory testing of the system. Phase B consists of the prototypes' optimization and field testing. At the end of each phase there is a certification step. Lastly, after composing operation and maintenance manuals, complementary actions such as commercialization study, alternative uses study, and various publicity actions take place. Technology Readiness Levels (TRLs) have been used as a method for defining the structure of the methodology stages, the general content, as well as a means to estimate the maturity of our technology from a concept idea to completion.

Operational specifications of the two UAVs are analyzed after taking into consideration the studies of the existing functional framework. Specifications are set regarding the system's general capabilities, environment restrictions, legal restrictions, versatility, interoperability, transportation and deployment by novice users. Technical specifications are defined after the operational specifications have been discussed through the research team, engineer team, and experts with operational experience. Defined technical specifications are then simulated in a calculation tool (https://www.ecalc.ch/xcoptercalc.php) providing essential feedback and a first indication of the UAV capabilities. This process leads one step closer to manufacturing.

Design and manufacture

The first step is to create CAD models of the UAVs fuselage and internal compartments. A CAD virtual environment provide tools that allow to test various materials and setups, experimenting prior to manufacturing process. The manufacturing materials selected are lightweight, durable, UV resistant, composite materials approved for aeronautical use, including among others, high quality carbon fibre (type 442 carbon fabric[1]) sheets and tubes, and Nomex Aramid Honeycomb cells (Can, 2020).

The design of the Phorcys UAV as a hexacopter in a Y6 configuration (Figure 1) has proven beneficial when confronting high wind velocities due to its reduced exposed surface compared to quadcopters (Chapman, 2020). This effect is enhanced by its aerodynamic shape and the fact that the motors are coaxial, providing overall, an increase of the power output with reduced drag coefficients.

Ceto's most important aspect is flight time. Its design characteristics revolve around that aspect. A lightweight, small size, fixed wing and low drag design offers the required lift to maximize its operational flight time (Fahlstrom,2012). In order to shape the composite materials we created molds. The technique used to shape the composite materials is the infused resin vacuum molding, in molds that have been created by Computerized Numerical Control (CNC) machines (Figure 1). The technique mentioned, results in a high quality and strong material bonding, providing a compact, robust and lightweight fuselage[2] (Zhang,2017) for both UAVs.

High quality components with specifications that comply with the defined technical specifications are selected

[1] http://www.ezentrumbilder.de/rg/pdf/td_en_ECC_Style442_E.pdf

[2] https://www.fibreglast.com/product/vacuum-infusion-Guide/Learning_Center

from various suppliers for the assembly. These components include among others, motors, propellers, electronic speed controllers, autopilot, GPS, companion computer, payload sensors, actuators, telemetry modules and controllers. The selected autopilot[3] encloses tree redundant IMUs, a failsafe co-processor, redundant power supply with automatic failover and the necessary serial ports to accommodate interconnections between other devices such as an onboard companion computer. Parameterization of the UAV's autopilot is controlled under the open source mission planner firmware[4], including sensor calibration, flight parameters calibration and failsafe adjustments.

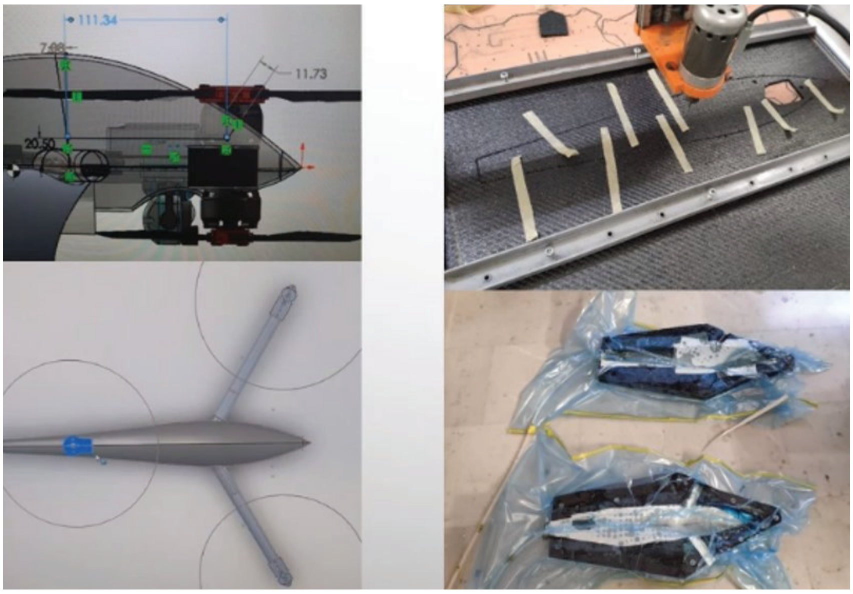


Figure 1: CAD-CAM designs (Left), CNC cutting process (Up right), infused resin vacuum molding (Down right)

Capture and analysis of data

The hybrid sensor allows day and night surveillance over long distances. According to Johnsons DRI criteria (Chevalier,2016), the visible sensor surpasses the detection range of 5 kilometers, the recognition range of 3 kilometers and identification range of 1,5 kilometers. The captured data are provided with a 640 x 480 thermal resolution (LWIR uncooled 8-12μm) while the powerful high definition optical sensor provide up to x40 zoom. The data processing system provides real-time EO/IR object tracking, geo location, video compression, IP encapsulation and video recording capabilities. The object tracking is 'locking' the camera to track a subject selected by the user within the camera's range. Accordingly, the 'locked' subject of interest always remains within the display (Figure 2).

Additional uses

ARSx2 UAVs can be used for assisting supplementary maritime security tasks onboard a merchant vessel, such as inspection of vessel's exterior fortification (hardening), recording of PCASP's exterior tactical drills, patrolling in occasions, eminent for a possible danger (robbers, stowaways etc.), collecting of important maritime security information (for example information regarding illegal, unreported, or unregulated activities) and its transmission to relevant authorities, other nearby vessels etc. Furthermore, assisting in tasks that take place onboard a merchant vessel other than the ones of maritime security, such as inspection of exterior parts and/or possible damages of a vessel as well as crew exterior routine tasks and drills, provision of an aerial light source, assistance in "abandon ship", "search and rescue" or "man at sea" situations, assistance in the geographical identification of sea pollution and/or oil slicks, collection of important information of different aspect and its transmission to relevant authorities etc.

Conclusions

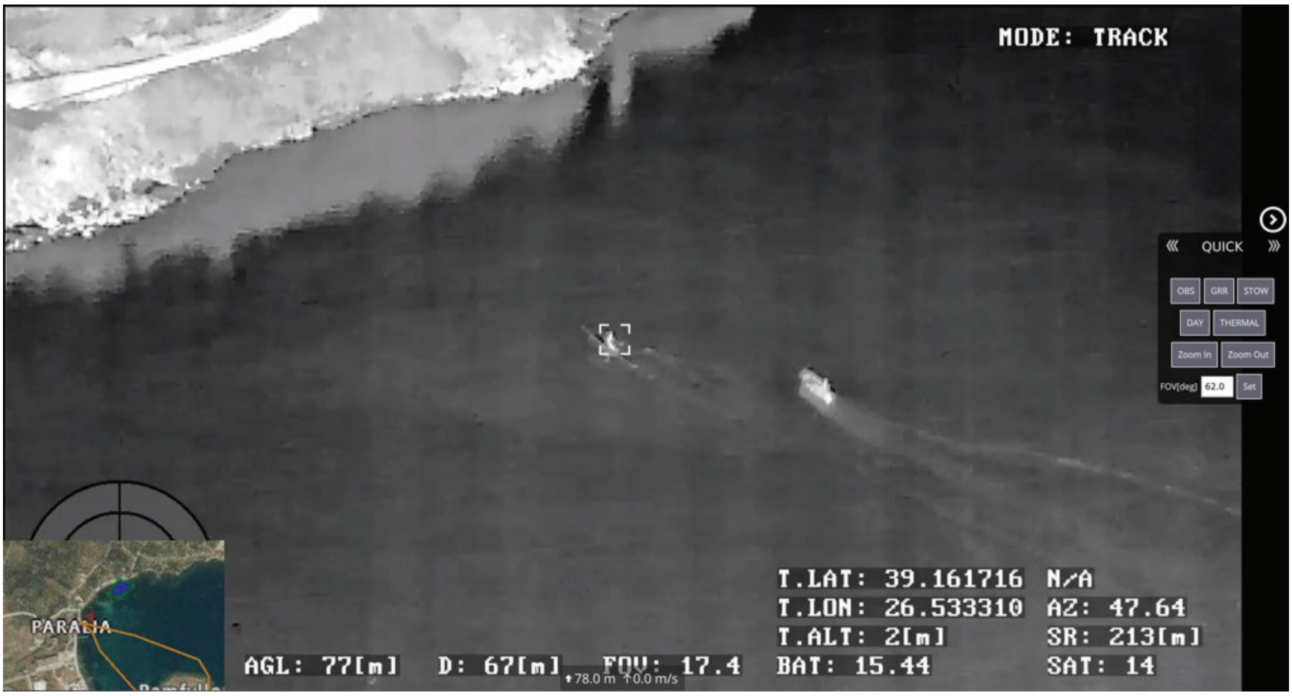
The significant increase in piracy and vessel-boarding incidents pose an economic and safety threat with social aspect (Møller, Bjørn, 2008). The discontinuation of international counter-piracy operations create a global concern on the future of piracy. Policy makers have been traditionally unable to effectively deal with the problem as potential national disagreements and conflict of interests are perplexing the situation. A new counter-piracy legislation is a difficult and time consuming task. In the meantime, new security issues arise at an ever-increasing rate.

ARSx2 system can provide increased "in situ" maritime surveillance ability, early warning of potential pirate threats, capturing, processing and analysis of data, real-time high precision intelligence to control stations and rescue authorities, remote operation with mission management and autonomous commands, fast, safe and robust data transmission, assistance to search and rescue operations, monitoring of a pirate attack or hostage situation, recognition and monitoring of marine hazards, alleviation of risk of injury or death of humans during or after a pirate attack.

Indirect advantages from the use of ARSx2 system include reduced insurance costs for crews, ships, and freights, reduced economic loss of

[3] HEX The Cube Orange - with ADS-B Carrier Board

[4] https://ardupilot.org/planner/



MODE: TRACK

T.LAT: 39.161716 N/A
T.LON: 26.533310 AZ: 47.64
T.ALT: 2[m] SR: 213[m]
AGL: 77[m] D: 67[m] FOV: 17.4 BAT: 15.44 SAT: 14

↑78.0 m ↑0.0 m/s

FOV[deg] 62.0

Figure 2: User interface of the ARSx2 system. The thermal channel is active while a subject is 'locked' and tracked during field tests. Information about the subject are calculated continuously.

countries adjacent to high-risk areas, optimization of ship routes, fuel saving and ship rental time saving. All of the above promote the security of the movement of humans and goods and assist PMSCs, local and international organizations and authorities, P&I clubs (Protection and Indemnity) and shipping companies to better decision making.

During our involvement in the ARSx2 project we stumbled upon many obstacles. We identified a lack of adequate companies specialized in constructing UAS and a rapid evolution of the UAS' technology. A major obstacle is the undefined legal boundaries from the use of UAS against piracy, in national and international levels. Despite the obstacles, we made an attempt to partially substitute and improve established procedures from the market based on PCASPs. The new technologies drastically change the rules and habits of industries in many economical, safety and efficiency aspects. They provide new and more effective capabilities on existing means in order to avoid and/or prepare and/or report potential piracy threats. In principle, this technology is a tool for enhancement of security, cooperation and coordination of maritime actors to uphold freedom of navigation.

Future work

Future systems optimization that is already conceptualized and researched is the use of Artificial Intelligence for direct real-time identification of targets, people, and objects on the Phorcys. Such a capability can accurately and immediately assess the presence of a threat and provide an accurate early warning. Regarding Ceto, vertical take-off and landing (VTOL) capability has already been examined and it is at its early stages of manufacturing, since it was considered essential capability in order to safely retrieve the UAV after an emergency situation. Additionally, we examine to prolong its flying time by embedding solar panels and/or develop a system consisting of RF beacons and nets in order to achieve the safe return and retrieval of at its base. Last but not least, additional automated commands for use against piracy or other surveillance tasks have already being developed and programmed to be released in future ARSx2 software updates.

References

- Andrew Chapman. (2020). Types of Drones: Multi-Rotor vs Fixed-Wing vs Single Rotor vs Hybrid VTOL - AUAV. AUAV. https://www.auav.com.au/articles/drone-types/
- Can, W. E., You, H., The, S., & Light, K. I. T. (2020). HERO ROHACELL ® HERO. April.
- Chevalier, P. A. J. G. (2016) "On the specification of the DRI requirements for a standard NATO target" https://www.researchgate.net/publication/297497162_On_the_specification_of_the_DRI_requirements_for_a_standard_NATO_target
- Fahlstrom, P. G., & Gleason, T. J. (2012). Introduction to UAV Systems: Fourth Edition. In Introduction to UAV Systems: Fourth Edition. https://doi.org/10.1002/9781118396780
- Lloyd, J. M. (2013). Thermal imaging systems. In Springer Science & Business Media. https://doi.org/10.1016/0963-8695(94)90752-8
- Møller, Bjørn (2008) "Piracy, Maritime Terrorism and Naval Strategy". Copenhagen: Danish Institute for International Studies
Zhang, W., Lv, S., & Guan, X. (2017). Application of lightweight materials in structure concept design of large-scale solar energy unmanned aerial vehicle. IOP Conference Series: Materials Science and Engineering, 242(1). https://doi.org/10.1088/1757-899X/242/1/012009
- BIMCO, ICS, IGP&I Clubs, INTERTANKO and OCIMF (June 2018) "BMP5_Best Management Practices to Deter Piracy and Enhance maritime Security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea", Witherby Publishing Group Ltd, ISBN 9781856095051
- CMF (2017) "GUIDANCE ON MARITIME SECURITY TRANSIT CORRIDOR" https://combinedmaritimeforces.com/2017/09/06/guidance-on-maritime-security-transit-corridor/
- EU, COUNCIL DECISION (CFSP) 2020/2188 of 22 December 2020
https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32020D2188
- IMO (2009) "REPORTS ON ACTS OF PIRACY AND ARMED ROBBERY AGAINST SHIPS". MSC.4/Circ.133, 19 March 2009
- IMO (2019) "REPORTS ON ACTS OF PIRACY AND ARMED ROBBERY AGAINST SHIPS Annual Report – 2018". MSC.4/Circ.263, 1 April 2019
- IMO (2012) "INTERIM GUIDANCE TO PRIVATE MARITIME SECURITY COMPANIES PROVIDING PRIVATELY CONTRACTED ARMED SECURITY PERSONNEL ON BOARD SHIPS IN THE HIGH RISK AREA". MSC.1/Circ.1443 25 May 2012
- IMO (2019) "Djibouti Code of Conduct".
http://www.imo.org/en/OurWork/Security/PIU/Pages/DCoC.aspx
- International Chamber of Shipping (2019) Shipping and World Trade
https://web.archive.org/web/20121209034126/http://www.ics-shipping.org/shippingfacts/worldtrade/number-of-ships.php
- Lloyd, J. M. (1975) "Thermal Imaging Systems. In Thermal Imaging Systems". Springer US https://doi.org/10.1007/978-1-4899-1182-7
- Lloyd, J. M. (2013) "Thermal imaging systems. In Springer Science & Business Media". https://doi.org/10.1016/0963-8695(94)90752-8
- LLOYD'S, Joint War Committee, "Committee Terms of Reference". APPENDIX 1 – LMA COMPETITION COMPLIANCE GUIDELINE
- Reuters (2017) "Somali pirates hijack first commercial ship since 2012".
https://www.dhakatribune.com/world/2017/03/14/somali-pirates-hijack-first-commercial-ship-since-2012
- UN "Convention on the Law of the Sea" 10 December 1982
https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf

EVANGELOS CHRISTODOULOU
He is retired officer of the Hellenic War Navy, specialized in submarines. Since 2012, is businesswise active in maritime security and the use of new digital and disruptive technologies in the merchant shipping market primarily, but not exclusively. He has graduated from the Hellenic Naval Academy and holds an MSc in Virtual Reality. His professional past is summarized in: a) being Head of the 3D Graphics Department of the Foundation of the Hellenic World (FHW), for more than 13 years, b) till the end of 2016, for 13 years, served as Adjacent Professor at the University of the Aegean in the cognitive subjects of "3D Graphics" and "Virtual Reality" and c) since 1995, as freelancer, created numerous digital productions for the Entertainment Industry, Museums and Archaeological Sites in Greece and abroad, awarded and distinguished in international festivals and conferences.

Artificial Intelligence and Cyber Security in 2030 Possible implications for the Maritime Sector

by Dr. Swantje Westpfahl and Tim Dalhöfer
Institute for Security and Safety
at the Brandenburg University of Applied Sciences, Germany

Abstract

This paper provides an introduction and an outlook into the use of Artificial Intelligence in the maritime sector and possible implications with regards to cyber security risks. We will first present an overview on maritime AI applications which are currently under development or already being deployed and Intelligent Decision Support Systems (IDSS). We will show how these developments can influence security in the maritime domain. Further, we will elaborate on risks associated with the use of AI both for the general use in maritime applications as well as for IDSS. We will specifically pinpoint risks which arise from cyber threats but also from human interaction with these systems, i.e. the matter of trust. We will show that in order to account for security in the maritime use of new technology, technical as well as ethical considerations have to be taken into account in understanding how cyber threats on maritime AI applications can affect maritime security. We shall then propose some recommendations for the development and deployment of AI and IDSS applications in the maritime sector with regards to cyber security as well as the human factor.
Content

Introduction

Artificial Intelligence (AI) is well on its way to become a defining factor on warfare in the coming years and decades. Great Powers such as the U.S. and China are heavily investing in AI research and development and prototype testing. The maritime domain has been no exception in this. However, the civilian maritime sector seems to be progressing fast in this regard[1], much faster than the military sector which of course is subjected to various bureaucratic, organizational, technological and also ethical constraints. So far, AI hasn't found its way into actually deployed applications. But this can very well change over the course of the decade.

At the same time, just as it is the case with conventional on-shore digital systems, increased digitalization brings with it an increased necessity for cyber security, to maintain system operability and mission success, as well as prevent unacceptable incidents. In addition to conventional computer systems, securing Artificial Intelligence systems poses different and complex challenges to cyber security. This presentation aims to establish a near-future outlook on the expected applications of AI in the maritime domain, as well as pointing out the cyber security challenges that come along with these

[1] Raveling, Jann (2021): Artificial intelligence within the maritime industry. Available from https://www.wfb-bremen.de/en/page/bremen-invest/artificial-intelligence-within-maritime-industry#wfb-ai-ships

applications, both technically and ethically.

Maritime AI Applications

The idea of using AI to make operations more efficient has already found its way into the maritime sector some time ago, with many military stakeholders currently developing and testing new systems in the face of intense digital technology competition. The applications below describe noteworthy maritime AI applications which hold the potential the fundamentally change maritime security in the coming years. While some of the mentioned applications are already being tested by some stakeholders, their presumable deployment in the near future will be crucial to a new technological landscape in the field. Other applications mentioned are still at early development levels.

Application for Maritime Situational Awareness

In recent naval history, the sheer size of the seas has meant that maritime situational awareness has traditionally been the pivot on which successful naval operations have depended. Being aware of the adversary's movements on the vastness of the world's oceans, the positions and movements of own assets as well as those of allies has always presented a challenge for naval actors. Still, in the context of modern maritime security operations it constitutes a major factor for the successful completion of operations. Reducing the opacity of the ocean environment and increasing situational awareness through the creation of an 'observable ocean' would revolutionize the way maritime security is being done today and has been done for decades, according to Williamson (2020)[2].

AI-supported systems offer a particular promising potential for increased intelligence, surveillance and reconnaissance (ISR) capability by opening up and monitoring vast maritime areas without the direct and constant need for human engagement. Leveraging AI to make sense of the enormous amount of data generated by sensors promises the facilitation of a much clearer view of the operational environment in which human commanders can then make informed decisions. Counter-piracy and counter-smuggling operations can particularly benefit from these gains of AI-enabled situational awareness, as they increase efficiency and operation radius for deployed vessels, enabling a bigger portion of the sea to be monitored more effectively by each unit. A selection of AI applications which have the potential to enhance maritime security operations are explained in the following section.

Observable Ocean: Smallsats

SpaceX's Starlink has brought new attention to the idea of an encompassing global net of small satellites providing users with comprehensive internet coverage. Small satellite (smallsats) constellations are nothing new, with projects such as Iridium launching already in the 1990s. But with market analysts estimating 1,800 to 2,400 smallsats in the 1 to 100 kg range launching until 2025[3] and increased processing capability for AI functions, small satellite constellations can become a critical asset for maritime surveillance and reconnaissance. Smallsats could then potentially fulfill many roles:
The sensing capabilities of smallsats are constantly increasing through better optics, radar applications and other functionalities[4] but managing a big group of small satellites and merging and analyzing their accumulated data for security operations can be a difficult task. AI-supported edge computing approaches to smallsat operation can support human decision makers in this task. The role that AI can play in the use of smallsats for maritime security operations can herein vary.
Manning et al. (2018)[5] describe three applications of AI to small satellites: Autonomy, communication and analysis. Autonomy and communication both serve to facilitate optimum operability and functionality, even when direct contact with the satellite is threatened or reduced. New AI-supported on-board analysis functions on the other hand allow for an effective use of resources and directly support decision making on the ground. While high-performance AI these days usually runs on GPUs using up intensive resources, Manning et al. provide evidence that even smaller, on-board hardware can feasibly run AI analysis tasks, pointing towards an increasing potential throughout this decade.

With this, AI-supported smallsats could be able to provide crews in maritime environments with pre-analyzed orbital sensor data. With the connection of many satellites, an almost constant picture of the situational environment can be drawn, which military decision makers can then immediately use to translate into operational actions.

Observable Ocean: Autonomous Vehicles

The history of autonomous maritime vehicles such as Autonomous Surface Vessels (ASVs) and Uninhabited Un-

[2] Williamson III, William (2020): From Battleship to Chess Available from: https://www.usni.org/magazines/proceedings/2020/july/battleship-chess
[3] Ibid.
[4] Ibid.
[5] Jacob et al. (2018): Machine-Learning Space Applications on SmallSat Platforms with TensorFlow. Available from: https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4270&context=smallsat

derwater Vehicles (UUVs) is already long: The use of UUVs by navies dates back to the 1950s, with over a quarter of the world's nations currently employing such vehicles.[6] But while the general idea and its deployment is nothing new, the capabilities of this technology are growing considerably through advances in Machine Learning and Artificial Intelligence. Integrating some kind of autonomy into UUVs via AI is in the first place almost a necessity due to the difficulties of underwater communication[7]. But beyond this, AI is starting to open up new doors for operational capabilities. Like many AI trends in the maritime sector, the idea here started with reducing cost and staff while maintaining full capabilities. The increasing amount of data that gets collected and analyzed, equipping ASVs and UUVs with more autonomy and more processing capabilities and new sensor technology promises additional advantages.

Much like their more prominent spaceborne counterparts like the MQ-4C Triton, ASVs and UUVs can provide flagships with a diversified and broad but detailed picture of the operational environment while already carrying out on-board analysis tasks which reduce the need for monotonous human overwatch and support quick decision making[8]. Beyond this, equipping them with hard and soft-kill capabilities and combining them with increasing autonomy can turn such vehicles into effective operational assets, supporting the mission in scenarios that require a minimal invasive approach or acting as swarms. To facilitate interoperability between the associated devices, would however require the development of common communication protocols.[9] As with smallsat AI-integration, their use seems likely to increase in the coming years as the technology to facilitate resource-intensive AI tasks evolves to smaller hardware.

Observable Ocean: Ocean of Things

Ocean of Things, a research project started in 2017 by the Defense Advanced Research Project Agency (DARPA) describes a new type of AI-supported, distributed passive sensor network that can enable enhanced situational awareness on the oceans. Ocean of Things specifically envisions a constellation of thousands of sensor-equipped floats with on-board processing capability in which every individual unit collects oceanographical and meteorological data, while also allowing the detection and tracking of identified vessels and aircraft in the surveillance area. In an edge computing approach similar to that of smallsats, the collected data is then being accumulated and processed by the float itself before being reported and turned into actionable intel. The floats are made up of environmentally save materials and supposed to endure on the ocean for up to one year before scuttling themselves and descending to the ocean floor. The project itself is also marked by its estimated low cost per unit cost with 50,000 floats aimed at covering up to one million square kilometers of ocean.[10]

One important goal of the deployment of such a network could be the realization of a 'digital ocean'[11] concept. In this concept, the accumulated data of thousands of distributed sensors, such as the Ocean of Things floats, but also ASVs, UUVs and smallsats is being put together by AI into a digital visualization of a certain, limited oceanic area. In this area, invisibility for hostile vessels and units and their movements would be theoretically impossible. Layton (2021)[12] describes the realization of such a concept 'revolutionary' for naval warfare. But below that, if deployed, it seems particularly suitable to serve as an exceptional tool to prevent smuggling and piracy activities in delimited theaters such as the Gulf of Somalia.

Intelligent Decision Support Systems

Commanders as well as seamen find themselves having to make difficult decisions every day in the operational environment. With more and more autonomy being introduced into the operational space, massive influx of data and an increase in the pace of operations, optimal decision making becomes increasingly challenging. Sciences has been employed for decades now to assists military decision makers in decisions by creating decision support systems (DSS), which aim to provide their user with predefined recommendations based on the existence of certain situational variables. In the course of the global experimentation with military AI applications, Machine

[6] Matth ewson, Andro (2021): Responding to the Proliferation of Uninhabited Underwater Vehicles. Available from: https://cimsec.org/responding-to-the-proliferation-of-uninhabited-underwater-vehicles/

[7] Wilson, JR (2019): Unmanned submarines seen as key to dominating the world's oceans. Available from: https://www.militaryaerospace.com/unmanned/article/14068665/unmanned-underwater-vehicles-uuv-artificial-intelligence

[8] Galdorisi, George (2019): The Navy Needs AI, It's Just Not Certain Why Available from: https://www.usni.org/magazines/proceedings/2019/may/navy-needs-ai-its-just-not-certain-why

[9] Wilson, JR (2019): Unmanned submarines seen as key to dominating the world's oceans. Available from: https://www.militaryaerospace.com/unmanned/article/14068665/unmanned-underwater-vehicles-uuv-artificial-intelligence

[10] DARPA (2020): Broad Agency Announcement - Ocean of Things Phase 2 Data Analytics. Available from: https://www.darpa.mil/attachments/HR001120S0042.pdf

[11] Liquid Robotics (2016): The Digital Ocean. Available from: https://cdn2.hubspot.net/hubfs/287872/LR_DigitalOcean_eBook.pdf

[12] Layton, Peter (2021): Winning the AI-enabled War-At-Sea. Available from: https://cimsec.org/winning-the-ai-enabled-war-at-sea/

Learning and Artificial Intelligence seem an obvious choice for enhancing these support systems: Intelligent Decision Support Systems (IDSS) are envisioned to employ the fast data-analyzing capabilities of ML and AI to compensate for human shortcomings in decision making. A large compendium of literature on the pros and cons of the use of such IDSS already exists, pointing towards the possibilities and efficiency gains, as well as the legal and ethical issues associated with these systems. It is however worth mentioning how IDSS are conceptualized and how they can possibly be connected to the maritime AI applications mentioned above.

Van den Bosch & Bronkhorst (2018)[13] provide a useful description of IDSS: Consisting of a given domain model (e.g., naval operations), and an inference function, an IDSS employs Artificial Intelligence to scour through input data, analyze patterns and calculate feasible actions based on programmed values. This is an addition to normal DSS which contains a pre-defined set of solutions and recommendations for a certain situation.

The more data an IDSS is being fed (for example through various sensing applications discussed under 2a), the more accurately it can model the domain which constitutes the basis on which courses of action are proposed. However, van den Bosch and Bronkhorst (ibid.) also identify a number of shortcomings of IDSS, listing amongst others the vulnerability to adversarial attacks.

AI risks

Artificial Intelligence is often ascribed the potential to fundamentally transform societies in the coming years and decades through its many possible applications that could assist or replace humans in different tasks. Yet, despite its potential positive impacts, critique of Artificial Intelligence and Machine Learning has accompanied the debate around the technology since its inception: AI's complex nature and ethical issues surrounding its use have led many experts to warn about its application in high-stakes environments. It also poses some inherent risks to its functioning and the associated operations around it.

In their policy brief for Georgetown University's Center for Security and Emerging Technology, Arnold and Toner (2021)[14] point towards the very real problem of unintentional AI accidents as a result of AI safety issues: Robustness, Specification and Assurance issues surrounding AI raise awareness of how inputs are being transformed into outputs by the system and what can go wrong inside AI mechanisms such as neural networks during this process due to its complexity. In their brief, the authors illustrate a number of possible cases of AI accidents based on actual events.

They explain how AI functionality can be impeded by abnormal or unexpected inputs, a not specified enough AI or the absence of control and intervention mechanisms of the system for human supervisors. The three problems of robustness, specification and assurance signify possible openings for unintentional AI failures.

AI Cyber Security Aspects

On top of that, these openings also play an important role for malicious actors seeking to undermine the AI's functionality by intent. Because just like any other computer system, Artificial Intelligence can be hacked. In fact, the complexity and opaqueness might make it even easier to manipulate, making AI a potential cyber security risk, also in maritime applications.

When it comes to hacking Artificial Intelligence, Lohn (2020)[15] differentiates between Integrity, Confidentiality and Availability attacks, focusing on the first two representing which to him constitute the most dangerous attacks. These are aimed at forcing AI-enabled systems to error or at extracting valuable information about the systems AI itself (which can then in turn be used to facilitate Integrity attacks). Lohn goes on to separate Integrity attacks into data poisoning and evasion attacks, with the former looking to insert specific training data on which the machine learning models are trained to control the learning content and subsequent output of the learning models, while the latter exploits the AI model's 'programming' to force unintended assessments by controlling the inputs of the deployed system.

Confidentiality attacks on the other hand are categorized by Lohn as Model Extraction, Membership Inference and Model Inversion. These types of attacks are mainly aimed at gaining knowledge about how the AI system's machine learning model works and the data it is trained with, in order to also generate further attacks against the AI with that knowledge.

Countermeasures to these attacks already exist, for example in the form of adversarial and explainable AI.[16] However, currently there still remains a trade-off between AI performance

[13] Van den Bosch & Bronkhorst (2018): Human-AI Cooperation to Benefit Military Decision Making. Available from: https://www.researchgate.net/publication/325718292_Human-AI_Cooperation_to_Benefit_Military_Decision_Making

[14] Arnold & Toner (2021): AI Accidents: An Emerging Threat
What Could Happen and What to Do. Available from: https://cset.georgetown.edu/publication/ai-accidents-an-emerging-threat/

[15] Lohn, Andrew J. (2020): Hacking AI. A Primer for Policymakers on Machine Learning Cybersecurity. Available from: https://cset.georgetown.edu/wp-content/uploads/CSET-Hacking-AI.pdf

[16] Woodie, Alex (2020): Hacking AI: Exposing Vulnerabilities in Machine Learning. Available from: https://www.datanami.com/2020/07/28/hacking-ai-exposing-vulnerabilities-in-machine-learning/

and resilience, meaning that AI performance is decreased while resilience measures are enabled.[17] Much like high-performing but vulnerable AI, in a high-stakes environment such as in maritime security, lowered AI performance can cost lives when operators heavily rely on their systems. This assumption feeds directly into the issue of AI trust.

AI Trust

The aforementioned vulnerabilities clearly show that AI systems are far from being the silver bullet when it comes to handling all kinds of problems in cyberspace, instead, they add some problems on their own part. This plays into one of the most critical aspects of AI deployment: Trust. Despite their vulnerabilities, well trained, tested and validated AI systems do and will offer humans exceptional performance and efficiency gains, that would otherwise be impossible for humans to achieve. A sailor who learns that an AI-supported navigation or reconnaissance system can assist him extremely well during day-to-day operations, will inevitably begin to establish a certain amount of confidence in the AI's performance. If not well designed, this might even happen although the sailor is unable to understand how the AI system works, how it processes inputs and how it generates actions. This trust – be it because of the good performance, lack of understanding or both – poses a serious risk to cyber security of deployed systems and operations as a whole. This is due to the difficulty of realizing abnormal outputs by the system in time when it is experiencing an unintended incident or has been hacked intentionally. History is already full of accounts of accidents in which a blind trust in AI systems led to dramatic consequences: people crashing in their self-driving cars being a sad yet prominent example.[18]

Considerations on cyber security for maritime AI applications

The selected maritime AI applications listed above stand to potentially bring extraordinary change to the field of maritime security in the coming years by increasing maritime situational awareness and striving for an 'observable ocean' on which vessels can no longer entrust the vastness of the oceans to obfuscate their movements. AI seems set to play a major role in the reshaping of maritime security operations by processing and analyzing gigantic swathes of data, impossible to be processed adequately by humans. But embedding AI into naval systems brings with it its known shortcomings of being vulnerable to fooling and manipulation. AI can then become a target itself, compromising operations which rely on it. This raises the following question: How will the operationalization of AI-supported systems and the rise of AI dependency in maritime security operations affect maritime cybersecurity and maritime security in general?

Technical considerations

The aforementioned vulnerabilities of Machine Learning and Artificial Intelligence also apply to an emerging use of AI in the maritime domain. These technologies promise to revolutionize the way the operational environment of the world's seas as an opaque terrain marked by its hard to surveil vastness towards a more observable environment in which actors will have to adapt their tactics and strategy. Their importance for enabling this observability would also change the role of cyber security for operators, as the loss of "sight" on sea will come with a marked disadvantage, especially in a time when navies are trying to accomplish missions with less human staff than ever before. Adversaries have therefore much to gain when they try to inhibit AI-enabled maritime situational awareness through cyberattacks.

Losing situational awareness could happen for example through cyber attacks against sensors like DARPA's Ocean of Things floats. These devices will need to communicate their observations and analyses somehow to data centers or flagships and possibly even directly into a vessels IDSS. Gaining access to the device by hacking this connection could allow adversaries to manipulate the outputs of the sensor, for example through evasion attacks against the data center or the IDSS.

Another way to compromise situational awareness and disrupt trust would be through poisoning of the training data sets of the sensor, either before or during deployment. Intelligence communicated to the human operator could then be distorted (e.g., manipulated friend-foe distinction), which in the event of kinetic engagements could have dramatic consequences.

Also, fielding AI in great numbers through UUVs, floats and other devices increases the risk of extraction of AI assets through Confidentiality attacks. If the adversary, through attacks like the model extraction or model inversion, can learn to understand the deployed AI, he would be able to use that knowledge to further manipulate the AI for his purposes.

Classic cyber security will increase in importance as well. After all, when the Cyber Physical Systems (CPS) are hacked in which ML and AI are embedded, this causes the unavailability of the AI on which an operation might depend.[19] For this, the CPS wouldn't

[17] Ibid.

[18] The Guardian (2021): Tesla's Autopilot faces US investigation after crashes with emergency vehicles. Available from: https://www.theguardian.com/technology/2021/aug/16/teslas-autopilot-us-investigation-crashes-emergency-vehicles

even have to be destroyed: Having a "rogue" UUV in the field which still sends data to the rest of the forces but is all the while controlled by the adversary could distort the operational bigger picture of commanders.

All these aspects of cyber security feed into the issue of AI trust. Plenty of authors[20] have pointed out the need for explainable, trustworthy AI that can integrate with the human operator to truly enhance operational capabilities and not degrade them. Especially in an operational environment as challenging as the maritime one, humans have to make important decisions constantly; decisions that need to be based on the most accurate information available. If the information on what the commander faces ahead of and around him is flawed, making the right decision becomes problematic. The same applies to any decision support system that either employs some form of AI-enabled inference model or is being fed by the information collected and analyzed by AI-supported sensing devices.

Finally, AI accidents will also need to be factored in, especially as more and more decisions and day to day operation rely on these applications. Human operators have no time to 'think for' a digital system, i.e., which in- or outputs they cannot fully trust. Understanding the ways in which an AI system can accidentally fail can help the operator to prevent or quickly account for these situations and adapt to achieve optimal mission outcome.

Ethical considerations

As shown above, the future maritime security environment will be marked by massive amounts of data, interconnection and short, critical decision windows. AI in connection with edge computing offers to leverage the data and provide close to real-time situational awareness for naval commanders. But a commander's decision will also rely on the performance of machines more than ever, with AI distributed along the intelligence chain. Making high-stakes decisions based on AI assessments raises ethical questions: To which degree is the commander's decision still his own if input data is increasingly pre-analyzed by AI?

As pointed out above by Lohn, the loss of availability of AI systems might be problematic, but far less crucial than the loss of their integrity, or the loss of confidentiality to achieve the latter. If an AI system on 'the edge' is compromised and the data it relays back to the back-end is compromised, a false picture of reality with which the commander is confronted can appear. Decisions made based on such a false image of reality can have drastic consequence if decision makers fail to detect that compromise. What makes this even more challenging is the speed at which decisions will have to be made in the near-future maritime environment. The pace of the battlefield will shorten the time commanders have to verify intelligence inputs, increasing the risks of situational awareness data analyzed by AI. Combined with the possibility that decisions based on these technologies could entail the use of lethal force, the stakes become even higher.

This illustrates that navies need to develop special sensitivity to these ethical considerations which can arise out of a pervading use of AI in the maritime environment in the coming years. Keeping a human 'in the loop' might be an imperative today, but the degree to which he or she might actually be involved when it comes to making high-stakes decisions in a fast-paced maritime environment could vary and decline without always being noticed. Addressing these issues should therefore accompany considerations of integrating AI technologies in navies across the world.

Recommendations

Combining the dawn of new AI-supported applications in the coming years for the maritime security sector with our current knowledge about Machine Learning and Artificial Intelligence weak points, raises important issues for the (cyber) security of the domain. These issues have been shown to be of technical as well as ethical character, both of which should be addressed by maritime actors aiming to deploy these systems in the near future. To address these issues, we recommend the following:

Navies should consider the possibility of AI failure or manipulation in the operational context: Being aware of the vulnerabilities of AI-supported situational awareness concepts constitutes the first step towards creating security conceptualizations for these systems. The oncoming changes in the operational environment require navies to carefully consider how their AI systems will need to be secured to achieve their best possible impact.

This is in direct relation to the issue of adversarial acquisition of AI systems, ML models and algorithms. Any operational concept around AI systems needs to consider the effects of an AI system or part thereof falling into unauthorized hands, which could have far-reaching consequences for decisions are made.

This would also mean a dedicated handling for the surveillance of AI assets: processes for the monitoring of

[19] Pupillo et al. (2021): Artificial Intelligence and Cybersecurity. Available from: https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf

[20] See Vilone & Longo (2020): Explainable Artificial Intelligence: A Systematic Review (Preprint). Available from: https://arxiv.org/abs/2006.00093

AI systems concerning their availability and integrity should be implemented on a technical level to recognize tampering early and subsequently adapt operations accordingly.

Directly tied to these points is the need for consideration of the architecture of AI and edge computing systems. These systems should be designed and implemented with the security issues outlined above in mind. Included in this are provisions for the possible failure or manipulation of components and how the overarching system can continue to function without them.

As pointed out in the previous section, an ethical design of Intelligent Decision Support Systems in particular is an important aspect which should not be ignored. Navies must make good use and further develop approaches such as Explainable AI and human-in-the-loop, while carefully weighing how much trust commanders should be able to put into AI systems. A delicate balance needs to be struck here between operational efficiency and the awareness of the flaws of current AI systems. From the other perspective, AI and IDSS can support in less flawed decisions, avoiding human bias and self-interest of individuals and illogic motivators such as bravery, cowardice, prudence, or fight or flight instincts. Either way, the goals of the decision making process need to be very carefully set in order to be able to clearly define what the 'best' decision would be.

Conclusion

With the coming dawn of operational artificial intelligence, the security domain is facing a radical technological change in the coming years. The maritime domain won't be excepted from this phenomenon. Ongoing interconnection of human actors and technology, as well as the acceleration of the pace of the battlefield stand to bring new challenges to maritime security actors. Artificial intelligence and IDSS can play a significant role in enabling these commanders to make calculated decisions in short time frames, drawing from and analyzing massive amounts of data. At the same time, the reliance on AI for these tasks brings with it particular security risks, in addition to already existing 'conventional' security risks of digital technology. AI is not a flawless technology in its current and foreseeable form and adds complexity to the already complex operational environment. This paper presented a selection of AI applications which are likely to play an important role in the maritime security environment in the coming decade, while also pointing to the security risks associated with AI systems. It also presented some major technical and ethical challenges in this respect, concluding in a series of recommendations for increasing the security of AI-supported approaches to maritime security.

Acknowledgements

We would like to thank the NMIOTC Cyber Security Conference organization team and especially so Commodore Charalampos Thymis, Commander Periklis Pantoleon, Lieutenant Commander Kostas Papanastasis, and Captain Rosario Lapira, for inviting us to contribute with a presentation and paper at the 5th NMIOTC Cyber Security Conference in the Maritime Domain. We would also like to express our gratitude to our peer reviewers Gerry Copitch (Business Development Director at mmd), Dr. Odilia Coi (Director of Innovation at MKAI – the Inclusive AI Community -, Author on Digital Trust and Guest lecturer at University of Cagliari), Sam Chaher (Data & AI Community Organiser and Data Analytics Recruitment Specialist at Austin Fraser), and Chronis Kapadilis (Principal at Information Security Forum).

Dr. Swantje Westpfahl is the acting director of the Institute for Security and Safety at the Brandenburg University for Applied Sciences.
Holding a PhD in the interdisciplinary field of linguistics and machine learning she is experienced in a variety of scientific methods, and in the coordination and organization of research and educational projects. At the Institute for Security and Safety her main objectives are the strategic development of the institute and the expansion of cooperation projects. Thus, she's also the personal point of contact for all cooperation partners. She coordinates the research and development as well as the capacity building activities of the Institute, especially with a focus on new developments in cyber security, e.g. with respect to the energy and automotive industry.
As a key point of contact with international institutions, she is the ISS's representative at the United Nations OEWG on ICT in the context of international security and also, together with ISS Director Guido Gluschke, in UNECE's WP.29 GRVA. Her main areas of expertise are security culture, capacity building and didactics, and cyber security in international relations.

Tim Dalhoefer is Project Manager for international projects at the Institute for Security and Safety. In this role, he coordinates projects with collaboration partners world wide. He also works on research projects for cyber security in the energy sector and supports the institute's efforts at international Internet Governance such as the United Nations Open-ended Working Group (OEWG) on international cyber security. Tim holds a Bachelor's degree in International Relations from the University of Erfurt. His main fields of academic interest are International Security Policy and Internet Governance.

Bibliography

- Arnold, Zachary & Toner, Hellen (2021): AI Accidents: An Emerging Threat. What Could Happen and What to Do. Available from: https://cset.georgetown.edu/publication/ai-accidents-an-emerging-threat/
- DARPA (2020): Broad Agency Announcement - Ocean of Things Phase 2 Data Analytics. Available from: https://www.darpa.mil/attachments/HR001120S0042.pdf
- Galdorisi, George (2019): The Navy Needs AI, It's Just Not Certain Why Available from: https://www.usni.org/magazines/proceedings/2019/may/navy-needs-ai-its-just-not-certain-why
- Jacob et al. (2018): Machine-Learning Space Applications on SmallSat Platforms with TensorFlow. Available from: https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4270&context=smallsat
- Layton, Peter (2021): Winning the AI-enabled War-At-Sea. Available from: https://cimsec.org/winning-the-ai-enabled-war-at-sea/
- Liquid Robotics Inc. (2016): The Digital Ocean. Available from: https://cdn2.hubspot.net/hubfs/287872/LR_DigitalOcean_eBook.pdf
- Lohn, Andrew J. (2020): Hacking AI. A Primer for Policymakers on Machine Learning Cybersecurity. Available from: https://cset.georgetown.edu/wp-content/uploads/CSET-Hacking-AI.pdf
- Matthewson, Andro (2021): Responding to the Proliferation of Uninhabited Underwater Vehicles. Available from: https://cimsec.org/responding-to-the-proliferation-of-uninhabited-underwater-vehicles/
- Pupillo et al. (2021): Artificial Intelligence and Cybersecurity. Available from: https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf
- Raveling, Jann (2021): Artificial intelligence within the maritime industry. Available from https://www.wfb-bremen.de/en/page/bremen-invest/artificial-intelligence-within-maritime-industry#wfb-ai-ships
- The Guardian (2021): Tesla's Autopilot faces US investigation after crashes with emergency vehicles. Available from: https://www.theguardian.com/technology/2021/aug/16/teslas-autopilot-us-investigation-crashes-emergency-vehicles
- Van den Bosch & Bronkhorst (2018): Human-AI Cooperation to Benefit Military Decision Making. Available from: https://www.researchgate.net/publication/325718292_Human-AI_Cooperation_to_Benefit_Military_Decision_Making
- Vilone & Longo (2020): Explainable Artificial Intelligence: A Systematic Review (Preprint submitted to Elsevier). Available from: https://arxiv.org/abs/2006.00093
- Williamson III, William (2020): From Battleship to Chess Available from: https://www.usni.org/magazines/proceedings/2020/july/battleship-chess
- Wilson, JR (2019): Unmanned submarines seen as key to dominating the world's oceans. Available from: https://www.militaryaerospace.com/unmanned/article/14068665/unmanned-underwater-vehicles-uuv-artificial-intelligence
- Woodie, Alex (2020): Hacking AI: Exposing Vulnerabilities in Machine Learning. Available from: https://www.datanami.com/2020/07/28/hacking-ai-exposing-vulnerabilities-in-machine-learning/

Securing the Software Supply Chain for Naval Warfare Systems

by Eric Hill
Synopsys

Introduction

The last several years have placed a spotlight on the exploitability of software in the supply chain. Critical infrastructure and the defense sector present a heightened need to manage risk. Recently, amongst other incidents, 2020 brought us the Solar Winds Supply Chain Campaign and 2021 the Colonial Pipeline outage as well as the Hafnium MS Exchange campaign.

On May 12, 2021, USA Presidential "Executive Order on Improving the Nation's CyberSecurity" (14028) was published. Section 4 ("Enhancing Software Supply Chain Security") specifically provides a focus for a more secure software supply chain future. More importantly, it reframes the importance of securing the software supply chain.

As a result of Executive Order 14028, **NIST** (National Institute of Standards and Technology) released "Guidelines on Minimum Standards for Developer Verification of Software" on July 11, 2021. The document defines verification of software and practices that should be utilized, where applicable, to secure the software supply chain. The list includes:

- Software Composition Analysis - SCA
- Static Application Security Testing - SAST
- Interactive Application Security Testing - IAST
- Dynamic Application Security Testing - DAST
- Fuzzing.

On July 12, also a result of the EO, the NTIA (National Telecommunications and Information Administration) published "The Minimum Elements For a Software Bill of Materials (SBOM)". This was a highly tactical NTIA release that broadly brushes on many concerns. Most importantly, however, the document recommends a starting point and approach.

In addition, during the month of July 2021, The US Department of Defense staff officially signed off on the DevSecOps 2.0 series of guidebooks. Central to DoD DevSecOps (DSO) is the concept of DSO Software Factory and its "control gates" with software verification tools and practices being applied in the software development life cycle.

SCA, SAST, IAST and DAST, all identified and defined in the NIST "Guidelines on Minimum Standards for Developer Verification of Software", are given a more operational context in the DoD DevSecOps documentation set places SCA, SAST, IAST and DAST into the DSO Software Factory context while the NIST "Guidelines on Minimum Standards for Developer Verification of Software" gives broader definition of each as a discipline and includes fuzzing. For our discussion on best practices in the Software Factory,

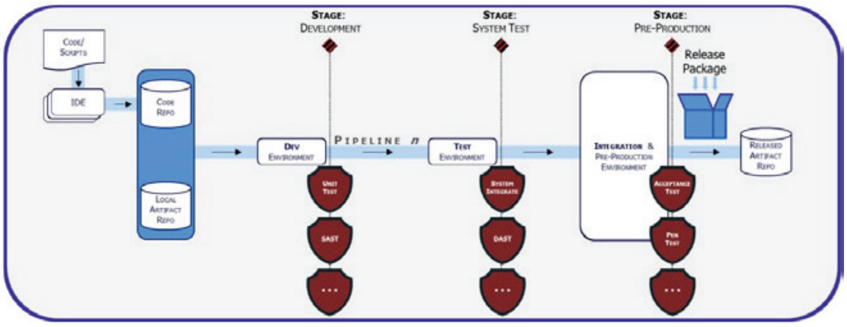


Figure 1. Notional Expansion of a Single DevSecOps Software Factory Pipelin
(DoD Enterprise DevSecOps2.0- Strategy Guide)

we will thus add fuzzing along with SCA, SAST, IAST and DAST as it is present in the documentation resulting from EO 14028. This is not random as the author is aware of fuzzing being utilized in the defense sector. It is well placed in the Software Factory efforts.

It should be noted that SCA, SAST, IAST, DAST and fuzzing software verification tools and practices can be, and in fact are, applied to software components destined to maritime port systems, considered critical infrastructure, just as well as well as naval warfare systems. The same rigor and general best practices apply. The rest of document can be considered to address both implicitly.

CWE's, CVE's and CAPECs

Before continuing further into the presentation of the Software Factory let us back up a bit and define several important concepts to frame the conversation and, in fact, the larger cyber security picture.

A Common Vulnerability and Exposure (CVE) is a vulnerability reported to the USA's National Vulnerability database against deployed software components. All vulnerabilities, CVE's and unreported vulnerabilities can be mapped to one or more weakness (CWEs). This relationship is depicted in the Venn Diagram in Figure 2. Thus, it could be stated CVE's represent CWE's present in deployed software that have been advantaged via a CAPEC(s). A CVE entry in the NVDB (National Vulnerability Database managed by NIST) could be the result of activities by any number of parties including: a state aggressor, organized crime, white hat hackers, or even corporations (the latter may have even taken on responsibility as a numbering authority).

We gain situational awareness with CVE entries and their severity, including mapping to a CWE(s). However, we must never lose sight of the fact that this is now a publicly noted exploit that demands risk assessment and appropriate velocity in remediation via update of the software component, most often open source.

In proprietary code the goal should be to apply a practice of "CWE Avoidance" where developers minimize introduction of CWE's to a project's release package and thus exposure to exploits.

The Software Factory

The implementation of a Software Factory and its related practices enables agility in using open source software securely by understanding CVE risk posture. A proper practice also empowers project teams' developers to execute on preemptive avoidance of CWE's introduced into their proprietary code. This proprietary code is inevitably part of a software component destined to be deployed as part of a system. In the context of this discussion, and according to the author's industry experience, the software component could be destined for a Naval Warfare System.

The rest if this written discourse will be framed in the context of the DoD Software Factory as defined in the version 2.0 suite of guides:

It should be noted that both the DoD DevSecOps documentation set and the NIST "Guidelines on Minimum Standards for Developer Verification of Software", both consider each type of the software verification methods

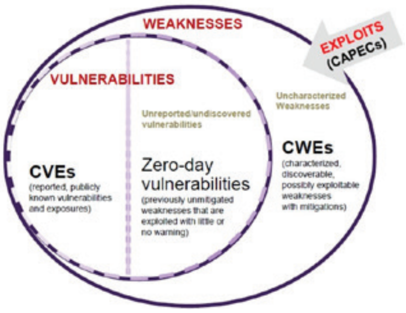


Figure 2. CWE/CVE/CAPEC
Venn Diagram
(Synopsys SIG Tool Reporting Using
Standards-Based Security)

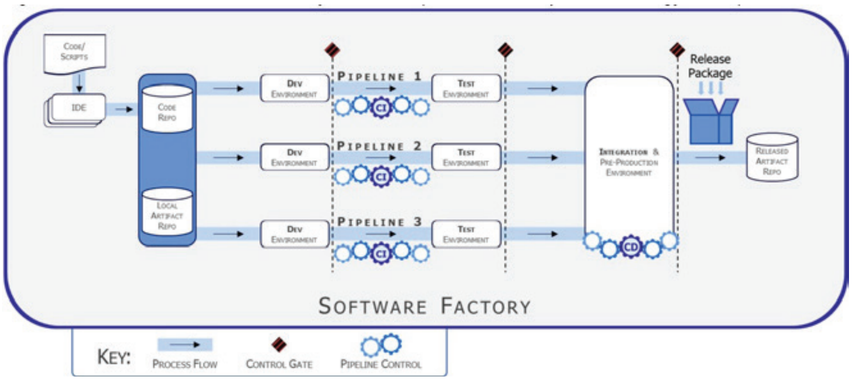
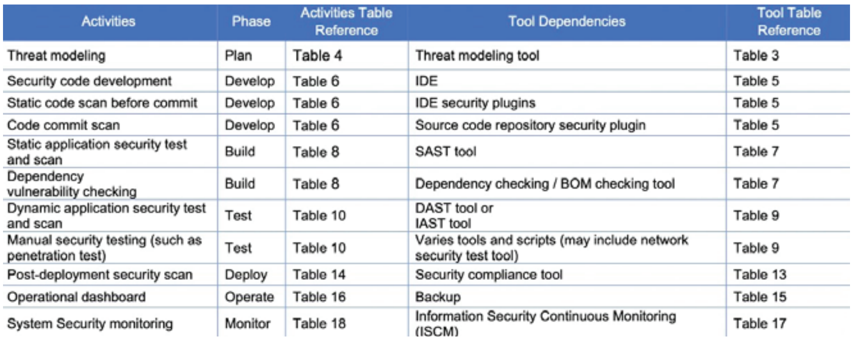


Figure 3 – Normative Software Factory Construct (DoD DevSecOps 2.0: Strategy Guide)

and related practices different enough to apply them in the same software lifecycle where warranted. Although there may be some overlap, for instance, in a sampling of CWE's that are identified both by SAST applied at a control gate vs IAST at a control gate in the test phase, the different methods and their rigor should be applied where applicable. Further in static scanning (SAST), the DoD specifically supports the findings of industry in that it is a best practice to apply in both the Develop as well as the Build Phase as indicated in the table below.



Activities	Phase	Activities Table Reference	Tool Dependencies	Tool Table Reference
Threat modeling	Plan	Table 4	Threat modeling tool	Table 3
Security code development	Develop	Table 6	IDE	Table 5
Static code scan before commit	Develop	Table 6	IDE security plugins	Table 5
Code commit scan	Develop	Table 6	Source code repository security plugin	Table 5
Static application security test and scan	Build	Table 8	SAST tool	Table 7
Dependency vulnerability checking	Build	Table 8	Dependency checking / BOM checking tool	Table 7
Dynamic application security test and scan	Test	Table 10	DAST tool or IAST tool	Table 9
Manual security testing (such as penetration test)	Test	Table 10	Varies tools and scripts (may include network security test tool)	Table 9
Post-deployment security scan	Deploy	Table 14	Security compliance tool	Table 13
Operational dashboard	Operate	Table 16	Backup	Table 15
System Security monitoring	Monitor	Table 18	Information Security Continuous Monitoring (ISCM)	Table 17

Figure 4- Security Activities Summary Cross-Reference (DoD DevSecOps Tools & Activities Guidebook)

Note the exclusion of fuzzing in the table above. Fuzzing is well noted in the NIST "Guidelines on Minimum Standards for Developer Verification of Software. As stated previously, it is recommended by the author that fuzzing be considered in the Test phase, where DAST and IAST tools and their practices are applied, where warranted.

While we will be navigating left to right in the Software Factory diagram (review Figure 1 and 2), to more easily match life cycle phase and appropriate application of software verification tools and their practice that are recommended, and the author in many cases has advised in practice.

Software Composition Analysis

In regards, to Software Compositions Analysis, NIST notes that "these tools can aid in determining what software is really imported, identifying reused software (including open source software), and noting software that is out of date or has known vulnerabilities"1 . For sake of this paper, and the context of the Software Factory, we will assume SCA is applied for the evaluation of open source brought into the factory and placed into the Local Artifact Repo (see Figures 1 and 3).

In applying Software Composition Analysis, it is best to rule by exception. Thus, we use policy risk violations as our guide. For instance, Synopsys SCA platform has 3 types of risk: license risk (legal), operational (age) and security (CVE accumulation). These are, in turn, taken into account by stake holder policy applied to the BOM of the open source software utilized in a project. In an automated fashion, stake holders can be alerted via policy thresholds being exceeded by crossing a CVE security risk threshold. For the sake of this paper we are most concerned with security risk.

In this same vein the author recommends choosing a solution that dynamically updates CVE accumulation of open source software components that are recorded in the mission projects SBOM at assignment to the project. This will enable notification of changes to cyber security posture for open source maintained in the local artifact repo (see Figure 1 and3), over time and empower stake holder decisions related to updating open source software components for mitigation in project(s) that use it.

In practice, at each phase of the SDLC, SCA may be applied at the respective control gate to: simply baseline the SBOM, evaluate and ensure the software components that make up the SBOM have not deviated from initial allocation, and as well ascertain if CVE accumulation on a software component has caused security risk to cross a defined policy threshold; invoking product/mission stakeholder assessment and decisions. Note that the DoD (see table in Figure 4) specifically reserves the security control gate at the Build phase for SBOM activity; addressed later in this document. However, if you have an SCA product that dynamically updates CVE allocation to the open source components, such as Synopsys' Black Duck, this is handled automatically throughout the SDLC and thus all phases in the software factory the SBOM reflects CVE-related security risk.

SAST and Shifting Left

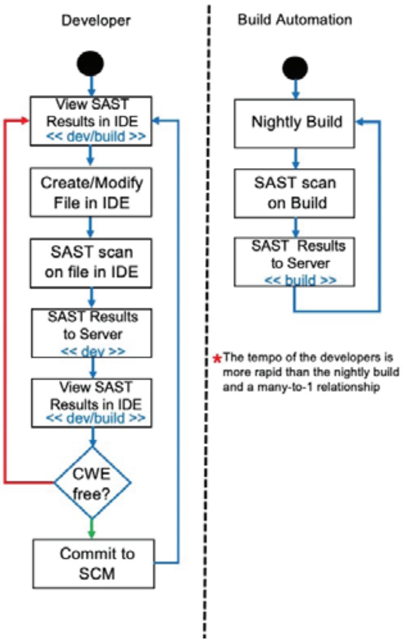

Developer
Build Automation
View SAST Results in IDE << dev/build >>
Create/Modify File in IDE
SAST scan on file in IDE
SAST Results to Server << dev >>
View SAST Results in IDE << dev/build >>
CWE free?
Commit to SCM
Nightly Build
SAST scan on Build
SAST Results to Server << build >>
*The tempo of the developers is more rapid than the nightly build and a many-to-1 relationship

Figure 5- Shifting Left w/ SAST into the Developer IDE

In regards to SAST, DoD notes on SAST "analyzes application static codes, such as source code, byte code, binary code, while they are in a non-running state to detect the conditions that indicate code weaknesses") I1 (p20 Tools and activities") This is an important distinction later when considering DAST, IAST and fuzzing and why they are applied later in the SDLC.

In applying SAST as a practice we are scanning proprietary program code that is created by the Software Factory developer team. We want the developer to stay in the role with which they are familiar within their development IDE environment evaluating and mitigating CWE's found both by their own local scans during the Development phase and the automated build system scans during the Build phase (see Figure 4). This is a key enabler in "shifting left". As well, to interact with results from the SAST scans performed against the broader code base as a control gate in the build phase and to fix them in their IDE. A representation of such a process flow is represented in the diagram below.

In any case, by definition, SAST scans are applied against static code. Various programming languages may be supported by a given SAST tool.

As far as onboarding legacy code, it is almost inevitable the first scans will introduce a number of CWE's; possibly thousands. We tend to refer to this as "technical debt". At Synopsys we recommend tagging these as "Legacy" and working of this debt at a rate over time that is reasonable for the organization. At the same time, the goal is to introduce as few CWE's as possible.

The goal in applying SAST in conjunction with other aspects of the DSO Software Factory, is to minimize impacts on developer velocity in adding value to the secure code to the code base that support mission requirements.

IAST (Test Phase)

The DoD defines IAST as to "Analyze code for security vulnerabilities while applications is run by an auto-test, human tester, or any activity 'interacting" with the application functionality."

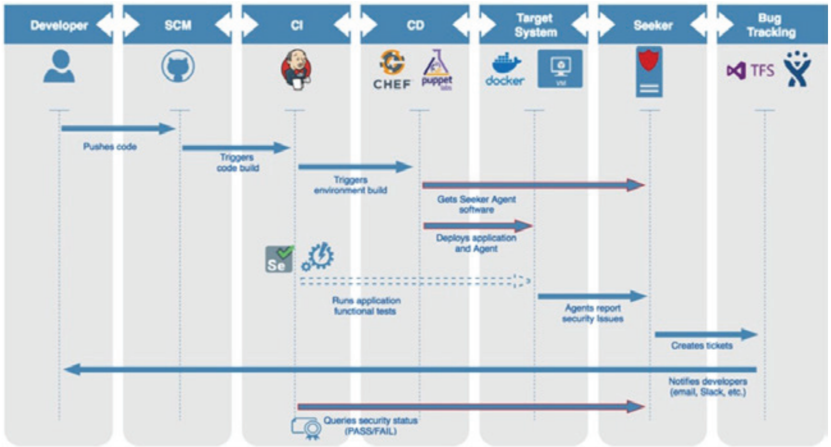

Developer
SCM
CI
CD
Target System
Seeker
Bug Tracking
CHEF
puppet labs
docker
VM
TFS
Se
Pushes code
Triggers code build
Triggers environment build
Gets Seeker Agent software
Deploys application and Agent
Runs application functional tests
Agents report security Issues
Creates tickets
Notifies developers (email, Slack, etc.)
Queries security status (PASS/FAIL)

Figure 6 - IAST CI/CD Workflow (Seeker Guides, Synopsys 2020)

As a software component(s), passes through the life cycle to the next control gate, we will want to possibly deploy into infrastructure and place it under test. In the case of a web user interface, whether SOC or NOC or even a console, IAST (Interactive Application Software Testing) is a unique type of testing where will have the opportunity instrument the software package and deploy in an environment under test. As a test professional navigates through the user interface under test, tests are applied against the instrumented system. The diagram below represents the interaction with an example CI/CD system and deployment of the instrumented package.

An IAST verification tool should be able to provide CWE's mapped to the source code as well as CVE's that have been reported against open source used in the package. In the latter case, it is an opportunity to ensure situational awareness of any critical CVE's that may have accumulated later in the lifecycle and presented with the test results. It is understandable that the IAST will have some overlap with CWE's discovered in applying SAST. However, the methodology is in fact different and will find CWE's not found in applying SAST as in at least it is recognized that there are instances of CWE's that will only manifest in code that is executing.

Synopsys IAST tool, known as Seeker, can identify CWE's, CVE's and CAPEC's in the software component under test. The previous circumstance noted of overlapping CWE identification has been noted in practice. Thus, the author can state that the DoD, and as well now NIST paradigms (as a result of EO 14028), application of SAST and IAST in the same SDLC has been verified.

DAST

Alternatively, we may be building a webservice that is part of a larger deployment. In this case, DAST (Dynamic Application Security Testing) would fit the case for testing a webservice (REST or otherwise) that may or may not be part of a larger service mesh architecture. It should be noted that a complete DAST software verification tool will not be limited to REST. Regardless, DAST would be used to exercise all methods of the webservice and report results. Typically, DAST products are delivered with automated test suites that may be expanded and new suites created. Regardless, the security goals are to stress the software under test in all of its iterations for exposure of CWE's.

Fuzzing

In regard to fuzzing, it is noted that software verification tool and practice: “induces program failures by deliberately introducing malformed or random data into software programs. Fuzz testing strategies are derived from the intended use of the applications and the functional and design specifications for the applications” – NIST 800-53 rev 5

A typical fuzzing tool will come with automated test suites for testing massive number of variable inputs and even randomized values. It is particularly useful in testing embedded code implementing communications protocols.

Synopsys’ fuzzer, Defensics, was used to discover the Heartbleed vulnerability (CVE-2-14-0160) in 2014 using this method.

For an example, we could be deploying a sensor under test that requires embedded code possibly supporting proprietary messaging protocols. The fuzzing software verification tool would ensure integrity of the sensor in handling variable and even malformed protocol fields and payloads.

Integration

We may choose to implement an integration sub-phase in the Test phase. As we integrate software components into a system, we apply a more complex test structure at the security control gate in the next phase. For instance, our CI/CD pipelines may be used to deploy a complex system service mesh of many webservices and a web visual front end. In this case, one could use DAST to supplement manual Pen Testing and as well revisit fuzzing. The strategies depend on the software components being delivered and the definition of the system.

Pre-Production

Here our CI/CD pipelines will build a deployable package depending; varied by the scenario. In Pre-Production, the team may choose to apply DAST or fuzzing as part of acceptance testing. This is also an opportunity to apply a final check via SCA to ensure no active policies have exceeded risk thresholds at this final step to release for the project version. . It is also wise to apply SCA in this pre-production phase to ensure the package’s software components preserve the continuity that has been maintained throughout the lifecycle phases up to this point.

In practice, the final release package may be composed of Open Container Initiative (OCI) compliant images and artifacts destined for a Kubernetes deployment. In other cases, the release package may be constituted of binary component(s) and accompanying artifacts.

SBOM

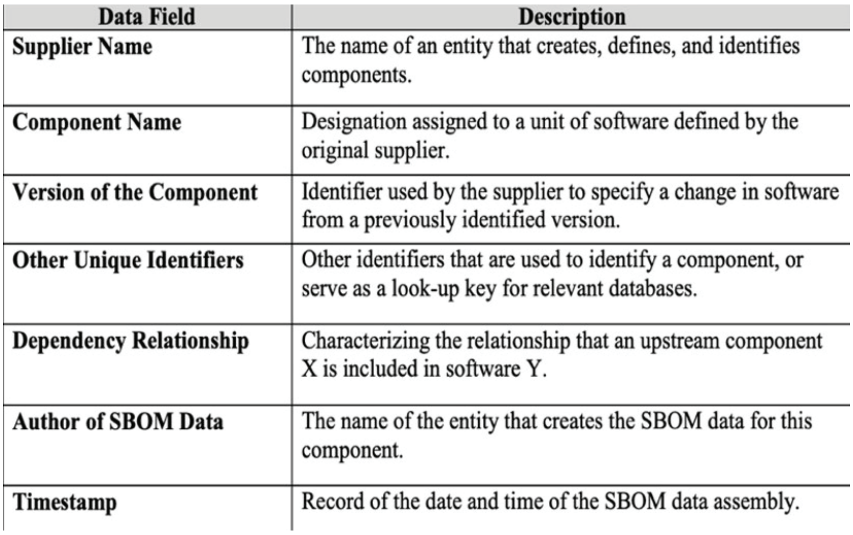
The Software Bill of Materials is mentioned by name in EO 14028 and considered key to supply chain risk management. With working groups addressing the issue, the NTIA very quickly released “The Minimum Elements for a Software Bill of Materials (SBOM)” reference document. This document clearly points to the fact that the providing an appropriate SBOM for national security is an evolving practice.

More specifically, it recommends that the SBOM not carry “vulnerability data” as this varies over time and can be found in external sources. However, the document notes the needs for more meta data in an SBOM and acknowledges also that this is a work in progress.

In the author’s defense sector experience, there are customers of proprietary software, as well as auditors, who have historically requested CWE data related to “phase” (in DSO Software Factory terminology) of its discovery. This enables the customer or auditor understand the supply chain risk of the software being delivered. Thus, the author is willing to state CWE related data is likely to be included in consideration of future SBOM work.

The table in Figure 7 below depicts the current recommendation for a minimum SBOM by the NTIA.

The SBOM compilation is considered a “Build” phase activity in the Department of Defense DevSecOps documentation suite (see Figure). However, and regardless of fields to be included, it is coupled with the SCA software tools and practices and can be implemented in all phases of



Data Field	Description
Supplier Name	The name of an entity that creates, defines, and identifies components.
Component Name	Designation assigned to a unit of software defined by the original supplier.
Version of the Component	Identifier used by the supplier to specify a change in software from a previously identified version.
Other Unique Identifiers	Other identifiers that are used to identify a component, or serve as a look-up key for relevant databases.
Dependency Relationship	Characterizing the relationship that an upstream component X is included in software Y.
Author of SBOM Data	The name of the entity that creates the SBOM data for this component.
Timestamp	Record of the date and time of the SBOM data assembly.

Figure 7- “The Minimum Elements for a Software Bill of Materials (SBOM)” the DSO Software Factory for a given pipeline. This can reduce supply chain risk in ensuring the actual open source software components of a given project in a given SDLC don't deviate from an original allocation approved by stake holders.

Release Artifact Repo

Finally, our CI/CD automations place the entire release package, including the SBOM, for the project into a version release artifact repo. From here the software is considered production deployable and at its final destination in the Software Factory. The release will be superseded by the next release per the velocity demanded by security risk assessment of the release software components.

Software Factory Situational Awareness

As project version software components move through the DSO Software Factory with velocity, the software verification toolchain may need to be recalibrated. A perfect example of this is the need to reduce false positives at each control gate. Also, as would be expected, Software Factory stakeholders tend to want to navigate security risk at varying grains: such as project, project release version and aggregations of projects over time.

The author contends that industry software products that fall into the Gartner ASOC (Application Security Orchestration and Correlation) category can in many ways support situational awareness needs that arise as the Software Factory matures.

Figure 8 is a simple data flow of the software verification tool chain, present in the software factory, feeding project security risk data to an ASOC tool to provide situational awareness to stake holders.

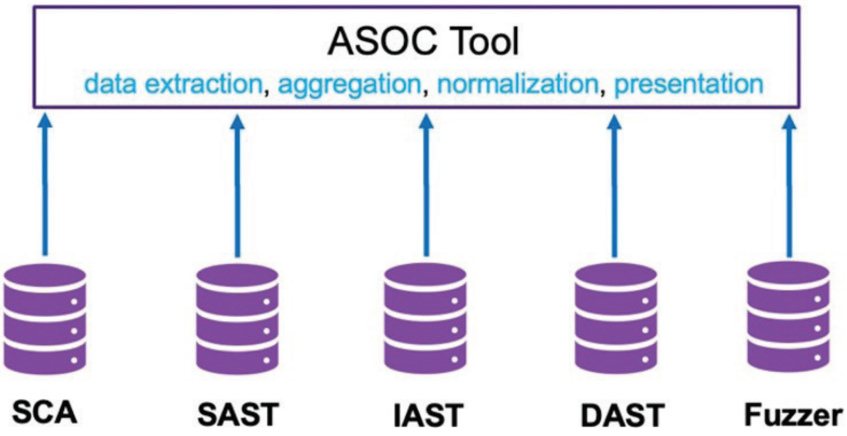


Figure 8 – ASOC Data Extraction, Aggregation and Normalization

Deployment

When we discuss the Deployment phase, the project version release package passes beyond the bounds of the DSO Software Factory. Nonetheless, landmark event that occurred during 2021 that will perhaps help us peer into the future of deployment to warfare assets be they at land, sea or air is perhaps worth consideration.

On January 6, 2021, the US Airforce deployed an AI to a U2 spy plane the defense contractor that participated in the effort credited DevSecOps for velocity of deployment with a security focus.

Data Protection

Much of the focus on the exploitability of software in the supply chain has been on software being used as the source vector for the exfiltration and loss of data in critical infrastructure and the defense sector. DoD's Cybersecurity Maturity Model Certification (CMMC), that is used to assess the protection of Controlled but Unclassified Information (CUI), is specified in DFARS 252.204 to assess controls specified in NIST SP 800-171. The Department of Homeland Security, in many ways having authority over critical infrastructure, has stated it will adopt a certification system similar to the CMMC.

From a supply chain perspective, software can be tested and evaluated to determine if it has weaknesses that represent source vectors for data leakage. In fact, through the Consortium for Information and Software Quality (CISQ), the Object Management Group is releasing the end of 2021 the Automated Source Code Data Protection Measure, based on 89 CWEs, any of which if present in the software, represent source vectors for unauthorized access to read or modify data. This specification covers common weaknesses (CWEs) that affect the protection of controlled or confidential information and data associated with intellectual property and privacy. Specifying this measure is important as a source of evidence for complying with laws and regulations such as in Europe the General Data Protection Regulation (GDPR) and in the United States the Cybersecurity Maturity Model Certification (CMMC). The key concept behind this is that software weaknesses can be identified and mitigated before they are used as source vectors for data leakage.

Summary:

In his work in industry the author has witnessed rapid adoption of DevSecOps methodologies across the defense sector in a short period of time; with a high focus on the frame of reference given by the Department of Defense. These projects have involved weapons systems, intelligence gathering and other assets across the domains, including naval warfare systems.

The author does not believe this defense industry increased velocity of change coinciding with cyber events and campaigns of a very public nature affecting national security of many nations is by chance. It seems inevitable that there has been a positive shift in the cyber security posture.

Many of the paradigms put into order by the DoD DevSecOps documentations suite were adopted from the private sector. The model, and in particular the DSO Software Factory, is being executed in practice and refined in the defense sector.

With the aforementioned exchanges of security principals in mind, it seems inevitable that many of the paradigms defined and outlined in the DoD DevSecOps 2.0 as well as the NIST and NTIA documents resulting from EO 14028 will cross-pollinate as inferred throughout this document.
Perhaps we have reached an inflection point increasing the national security of the United States of America and that of our allies and partners to meet the challenges forced on us all by aggressor nations and syndicates.

References

- Executive Order 14028 - https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
- NIST “Recommended Minimum Standards for Vendor or Developer Verification (Testing) of Software Under Executive Order (EO) 14028” - https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/recommended-minimum-standards-vendor-or
NTIA “The Minimum Elements for a Software Bill of Materials (SBOM) - https://www.ntia.gov/report/2021/minimum-elements-software-bill-materials-sbom
- DoD Enterprise DevSecOps 2.0 Strategy Guide - https://software.af.mil/wp-content/uploads/2021/05/DoD-Enterprise-DevSecOps-2.0-Strategy-Guide.pdf
- “Homeland Security Considering CMMC-like Compliance Effort”, Frank Konkel https://www.nextgov.com/cybersecurity/2021/08/homeland-security-considering-cmmc-compliance-effort/184561/
- “Heartbleed bug: How it works and how to avoid similar bugs”, https://www.synopsys.com/blogs/software-security/heartbleed-bug/
- Booz Allen Helps U.S. Air Force Give Flight to AI Copilot in the U-2 Dragon Lady, BusinessWire, https://www.businesswire.com/news/home/20210106005294/en/Booz-Allen-Helps-U.S.-Air-Force-Give-Flight-to-AI-Copilot-in-the-U-2-Dragon-Lady
- NIST 800-53 Rev 5 - https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
- Cybersecurity Maturity Model Certification – https://www.acq.osd.mil/cmmc
CISQ - Automated Source Code Measure for Data Protection - https://www.it-cisq.org/automated-source-code-measure-data-protection/index.htm
- Open Container Initiative – https://opencontainers.org/

Other References

- National Vulnerability Database – https://nvd.nist.gov
- Common Weakness Enumeration – https://cwe.mitre.org
- Common Attack Enumeration and Classification – https://capec.mtire.org
- DoD Enterprise DevSecOps Fundamentals - https://software.af.mil/wp-content/uploads/2021/05/DoD-Enterprise-DevSecOps-2.0-Fundamentals.pdf
- DoD DevSecOps 2.0 Fundamentals: Tools and Activities Guidebook.- https://software.af.mil/wp-content/uploads/2021/05/DoD-Enterprise-DevSecOps-2.0-Tools-and-Activities-Guidebook.pdf
- DoD DevSecOps 2.0 Fundamentals Playbook : https://software.af.mil/wp-content/uploads/2021/05/DoD-Enterprise-DevSecOps-2.0-Playbook.pdf
- NTIA SBOM Working Group - https://www.ntia.gov/sbom

Eric Hill has a BS in Computer Engineering from the University of New Hampshire and his career spanning nearly 3 decades. He has been involved with product development life cycle of telecommunications equipment and the advanced software that manages it. For nearly a decade he consulted in automation efforts on critical infrastructure. Today, Eric is a Technical Account Manager for Synopsys Software Integrity Group’s defense sector & federal customer base where he endeavors to provide industry thought leadership.

Maritime Cyber Risk and Global Security

by David Nordell
Synapse Cyber Strategy, Israel

The recent blockage of the Suez Canal by the container ship Ever Given in late March created an estimated loss to international trade of at least $10 billion per day. This blockage was apparently caused by poor seamanship as well as a sudden crosswind. But even our limited knowledge of cyber attacks at sea indicates that terrorists, criminals or even a nation state could deliberately cause a similar incident through a cyber attack on a vessel's control systems. Similarly, the cyber attack on Ukrainian networks in June 2017, which paralysed the global cargo management network of giant Maersk, not only cost the company at least $300 million, but created traffic jams of ships all over the world unable to dock and unload cargo. That incident was not a deliberate attack on Maersk, just collateral damage; but a terrorist or criminal group could deliberately cause similar havoc across the global shipping industry.

These and other relatively isolated cases indicate that shipping, ports and the data and control systems that connect them are a single global ecosystem vulnerable to cross-infection. This ecosystem is made up of the shipping companies themselves, their vessels, the ports and terminals, and all of the data systems managing and controlling the flow of containers, bulk freight, oil and gas not only at sea, but across the intermodal system. It also includes the hydrographic chart system that enables ships to know where they can navigate safely; and lastly the submarine cables that carry data not only for consumers and land-based businesses but also for the many ports, mainly in Africa, that don't have easy access to land-based telecoms infrastructure.

The global maritime industry is responding to the growing threat, with IMO cybersecurity guidelines, cyber classification rules for vessels, new insurance guidelines and most recently to guidelines just published by the International Association of Ports and Harbours. There is also a lot of new cyber-defence technology. But all these are probably not enough to prevent any deliberate large-scale cyber attack on the maritime world and massive economic damage, because there is a very big gap between guidelines or regulations and actual implementation.

The problem is mainly a civilian one. However, even though naval vessels and command structures tend to be better protected against cyber attacks, their global supply chains remains vulnerable, especially civilian ports. If NATO, or a national navy, needs to operate in open seas, let alone project military power and materiel like during the Gulf War, it may find its efforts sabotaged by cyber attacks. And, of course, NATO in Northwood also has a cell with some responsibility for overseeing the security of civilian shipping.

This whole paper is focused on an assessment of threat and vulnerability to cyber attacks in the extended maritime domain. I am deliberately avoiding detailed discussion of technical issues, both because there are other speakers here more expert than me, and because I believe that stakeholders, all the way up to national governments and the UN, need to take a more holistic view of the bigger picture in order to decide on policy priorities.

The level of threat to the global maritime ecosystem is increasing significantly. I would like to suggest several reasons for this.

First is the cyber-attack community as a whole. I don't necessarily mean the proverbial hackers in their hoodies looking for ways to earn some money from ransomware attacks or to get a thrill from a DDOS attack that paralyses some big company's servers. Cybercrime and cyber terrorism have become professionalised, with a lot of information and cyber weapons being shared and also sold across the dark web, and with nation states, such as China and Russia, not only building their own cyber armies that work 9 to 5 jobs in government offices, but also carry on freelancing in their own time, with the encouragement and even protection of the national government. Naturally, this overall group also includes proxies and false-flag actors. And in the same way as national intelligence organisations and large high-tech organisations have their own dedicated horizon scanners and R&D teams to develop and exploit intelligence insights, so do the better offensive cyber organisations. They read not only the news, but everything about maritime trade on the Internet, and by now they understand extremely well how vulnerable the maritime ecosystem is. They also know that even if most of the world isn't really aware of what happens at sea, and that big bank hacks or data breaches of consumer credit company have dominated the cybersecurity news, they can change this and create huge publicity and fear if they make another big container ship run aground in the Suez Canal, or stop a cruise ship from functioning in mid-ocean, with dead fresh water plant and food refrigeration threatening the health and lives of a few thousand passengers.

Next is the rapid digitisation and computerisation of this ecosystem and its growing dependence on the Internet and other communication infrastructures. We are already entering the age of semi- or fully autonomous vessels, not only for civilian trade but also for navies. We cannot assume that an autonomous vessel will behave exactly as programmed, because any system that can possibly be hacked will eventually be hacked. If the GPS infrastructure is hacked or spoofed – something that has already happened at least a few times, there is probably nobody on board who can correct the vessel's navigation using the good old-fashioned sextant and compass. In fact, this problem already exists on fully manned vessels where there is a fault in the ECDIS. It's easy to imagine, and to model, as situation in which any vessel heavily reliant on computerised systems – manned or autonomous, is hacked in order to ram other vessels, or run aground, or ram a jetty with container cranes sitting on it and thereby knock a whole terminal out of action. After all, these things have all happened already because of bad seamanship. Obviously, ships' ballast controls can be hacked to make the ship list seriously and even capsize, to say nothing of pumping out polluted ballast water.

Almost everything that can be made to go wrong with ships' controls can also happen shore side. Container cranes, as well as bunkering systems and bulk management systems, are now heavily computerised, with the most modern container cranes being managed on groups of up to about eight, by a single remote operator. Ports are also moving from manned container stackers to fully automated ones that can receive instructions from the port networks on where to stack containers just taken off a ship, or where to load them onto a train, truck or place them for movement to a ship. And, of course, a large port operation needs to store and manage many terabytes of data about which containers arrived on which vessel, from where, what they contain, special risks and now also electronic Bills of Lading. But all this sophistication creates great vulnerabilities. Location of container stacks depends on reliable GPS or ground-mounted RF beacons. We already know that GPS can be disabled or spoofed; and beacons are just relatively insecure OT gadgets that can also be hacked, typically using the new generation of 5G communications. The data needs to be stored securely, something we can't take for granted. Not only because the data can be wiped or become the target of ransomware: container operations are incredibly vulnerable to data manipulation. What if all the instructions for onward shore-side movement or trans-shipment of even a single ship's load of 20,000-odd TEU are deliberately scrambled by hackers so that every single container is sent to the wrong destination? Not only will there be massive financial damage but also reputation damage to the terminal company and perhaps the shipping company too.

It's also important to recognise that 5G in itself creates a whole range of cyber vulnerabilities, especially because its capabilities are ideally suited to networking all the systems of smart ports. Since this is a NATO conference, I think it is possible to be frank and acknowledge that the global domination by Huawei of the 5G market, not only for ground stations, but also for other devices using this protocol, presents a very grave risk to the global maritime industry if we reach any significant political or even economic conflict with China on one side.

The next point is the growing sophistication of technologies available for cyber attacks. Artificial intelligence is not only being used for defence, but very clearly for attack as well. Deep fakes can now be used, not only to fabricate identity photographs and videos, with suitable-sounding voices, but also to spoof telephone calls. For example, a British energy company was defrauded of 220 thousand Euros by a call that sounded as if it came from the CEO of its German parent company, complete with authentic accent and intonation, instructing it to transfer the money to a bank in Hungary. We can expect this kind of deep fake, even using fabricated video content, to be used for future frauds, not only to steal money from shipping companies and ports but also to give fake instructions to ships' masters ordering them to steer a course that will ground the vessel, or to download a last-minute software patch that actually infects the vessel's control systems, or even to take on unplanned passengers at sea who actually turn out to be hijackers.

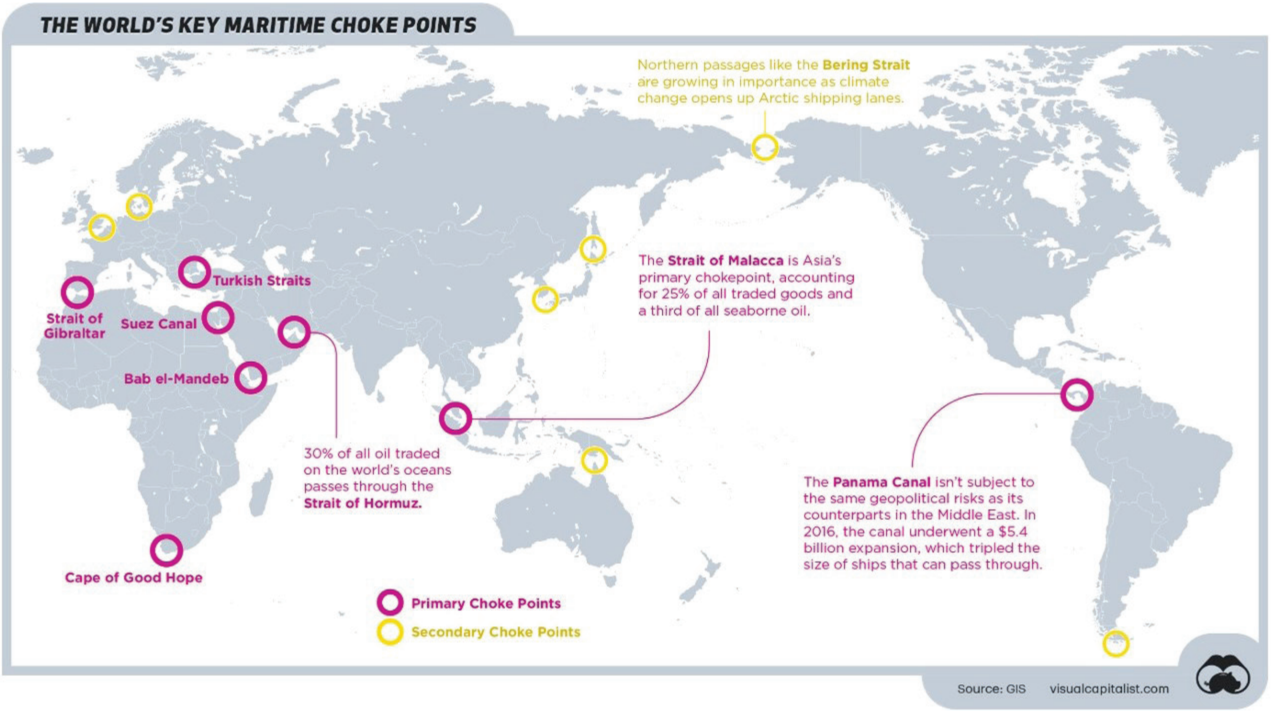
You have possibly seen the deep fake video someone produced of Barack Obama making a political speech. But what happens in the maritime domain if someone creates and publishes a deep fake pornographic video of the CEO of a major publicly-listed shipping company with a child? At the very least, it's going to make the board suspend the CEO pending a police investigation. But it's also likely to make the company's share price plummet for a while and affect the company's reputation.

More importantly, AI tools can be, and are already, used to enhance existing attack techniques, including scraping web sites for target e-mail addresses, controlling botnets and more.

Another tool that can be enhanced by AI is Shodan, the increasingly popular intelligence tool that can gather data on both IT and OT systems, using even satellite communication channels. If a hacker knows that a particular bit of equipment is vulnerable, he can actually search for implementations all over the world, including in ships, and methodically go about attacking them using AI for faster and more efficient data analysis.

So what does all this have to do with global security? I do think there are scenarios of maritime cyber attack that could lead to a war like what we witnessed post 9/11. But we are already facing other, less extreme and more likely situations. The first is the growth of ransomware used against both ships and ports. But ransomware is not just used to enrich individual hackers or criminal gangs. On the contrary, there is evidence that major ransomware attacks are being used to finance terrorist activity aimed at killing people and destabilising governments. Bear in mind that of the big four hostile cyber powers – China, Russia, Iran and North Korea – the last two are not noticeably responsible but support or even carry out terror attacks on their own or through proxies.

I mentioned the accidental blockage of the Suez Canal at the beginning of this paper. But that is only the most vulnerable of the world's maritime chokepoints because it's so narrow and relatively shallow. The 2017 Chatham House report on global trade chokepoints shows how more than half the world's basic food supply travels through 14 chokepoints, of which most are at sea. A deliberate cyber attack resulting in an oil freighter spilling its cargo that is then set on fire by a drone


THE WORLD'S KEY MARITIME CHOKE POINTS
Northern passages like the Bering Strait are growing in importance as climate change opens up Arctic shipping lanes.
Turkish Straits
Strait of Gibraltar
Suez Canal
Bab el-Mandeb
The Strait of Malacca is Asia's primary chokepoint, accounting for 25% of all traded goods and a third of all seaborne oil.
30% of all oil traded on the world's oceans passes through the Strait of Hormuz.
The Panama Canal isn't subject to the same geopolitical risks as its counterparts in the Middle East. In 2016, the canal underwent a $5.4 billion expansion, which tripled the size of ships that can pass through.
Cape of Good Hope
Primary Choke Points
Secondary Choke Points

Source: GIS visualcapitalist.com

could easily block the Bosphorus or the Strait of Gibraltar for long enough to cause a major disturbance to food supplies. And, by the way, a similar attack on the English Channel or cyber attacks on UK ports could do much the same, as the UK only has about five days of strategic food reserves.

China, incidentally, is also highly vulnerable to cyber attack on its ports or major shipping channels, which could in extreme circumstances could come from a country such as South Korea or Vietnam that feels threatened by Chinese maritime aggression.

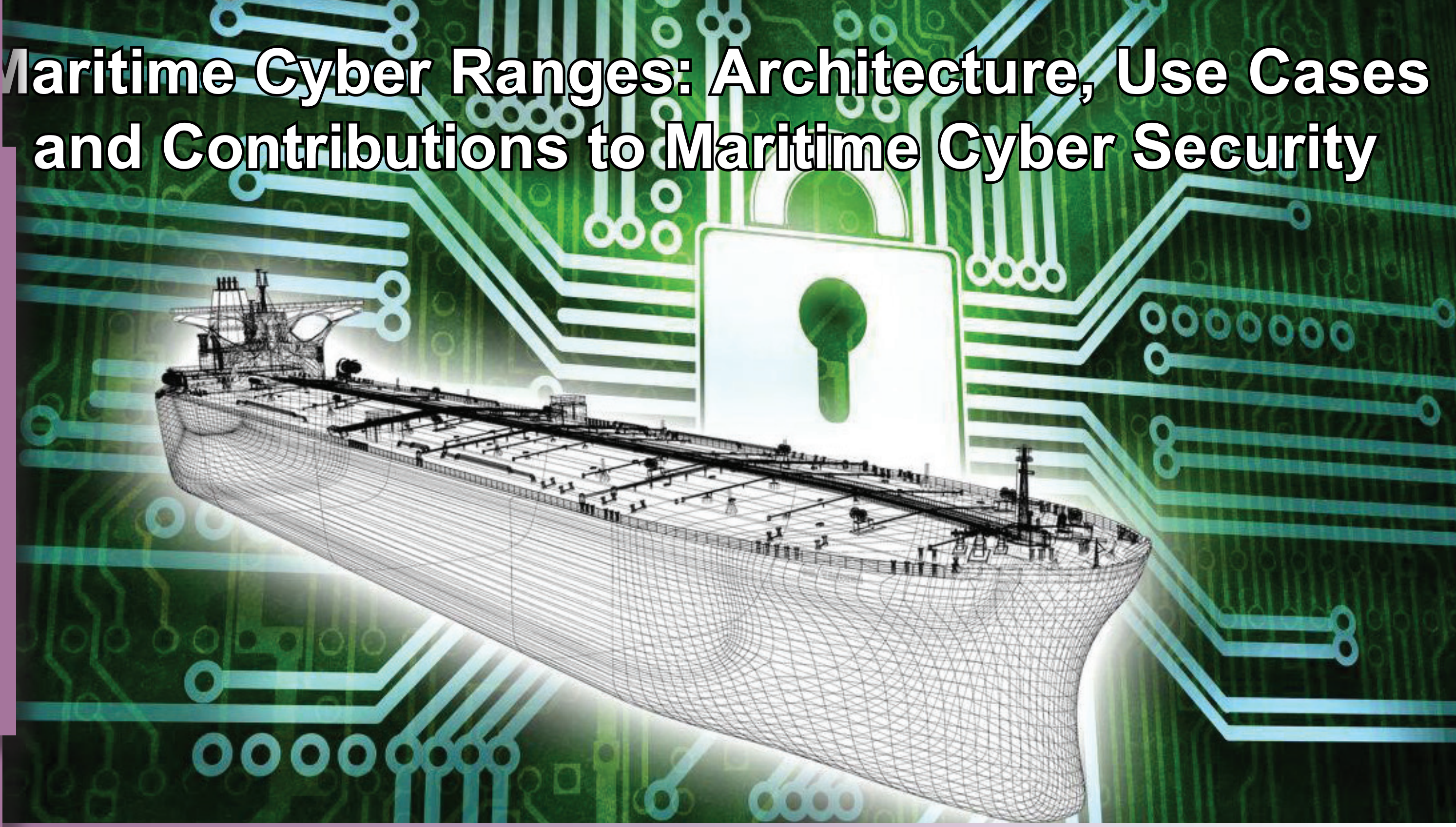
I'm not suggesting that such an attack on Western interests would immediately be interpreted as a casus belli resulting in a call on allies according to Article Five, as it's most unlikely that even a nation state responsible for the attack would admit responsibility. But it would certainly result in intensified intelligence activity looking for the responsible parties, and very possibly retaliation by and against sub-state actors, leading to escalation. Is this all fantasy? By no means, when we remember that a small but highly motivated terrorist group killed more than 3,000 civilians on 9/11 and set in motion twenty years of war in two different theatres, with NATO involvement.

In conclusion, I believe that we need to understand that maritime cyber attacks pose a very real, if not immediate, threat to regional or perhaps global security, although when or in what shape the threats manifest themselves remains unknown. I don't believe that all the new IMO and other regulations and guidelines, even those coming from as professional an organisation as the US Coastguard, will totally solve the problem, because implementation will take a very long time, and when it comes to operational technology, many not even be practicable. So we need national governments, the insurance industry and financial institutions to put as much pressure as possible on the industry stakeholders to implement better defences, including education and training, without delay.

What we also need is to put some serious effort into scenario planning, simulations and war games, including for crisis management, since we must assume that anything that can be hacked will be hacked. And, of course, NATO can play an important role in doing this.

David Nordell is an international cybersecurity and information strategy consultant based in Israel. He was senior vice president for strategy and policy for five years of the London-based international cybersecurity think tank, the Centre for Strategic Cyberspace and Security Science, and has spoken extensively at conferences around the world on cybersecurity, cyber crime and related topics. He was an invited expert to Chatham House (the Royal Institute of International Affairs) workshops on the cyber-security of space and on the US nuclear weapons command chain, and is also a member of Chatham House. He is a leading expert and thought leader on maritime cybersecurity, both shipping and ports; he spoken on this subject at the International Maritime Organisation, the UN Counter-Terrorism Executive Directorate and several industry conferences, and has also briefed the British government's National Cyber Security Centre on maritime cyber risk. He also chaired a conference on maritime cybersecurity as part of CyberTech, one of the largest cybersecurity conferences in the world. In addition, he has spoken at conferences about cyber risks to the financial industry (including briefing the risk officers of the International Financial Institutions), healthcare and pharmaceutical industries, the legal industry, and smart cities.
David is a member of the advisory board of an Israeli start-up developing technology for high-security tracking of shipping containers, and of the leading organisation of financial crime professionals, MLROs.com (Money Laundering Reporting Officers), as well as an editorial board member of the International Journal of Maritime Crime and Security, and of the Terror Finance blog.
David has a degree in civil engineering from the University of Southampton (UK) and served for three years in a reserve British Army special forces unit.
(https://www.linkedin.com/in/davidnordell/)

Maritime Cyber Ranges: Architecture, Use Cases and Contributions to Maritime Cyber Security



by Dr Olivier JACQ
CTO France Cyber MaritimeSynapse

Abstract

The hard work conducted by the maritime cyber security community over the last few years has led to promising first results. Tailored cyber security solutions, initiatives and organizations covering maritime public or private stakeholders needs, are progressively becoming a reality. However, long-haul actions still remain to be achieved to increase the maturity level on a wide spectrum of needs: initial and continuous education, training, research, dedicated cyber security solutions, secure architectures, pen testing or information sharing and realtime monitoring. When the time comes to implement those solutions, or when looking at future challenges, difficulties remain, mainly due to the peculiarities of the Information Technology (IT)/ Operational Technology (OT) systems of the sector and to the complexity of the overall architecture of a ship or harbour. Indeed, subjects like OT systems patch management, digital twins, secure architecture design, penetration testing or training are amongst difficult topics to implement for a maritime Chief Information Security Officer (CISO), a shipyard or a system integrator. In this article, we will present and detail the added value of maritime Cyber Ranges (CR) in such cases. Through three examples of maritime cyber ranges we currently use in France, we will detail the use cases and results of such assets to strengthen the cyber security level of our complex, yet critical sector.

Keywords: maritime, port, cyber security, cyber ranges, PLC

Introduction

In this first section, we will briefly describe our organization, France Cyber Maritime, its origins and different activities. We will then present the overall article organization.

About France Cyber Maritime

France Cyber Maritime is a non-profit organization, created in November 2020, backed by the French Secretary of the Sea (Secrétariat Général de la Mer, SGMer) and the French Information Security Agency (Agence Nationale de Sécurité des Systèmes d'Information, ANSSI) and with the initial support of over a dozen partners from both the public and private sectors. The organization is willing to contribute to increasing the resilience of maritime and port operations to cyber threats and develop a network of expertise in maritime cyber security. Three membership boards were created, one for administrations, state agencies and local authorities, the second for end users (operators of the maritime and port sectors) and finally, a third one for qualified providers of cyber security solutions. France Cyber Maritime also operates the Maritime Computer Emergency Response Team (M-CERT), to provide information and assistance to all maritime and port operators, in metropolitan France and French overseas territories, and internationally when needed. The M-CERT already analyses and shares regular bulletins on maritime cyber threats and tailored alerts to our constituencies, together with specific Indicators of Compromises (IoCs). The full operational capability of the organization is planned for 2023.

Article organization

In section 2, we will underline the peculiarities of maritime cyber security, the need for a tailored response, and the associated challenges. In section 3, we will present the characteristics and generic uses cases for cyber ranges, as well as their potential use to answer the needs of the maritime cyber security. In section 4, we will detail three maritime cyber security cyber ranges we are using in France, their use cases and the first return of experience. Before drawing the conclusion, underline the current limitations and the perspectives of development of these tools for the maritime community to better cope with future threats.

The call for maritime-tailored cyber ranges

In this section, we will underline the peculiarities of the maritime world, especially when at sea, and the underlying challenges when adapting traditional cyber security solutions to the maritime world.

The challenge of adapting cyber security solutions to the maritime world

Cyber security solutions providers developing solutions for the maritime and port sector commonly have to face a number of challenges when addressing the maritime sector. One of the frequent questions of cyber security Small and Medium Enterprises (SMEs) not accustomed to the maritime sector are: "how is the sector different from another one?". "Why would my products or processes be unsuitable to work on a ship?". "Is it so difficult to secure a ship from bow to stern?". The next round of questions often concerns the availability, on a medium to long term basis, of a representative and comprehensive ship platforms to perform pen tests, audits, or secure architecture work. The underlying common issue is: "how can we enhance our knowledge on maritime cyber security and test our solutions if we can't have a ship to practise or test?". In most cases, the answer is: there are few chances that the opportunity will be given to them to perform their tests on a real ship, except in a few cases where designers or pen testers of cyber security firm have a full access to an offshore platform or a ship. Indeed, it is understandable that maritime operators and stakeholders want to make sure that securing their IT and OT systems won't put the whole ship, port of offshore platform operations at risk. Another common issue is that a cyber security firm might have a full mandate to work on part of the ship's IT and OT, such as the satellite access only, the IT only, the OT or Industrial and Control Systems (ICS) only, but it is still quite rare that, especially on bigger ships, they have an access and a clear mandate to perform their work on really all systems.

Finally, we are also all aware that working a posteriori on securing a ship once she has been commissioned is a real challenge, sometimes made impossible due to the lack of knowledge on the full architecture of the ship. Those difficulties can be explained by industrial property issues, by the number of manufacturers involved, the lack of overall IT/OT and processes mapping, the lack of specialized human resources and low cyber security implementation. It is also still hard to add cyber security rules in many ship building or port overhaul contracts, due to the implementation price, to the number of applicable standards, regulations or rules and, simply, due to the lack of human resource workforce expertise and number, for instance in ICS or specific maritime OT hardening. Those challenges, to name a few, are delaying the possibilities to add in-depth cyber security features within a ship.

Impacts of the peculiarities and challenges of the maritime sector on cyber security

Even if several characteristics of port and ship IT and OT systems may sound familiar to people working in the industry, the addition of all peculiarities of the maritime and port sector have direct and challenging consequences for cyber security (Figure 1) [JBKS19].

Those peculiarities have consequences on cyber security implementation. On the connectivity point of view, the satellite constraints, in terms of truly available bandwidth for cyber use, but also speed, delays, costs and possible faults which have to be taken into account for instance in the design phase of a maritime Security Operations Center (SOC) [JBB+18]. Failing to do so may have consequences: loss of cyber metadata sent to shore, poor timeliness and freshness quality, troubles in the update of sensors signatures updates, patch management failures, impacts on overall bandwidth for other uses on board, etc. While the in-depth understanding of the onboard systems and protocols is essential to secure maritime architectures and mitigate cyber threats consequences, it is still quite usual to notice a relatively poor understanding of a ship overall architecture, strengths and weaknesses. Several factors can contribute to this: the ship may have been built by distant contractors, shipyards or integrators and subcontractors. This challenge can also be explained by the different interpretations of the term "architecture map" by the different parties. The consequence is mostly a "black box" effect, meaning that the SMEs working on enhancing onboard cyber security often have to start over with a major mapping process before any further work.

As the maritime community is aware, the patch management process on board a ship is also an important and actual challenge, to cope with the high monthly rate of vulnerability disclosures on IT and OT systems. Apart from the bandwidth constraints to send patches onboard, the biggest trouble is to make sure applying patches doesn't endanger IT and OT systems, especially when it comes to Cyber Physical Systems (CPS). Applying a critical Windows patch on an Electronic Chart and Display Information System (ECDIS) or on an ICS engineering station when at sea is prone to real world consequences. In the absence of regression-testing platform or "digital twin",the no-damage guarantee isn't often acquired, meaning patches will have to wait until the ship comes to a port of call where experts can come aboard and check for the absence of regression or, in many cases, be added to the ever-lasting postponement of applying patches.

Finally, when it comes to Operations and Human Resources, it might sometimes be complicated to correctly measure the impact of adding cyber security features or equipment onboard a ship. In the absence of cyber security experts on board, How will the Officer of the Watch (OoW), Electro Technical Officer (ETO) or captain react if they are alerted about a cyber attack going on? Will they take the proper measures? Is there any shore expert to help? Can they be trained or evaluated on their reaction depending on the type of cyber attack? How can they be helped in their decision to gain the state of knowledge of Maritime Cyber Situational Awareness (MCSA)? [Jac21]

Cyber ranges: definitions and possible maritime uses

In this section, we will first present the generic functions of cyber ranges, before describing their possible interest for the maritime domain.

Definitions

Cyber ranges have caught a high attention from the civil research and industry communities for the last ten years [DM13], and especially over the last five years, where the name itself has become widely used within the cybersecurity industry. However, one should not forget that such installations have existed at least over the last twenty years. Under the common name "cyber range", one should remember that there are, in fact, lots of different interpretations and implementations, depending on the users' needs and the manufacturer understanding and implementation. [UFH+20]

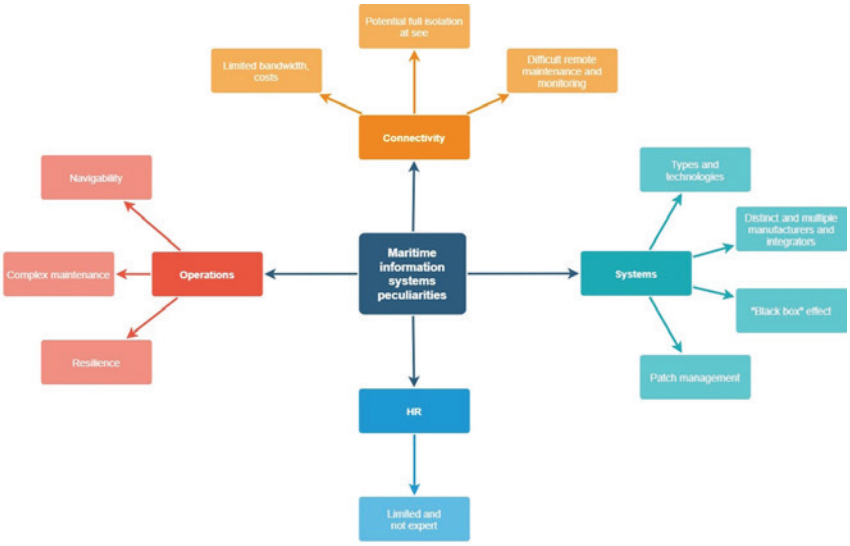


Figure 1: Unique characteristics of maritime information systems

While several definitions of a cyber range can be found in research work, most articles however refer to the definitiongiven by the US National Institute of Standards and Technology (NIST) in 2018: "Cyber ranges are interactive, simulated platforms and representations of networks, systems, tools and applications. They typically provide a safe, legal environment to gain hands-on cyber skills and a secure environment for product development and security-posture testing." [fCENCRPT18]

Indeed, cyber ranges use modern technologies such as simulation, emulation and virtualization to recreate a high-fidelity environment for cyber purposes. The achieved level of realism varies a lot, however: most cyber ranges remain generic, to meet the wide needs of most users, the most frequent situations and the most common technologies, but also to lower the cost which would be needed to reproduce the full complexity of an industrial installation, for instance. If this generic aspect increases the expected return on investment of the installation, it also reduces the likelihood that these CRs can be finally accepted by end users as truly representative of their daily IT and OT systems. Recent research articles on cyber ranges also confirm that CRs are predominantly used for training, education and awareness raising. [CKK+21] Training techniques, objectives and target audience vary from phishing awareness for end users to advanced exercises for red and blue teams or Capture The Flag (CTF) events. However, CRs capacities are much wider: they can also turn out to be very efficient tools for realistic data sets generations, machine learning work, patch management trials, secure architecture testings, or even for computer forensics purposes.

Cyber ranges for maritime needs

In Table 1, we cross the actual and future cyber security needs of the maritime sector and the potential use of cyber ranges to meet them. This short analysis underlines that maritime-tailored CRs could represent a relevant path to contribute to the identified maritime cyber security challenges.

Maritime Cyber Ranges Use cases

In this section, we detail three different civil cyber ranges currently used in France for maritime purposes within our constituencies.

French Naval Academy

The French Naval Academy is in charge of the initial education of navy officers. It also holds the Naval Cyberdefence Chair, created in 2014, where researches are conducted on many different subjects such as Maritime Cyber Situational Awareness, resilience and cyber events detection in the maritime context[1] .

Maritime context of use

In 2019, within the context of a European and regional project, the Academy created its Naval Cyber Range with two main goals: education and research. The development was later continued within the Foresight European H2020 project, aiming at developing an advanced cyber-security simulation platform for preparedness training in Aviation, Naval and Power-grid environments through the physical, logical and functional connection of the Naval Cyber Range with other industrial cyber ranges. The Naval Cyber Range is constituted of twenty Programmable Logical Controllers (PLCs) and related Human Machine Interfaces, reproducing the industrial processes of a medium-sized ship (Figure 2). A featured bridge was also created, with Global Navigation Satellite System (GNSS), Automatic Identification System (AIS) and Electronic Chart Systems (ECS). The overall cyber-range also comprises cyber sensors, cyber situational awareness elaboration processes, big data and visualization tools as well as user, kinematics and sensors/actuators life simulation.

Maritime cyber security challenges	Potential values of cyber ranges
Awareness, training and certification	Used with orchestrators and Learning Management Systems (LMS) and tailored to maritime needs, CRs can represent an asset in terms of training and certification.
Education	Maritime and Navy officers and ETOs can highly benefit from CRs to better assess risks.
Secure architecture	CRs can help SMEs designing and testing secure architectures for ports and ships.
Patch management	When representative of an actual IT/OT system, CRs can be used for shore patch testing and qualification prior to deployment.
Data sets generations	Maritime CRs can be high-value assets to generate datasets for research and intrusion detection purposes.
Intrusion detection and monitoring	CRs can contribute to the efficient design of maritime cyber monitoring architectures.
Pen testing	CRs can be used for pen testing, or for red team assets training on maritime IT/OT.
Computer forensics	CRs can contribute to the reproduction of a compromised IT/OT system for forensics operations.
Cyber security assessment and certification	CRs can contribute to cyber security and certification assessment with a reduced cost compared to the interruption of ships operations.
OT hardening	CRs can reproduce a complete OT system and ease its hardening by cyber security experts.
Cyber Threat Intelligence (CTI) implementation	CRs can help in the design of a complete ship / shore CTI infrastructure, for instance to implement maritime Computer Emergency Response Teams (CERTs) loCs on onboard sensors.
Autonomous ships	Modeling autonomous ships and vessels on a CRs will ease risk assessment and pen testings.
Risks and threats modeling	CRs are helpful tools for Dynamic Risk Assessment (DRA) and to build comprehensive threat infrastructures for research and investigation.
Mitigation implementation and testing	CRs can contribute to the implementation of mitigation measures to evaluate their safety and results.
Digital Twins	CRs can contribute to Digital Twins technologies and reproduce *in vivo* maritime IT/OT systems.
Maritime Cyber Situational Awareness	MCSA elaboration and its abstraction level can be modeled on tailored maritime CRs.

Table 1: Needs of the maritime sector and possible use of tailored maritime cyber ranges

Results and perspectives

The cyber range is fully operational: researchers working on maritime cyber topics are using the data sets generated by the CR for their data analysis, anomaly detection works, and deception research. Students of the Post Master's degree in maritime and port cyber security also use the cyber range during their courses to better understand the vulnerabilities – and strengths – of maritime IT/OT, and experiment on topics such as AIS or GNSS spoofing and jamming in a secure dedicated environment. In the future, within the Foresight project, the Cyber Range will be connected to other industrial cyber ranges in order to simulate whole parts of industrial sectors which can be found in a country, or at a European level. The Naval Cyber Range could also soon be connected to other maritime cyber ranges to create an interesting fleet of heterogeneous vessels for education and training purposes.

[1] https://www.chaire-cyber-navale.fr

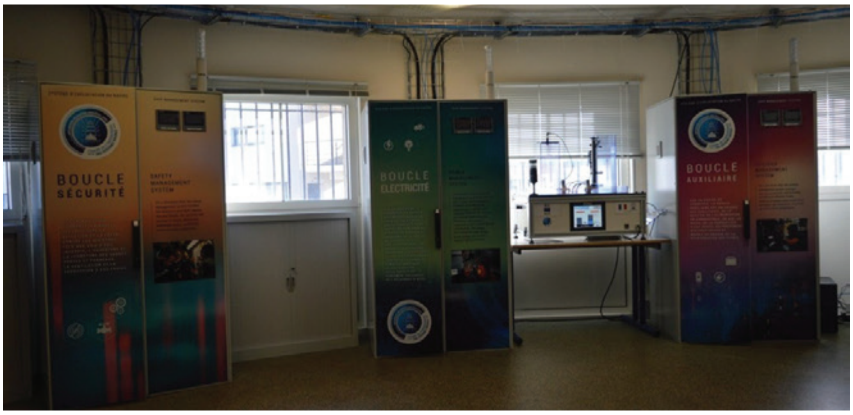


Figure 2: Overview of three of the four industrial loops of the Naval Cyber Range (source: personal work)

DIATEAM Cyber Range

DIATEAM is a French SME specialized in the design of hybrid cyber ranges[2]. Based on initial needs by the French Ministry of Defense (MoD) in 2002, its cyber ranges are now present within the industry, education and military sector, in France and abroad.

Maritime context of use

After a first experience in the naval context, DIATEAM has further been involved within the maritime community within the context of the European H2020 project Cyber-MAR. This project aims at developing cyber security simulation environment for accommodating the peculiarities of the maritime sector with the view to fully unlock the value of the use of cyber range in the maritime logistics value chain. DIATEAM Cyber Range is, before all, a cyber range framework constituted of diverse virtualization or emulation mechanisms but also of added-value components, such as Learning Management Systems, orchestrators, dedicated Human Machine Interfaces and hybrid interfaces. This physical and logical framework enables for the reproduction of IT and OT systems and hybrid interconnections to physical Programmable Logical Controllers, which can also be virtualized. Within the Cyber-MAR H2020 project, this CR has made it possible to reproduce the complex smart grid infrastructure of a major port to conduct both offensive (red team) and defensive (blue team) operations. The scenario architecture was detailed in [JSP+21] and its video footage is available online[3]. The maritime CR has now developed, with many new maritime IT and OT systems (satellite telecommunication systems, bridge displays, ECDIS, weather sensors, etc.). Those physical systems were integrated in the CR to enable live data to flow within the CR and to avoid an over rated use of simulated data and equipments.

Results and perspectives

The cyber range is fully operational and is today widely exploited within the Cyber-MAR project, but also for the benefit of the students of the Post Master's degree in maritime and port cyber security. Given the high level of integration of real maritime OT systems, recent interests have shown relative to maritime data sets generation with regard to intrusion detection and machine learning algorithm training and maritime digital twins design. Future plans are to connect DIATEAM's maritime Cyber Range features to other maritime cyber ranges in France and abroad to unlock advanced scenarios design and to create fleets of vessels. Upcoming remote access to the LMS, the orcherstrator and maritime topologies will be of high interest for the maritime and port sector.

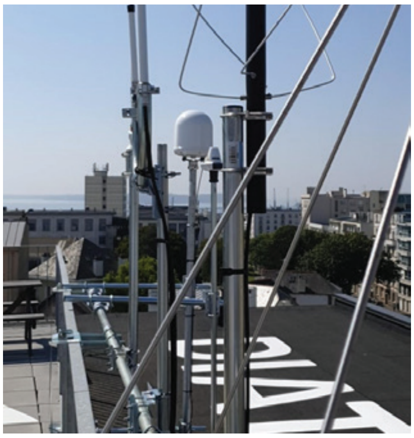


Figure 3: Part of the antennas at DIATEAM's maritime cyber range (source: personal work)

French Maritime Academy

The French Maritime Academy (École Nationale Supérieure Maritime, ENSM) is responsible for the initial and continuous education of maritime officers and ETOs. The academy has also developed a research department with a specific focus on maritime cyber security. Its main research projects concern Unmanned Surface Vehicles (USV) cyber security, with the Sea4M project[4].

Maritime context of use

The academy has acquired a maritime cyber security platform, called MARINS. MARINS is a STCW-compliant full mission bridge simulator dedicated to maritime cyber security research activities. It is composed of real physical commands, automatic pilot and NMEA-compliant equipment within a highly realistic 3D environment (Figure 4). A dozen operational cyber scenarios were created on the simulator to reproduce feared events. Another interesting subject concerns the human factor, with researchers looking for crew stress consequent to cyber attacks, for which trainees can be equipped with eye tracking, EEC and ECG sensors.

[2] https://www.diateam.net/what-is-a-cyber-range

[3] See https://www.youtube.com/watch?v=7dUEBOc_Gik&ab_channel=CyberMAR

[4] https://www.supmaritime.fr/en/sea4m/

Results and perspectives

ENSM is also part of a H2020 project called ISOLA aiming to "develop, integrate, test, deploy, demonstrate and validate asystematic and fully automated security approach by incorporating innovative technologies for sensing, monitoring, data fusion, alarming and reporting real-time during illegal incidents".

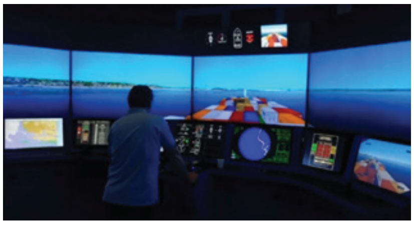


Figure 4: Overview of the MARINS cyber security research platform. Source: ENSM

Conclusion

In this article, we have underlined the possible uses of tailored CRs to contribute to the maritime sector cybersecurity. We have demonstrated that these CRs can represent highly added-value assets when it comes to addressing the major cyber security challenges we encounter. The three cyber ranges we detailed have generated a lot of interest, both from the maritime and port actors, but also from the cyber security sector. Still, a lot of work remains to be achieved in the years to come. The first main aspect will be to interconnect maritime cyber ranges between them, on a European and international level, to leverage their capacities and usage. The second step will be to continue the integration of real maritime and port IT and OT assets for added realism and expertise. The third step will probably concern autonomous ships and vessels integration on CRs. In our opinion, the numerous possibilities offered by maritime cyber ranges do widen the possible answers to maritime cyber security challenges and deserve more attention and experimentation. attention and experimentation.

References

- [CKK+21] Nestoras Chouliaras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. Cyber ranges and testbeds for education, training, and research. Applied Sciences, 11(4):1809, 2021.
- [DM13] Jon Davis and Shane Magrath. A survey of cyber ranges and testbeds. 2013.[fCENCRPT18] The National Initiative for Cybersecurity Education (NICE) Cyber Range Project Team. The cyber range: A guide – guidance document for the use cases, features, and types of cyber ranges in cybersecurity education, certification and training. 2018.
- [Jac21] Olivier Jacq. Real-time detection, contextual analysis and visualisation of cyber-attacks: elaboration of the Maritime Cyber Situational Awareness. PhD thesis, Ecole nationale supérieure Mines-Télécom Atlantique, 2021.
- [JBB+18] Olivier Jacq, Xavier Boudvin, David Brosset, Yvon Kermarrec, and Jacques Simonin. Detectingand hunting cyberthreats in a maritime environment: Specification and experimentation of amaritime cybersecurity operations centre. In 2018 2nd Cyber Security in Networking Conference(CSNet), pages 1–8. IEEE, 2018.
- [JBKS19] Olivier Jacq, David Brosset, Yvon Kermarrec, and Jacques Simonin. Cyber attacks real time de-tection: towards a cyber situational awareness for naval systems. In 2019 International Conference on Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA), pages 1–2, 2019.
- [JSP+21] Olivier Jacq, Pablo Giménez Salazar, Kamban Parasuraman, Jarkko Kuusijärvi, Andriana Gkaniatsou, Evangelia Latsa, and Angelos Amditis. The cyber-mar project: First results and perspectives on the use of hybrid cyber ranges for port cyber risk assessment. In 2021 IEEE International Conference on Cyber Security and Resilience (CSR), pages 409–414, 2021.
- [UFH+20] Elochukwu Ukwandu, Mohamed Amine Ben Farah, Hanan Hindy, David Brosset, Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. A review of cyber-ranges and test-beds: Current and future trends. Sensors, 20(24):7148,2020.

- The Cyber-MAR, Foresight and ISOLA projects have received funding from the European Union's Horizon 2020 research and innovation program under grant agreements No. 833389 (Cyber-MAR), 833673 (Foresight) and 883302 (ISOLA). Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

Olivier JACQ is a former LT CDR within the French Navy. He has been assigned, over the last 20 years, in many positions related to maritime cybersecurity for ports, ships and operations. He has worked on many subjects such as maritime cybersecurity awareness, education and training, has designed maritime cyber ranges architectures, developed and deployed intrusion detection systems and conducted forensics activities. He was also assigned at the French Naval Academy's cyber defense chair, where he conducted research activities on Maritime Cyber Situational Awareness.

Olivier JACQ has a PhD in computer security from the Institut Mines Telecom and the French Naval Academy, a Post-Master's Degree in Cybersecurity from Ecole Centrale and a computer security degree from the French Information Security Agency (Agence Nationale de Sécurité des Systèmes Information). He is currently Chief Technical Officer at France Cyber Maritime non profit organization, where he is in charge, amongst others, of the development of maritime cybersecurity awareness programs and of the Maritime Computer Emergency Response Team.

A Proposed Cyber Security Certification Scheme for Supply Chain Services

by Nineta Polemi[1,2], Department of Informatics, University of Piraeus
Alexandra Michota[1,3], Department of Informatics, University of Piraeus
Sotiris Ioannidis[4], Technical University of Crete

Abstract — In this paper we outline the main elements of the proposed Cybersecurity Certification Scheme for Supply Chain Services (SCS) as proposed by the EC project CYRENE [1]. The proposed CYRENE-EUSCS scheme used the published European Cybersecurity Certification scheme [2] as a template and the proposed EU scheme for cloud services [3] as an example. The CYRENE-EUSCS scheme aims to enhance the level of security of the SCS components including: business partners, processes/sub-processes, physical and cyber assets (hosted by different business partners).

Keywords—Supply Chain Service, European Cybersecurity Certification, Security, Conformity Assessment, Assurance

Introduction

The EU regulation 2019/881, known as Cybersecurity Act (CSA) [4] for cybersecurity certification, seeks to prevent market fragmentation and to make it easier for users to know to what extent ICT products (systems, devices, services, processes) are secure. The certification will attest that ICT products are certified in accordance to their schemes and comply with specified cybersecurity requirements. The proposal of NIS Directive 2.0 [5] contains measures for improving cybersecurity infrastructure; one of the key elements of the Commission's proposal is to address the security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in supply chains and supplier relationships. Cybersecurity certification of the SCS can be considered as a mitigation action against cybersecurity SCS risks.

CYRENE's EUSCS scheme is using the European Cybersecurity Certification scheme, EUCC as a template and the EU scheme for cloud services, EUCS but will also incorporate the notion of the escalating vulnerability assessment level in bond with the different assurance levels. More specifically, the higher the assurance level will be, the deeper the vulnerability analysis will be performed. Users of the scheme may be supply chain service providers who wish to assess the security of their supply chain services through third-party certification. They can use the EUSCS scheme:

- to assess how a supply chain service meets the requirements of a predefined set of security control objectives and a related set of measures, when used according to security recommendations provided by the business partners and agreed by them;
- to provide business partners the information required to make informed choices about the procurement and operation of supply chain services (including processes, assets, technologies and operators involved in the provision of the supply chain services), and to allow business partners to use certified supply chain services in their own development activities, and to meet their own security compliance requirements.

The paper is structured as follows: Section II presents the state of play of the cybersecurity certification in the European Union (EU). In section III, the relevant standards we

[1] Department of Informatics, University of Piraeus, Karaoli and Dimitriou Str. 80, 18534 Piraeus, Greece
[2] Trustilio B.V., Vijzelstraat 68, 1017HL Amsterdam, The Netherlands, cdpolemi@gmail.com
[3] FOCAL POINT SPRL, Avenue D'iena 11, 1410 Waterloo, Belgium, amichota@focalpoint-sprl.be, amichota@unipi.gr
[4] Technical University of Crete, University Campus, Akrotiri, 73100 Chania, Greece, sotiris@ece.tuc.gr

considered for preparing the CYRENE-EUSCS are described. In section IV, the assurance levels offered by the scheme are introduced. Section V presents the evaluation method and criteria defined in security objectives and requirements set for supply chains. Rules for compliance monitoring of SCSs security requirements are analysed in Section VI while Section VII presents the vulnerability handling and disclosure process. Finally, section VIII draws the conclusions of the current work and presents our future research directions.

Cybersecurity Certification in the EU

The EU cybersecurity certification is defined as a comprehensive set of rules, technical requirements, standards, and procedures that are established at the Union level and that apply to the certification or Conformity Assessment (CA) of specific ICT products. Each certification scheme shall specify the categories of products and services covered; the cybersecurity requirements that need to be met -such as standards or technical specifications-, the type of evaluation that is planned to be - done such as self-assessment or third party - and the intended level of assurance that is going to be achieved. The certificates will be valid across all Member States (MSs)

The EUCC

The EUCC will serve as a template to propose security certification schemes for ICT products. The EUCC scheme is based upon Article 54 of the CSA. The latter presents in detail the key elements that an EU certification scheme shall include.

Using the EUCC, any ICT product can serve as a Target of Evaluation (ToE) and can be the subject of a security evaluation also known as conformity assessment (CA) in which it is assessed against security requirements. The CA of the ToE is defined as the procedure that is followed for evaluating whether specified requirements relating to the ToE have been fulfilled. That being said, throughout the CA process, the ToE should be identified and security aspects should be concretely specified. The EUCC presents the key elements (e.g. category of product, cybersecurity requirements, standards, conformity assessment) that EU certification schemes shall include in all sectors. In this paper, the SCS is presented as a ToE for a CA process and based on the CC the security and assurance requirements for a SCS certification are identified. The SCS-ToE can be described from a business view (describing only the interconnected business partners and processes), the holistic technical view (capturing in addition all the physical and cyber assets participating in the SCS-processes) and the sector-specific technical view (snap-shot of the technical view that an individual partner adopts) [6], [7]. For preparing the CYRENE-EUSCS, the EUCC was utilised as a template and the EUCS as an example. The risk-based identification of security and assurance requirements described in the methodology for sectoral cybersecurity assessments by ENISA was also used for preparing the CYRENE-EUSCS [8].

Use of Standards

The scheme proposes compliance with the following standards depending on the assessment we need to conduct.

- **For risk assessment**, ISO 2700x series of standards [9] also known as Information Security Management System (ISMS) Family of Standards is proposed. This helps organisations to develop and implement a framework in order to manage information security risks and controls of their information assets as well as to prepare themselves to assess it.
- **For conformity assessment**, ISO 15408 [10] and ISO 18045 [11] are proposed. ISO/IEC 15408 also known as Common Criteria (CC) establishes the concepts, principles and techniques for IT security evaluation. ISO/IEC 18045:2008 is a companion standard of ISO/IEC 15408 and provides a methodology to help an IT security evaluator conduct a CC evaluation by defining the minimum actions to be performed.
- **For SCS risk assessment**, ISO 2800x series of standards [12] was utilised. These standards were used to capture the requirements that need to be addressed by the organisations in order to establish a management system to assure the quality or security of the aspects involved in the supply chain industry. When it comes to security controls, even though the ISO/IEC 27005 [13] and ISO 28000 series provide a very good basis they could not fully encapsulate the details for the present scheme. Having said that, the proposed scheme also considered other families of standards such as NIST's SP 2000 [14] which provide more focused controls for Federal supply chains extending the scheme application directives.

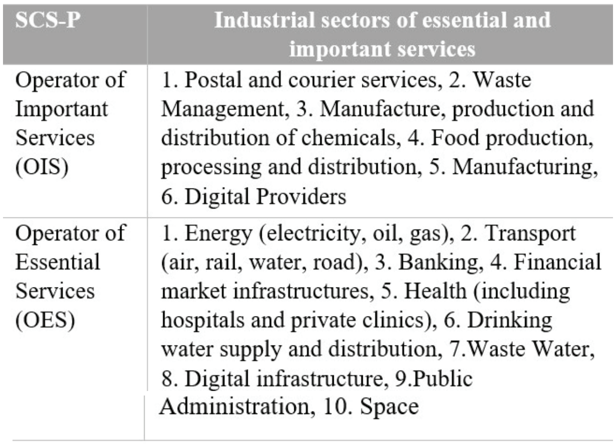
We consider the interplay and compliance of these standards to simplify the evaluation process.

CYRENE proposed the development of an Information Security Management System (ISMS) for the SCS based on ISO2800x and ISO2700x. An online certified SCS-ISMS will be operated by the SCS provider in collaboration with the business partners and it will support the SCS risk and conformity assessment processes. In particular the SCS-ISMS can be a useful tool to the SCS provider and business partners to perform their risk assessment and update their SCS-security policy and the SCS Protection Profile (PP) with all security requirements. The SCS-ISMS can also be used by the accessor during the conformity assessment process to find the necessary evidence to assess the security requirements (claims in the SCS-PP) and evaluate the controls implemented if they meet the corresponding security requirements throughout specified period.

Assurance Levels

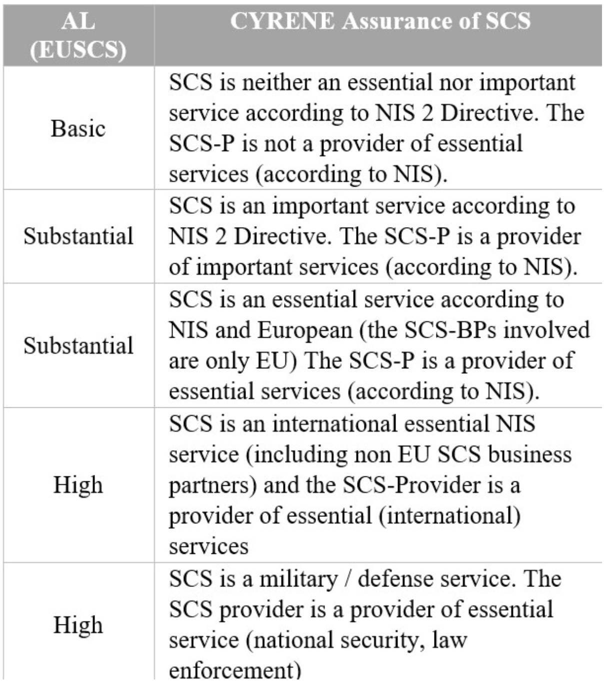
CYRENE-EUSCS covers a wide range of security requirements, by offering all three (3) security assurance levels (AL) defined in the EUCSA (basic, substantial, and high). The AL of the SCS depend on how important or essential a SCS can be according to NIS 2 directive. In particular, Table I below shows a mapping of SCS Provider (SCS-P) to the industrial sectors of essential and important services where Table II a mapping of the ALs based on the SCS criticality.

TABLE I
MAPPING SCS-P TO THE INDUSTRIAL SECTORS



SCS-P	Industrial sectors of essential and important services
Operator of Important Services (OIS)	1. Postal and courier services, 2. Waste Management, 3. Manufacture, production and distribution of chemicals, 4. Food production, processing and distribution, 5. Manufacturing, 6. Digital Providers
Operator of Essential Services (OES)	1. Energy (electricity, oil, gas), 2. Transport (air, rail, water, road), 3. Banking, 4. Financial market infrastructures, 5. Health (including hospitals and private clinics), 6. Drinking water supply and distribution, 7.Waste Water, 8. Digital infrastructure, 9.Public Administration, 10. Space

TABLE II
MAPPING EUSCS ALS TO THE SCS



AL (EUSCS)	CYRENE Assurance of SCS
Basic	SCS is neither an essential nor important service according to NIS 2 Directive. The SCS-P is not a provider of essential services (according to NIS).
Substantial	SCS is an important service according to NIS 2 Directive. The SCS-P is a provider of important services (according to NIS).
Substantial	SCS is an essential service according to NIS and European (the SCS-BPs involved are only EU) The SCS-P is a provider of essential services (according to NIS).
High	SCS is an international essential NIS service (including non EU SCS business partners) and the SCS-Provider is a provider of essential (international) services
High	SCS is a military / defense service. The SCS provider is a provider of essential service (national security, law enforcement)

As specified in the EUCSA's Article 52(5), assurance level **Basic** is "intended to minimise the known basic risks of incidents and cyberattacks" and can be further defined as follows: AL Basic should provide limited assurance that the SCS is built and operated with procedures and mechanisms to meet the corresponding security requirements at a level intended to minimize the known basic risks of incidents and cyberattacks. AL Basic should be suitable for SCS components that are designed to meet typical security requirements on services for non-critical data and systems. The typical attacker profile for AL Basic should be a single person with basic scored profile [15], [16] where necessary traits (capabilities, objectives, motives, resources, psychological and behavioural) are limited; for example the hacker cannot repeat a known attack but can perform social engineering attacks. The evaluation scope for AL Basic shall be defined by the description of the SCS and by the security objectives and requirements pertaining to assurance level Basic. The evaluation depth for AL Basic shall be driven by a predefined audit plan.

As specified in the EUCSA's Article 52(6), assurance level **Substantial** is "intended to minimise the known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources" and can be further defined as follows:

AL Substantial should provide reasonable assurance through evaluation by an assessor that the SCS is built and operated with procedures and mechanisms to minimise known cybersecurity risks, and the risk of incidents and cyberattacks carried out by actors with limited skills and resources. The assessor shall determine that the SCS provider has assessed those risks and implemented suitable controls that, if operating effectively, minimize those risks and meet the corresponding security requirements throughout a specified period.

AL Substantial should be suitable for SCS that are designed to meet typical security requirements on services for business-critical data and systems.

The typical attacker profile for AL Substantial should be a person(s) with a moderate score profile where most necessary traits are substantial; in particular substantial traits include the hacking abilities and access to a wide range of known hacking techniques such as penetration testing, including social engineering, but with limited resources, in particular to launch wide attacks or to discover previously unknown vulnerabilities.

The evaluation scope for AL Substantial shall be defined by the description of the SCS and by the security objectives and requirements pertaining to assurance level Substantial.

The evaluation depth for AL Substantial shall include, in addition to the requirements for assurance level Basic, on-site audit including interviews and inspecting samples, plus a verification that the implementation follows the specified processes and design, including the validation of the functional tests performed on that implementation.

As specified in the EUCSA's Article 52(7), assurance level High is "intended to minimise the risk of state-of-the-art cyberattacks carried out by actors with significant skills and resources" and can be further defined as follows:

AL High should provide reasonable assurance through evaluation by an accessor that the SCS is built and operated with procedures and mechanisms to minimise the risk of state-of- the-art cyberattacks carried out by actors with high score profile. The accessor shall determine that the SCS provider has assessed those risks and implemented suitable controls that operated effectively to minimize those risks and meet the corresponding security requirements throughout a specified period.

Assurance level High should be suitable for SCS that are designed to meet specific (exceeding level'substantial') security requirements for critical SCS services (e.g. military, financial sectors).

The typical attacker profile for assurance level High should be a person or a team of persons with a high score profile, most traits are highly scored, in particular the capabilities and resources with access to significant resources to design and perform attacks, get insider access, discover or buy access to previously unknown vulnerabilities.

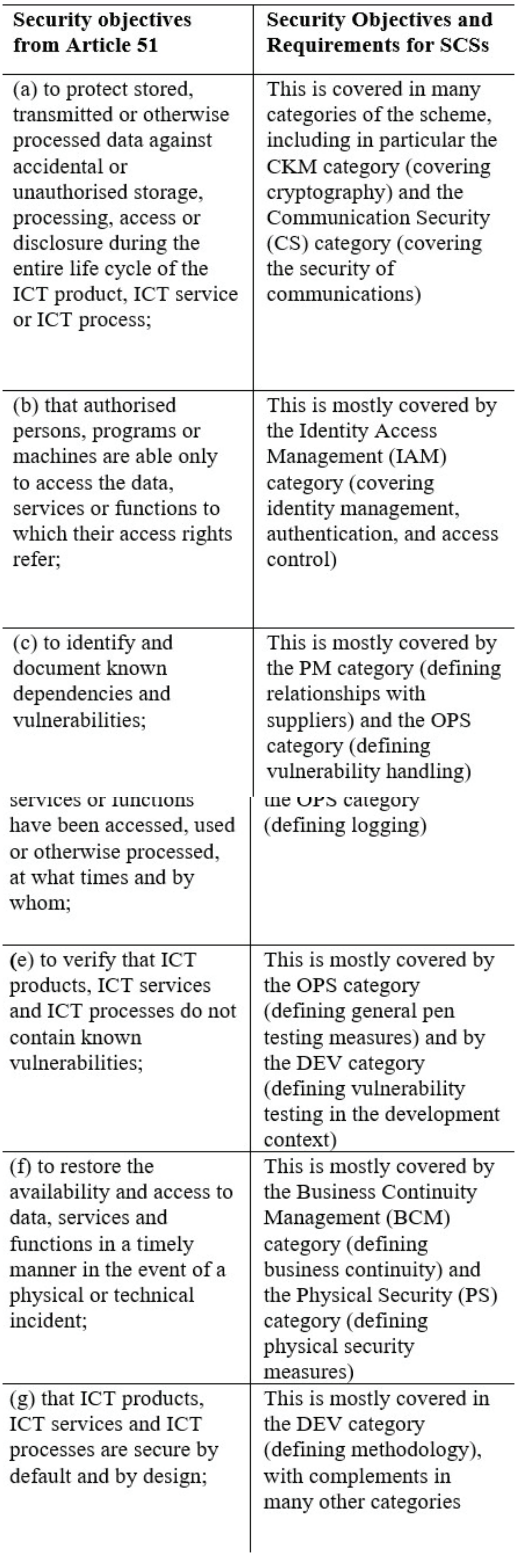
The evaluation scope for assurance level High shall be defined by the description of the SCS and by the security objectives and requirements pertaining to assurance level High. The evaluation depth for assurance level High shall be driven by a full justification of the coverage for all mappings, including for processes. It may also include higher expectations for some processes and their implementation, as defined in the security controls pertaining to AL High. Finally for assurance level High SCS: the attack paths need to be concretely modelled, the propagation of the vulnerabilities need to be estimated.

Evaluation Methods and Criteria

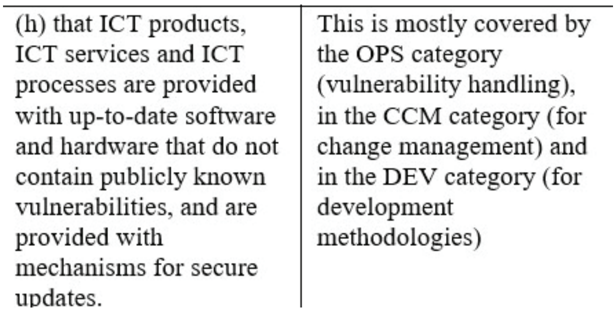
The EUSCS scheme uses a set of evaluation criteria defined in security objectives and requirements set for Supply Chains. The EUSCS assessment methodology is based on the ISO17065 standard [17]. This methodology defines two assessment approaches that may be used by accessors:

- An assessment approach that may be used for ALs Substantial and High. This approach is inspired from both the ISO17021 [18] standard and the ISAE family of

TABLE III
COVERAGE OR ARTICLE 51 BY REQUIREMENT CATEGORIES



Security objectives from Article 51	Security Objectives and Requirements for SCSs
(a) to protect stored, transmitted or otherwise processed data against accidental or unauthorised storage, processing, access or disclosure during the entire life cycle of the ICT product, ICT service or ICT process;	This is covered in many categories of the scheme, including in particular the CKM category (covering cryptography) and the Communication Security (CS) category (covering the security of communications)
(b) that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer;	This is mostly covered by the Identity Access Management (IAM) category (covering identity management, authentication, and access control)
(c) to identify and document known dependencies and vulnerabilities;	This is mostly covered by the PM category (defining relationships with suppliers) and the OPS category (defining vulnerability handling)
services or functions have been accessed, used or otherwise processed, at what times and by whom;	the OPS category (defining logging)
(e) to verify that ICT products, ICT services and ICT processes do not contain known vulnerabilities;	This is mostly covered by the OPS category (defining general pen testing measures) and by the DEV category (defining vulnerability testing in the development context)
(f) to restore the availability and access to data, services and functions in a timely manner in the event of a physical or technical incident;	This is mostly covered by the Business Continuity Management (BCM) category (defining business continuity) and the Physical Security (PS) category (defining physical security measures)
(g) that ICT products, ICT services and ICT processes are secure by default and by design;	This is mostly covered in the DEV category (defining methodology), with complements in many other categories



(h) that ICT products, ICT services and ICT processes are provided with up-to-date software and hardware that do not contain publicly known vulnerabilities, and are provided with mechanisms for secure updates.	This is mostly covered by the OPS category (vulnerability handling), in the CCM category (for change management) and in the DEV category (for development methodologies)

standards IAASB Handbook [19]

- An assessment approach that may be used solely for assurance level Basic.

CSA highlights that a European cybersecurity certification scheme shall contain evaluation criteria and methods capable of demonstrating the security objectives of article 51. Following the methodologies, Table III below provides a high-level vision based of the coverage of Article 51 requirements by presenting specific security objectives and requirements defined for SCs.

Compliance Monitoring

This section describes the rules for monitoring compliance of SCSs security requirements with the ones described by the proposed CYRENE-EUSCS proposed scheme. The requirements met in these rules tend to prevent a set of non-compliant applications and conditions, including but not limited to, the satisfaction of obligations in the context of the SCS certificate, the identification of major security incidents that could potentially lead to a data breach or leak of sensitive information, and the identification of existing or new vulnerabilities with adverse impact upon the SCS security mechanisms. The assessment of the SCS service will be conducted either by an independent accessor (for Assurance Level Basic SCS) or by a CAB (for Assurance Level Substantial/High SCS).

Non-compliance elements:

- Information mismatch between the supplied version of the certificate to the assessor and the version which has been established in the currently running environment.
- Deviation in the requirements met within a certificate content and the supplementary information required for that certification in terms of its format, documentation, and management aspects.
- Irregularities regarding the certification validity requirements including the inability to proceed with maintenance activities, enforce the supplied terms and conditions of the certificate, or deviate from the certified development and operating services.

Vulnerability Handling and Disclosure

The assurance level of the SCS implies the depth of the vulnerability assessment, i.e. SCS of assurance level basic, the accessor will rely upon the claims, vulnerability reports, treatment plans and implementation reports of controls as provided by the SCS provider, technical vulnerability assessment /penetration testing is optional or high level. For assurance level high, the accessor will perform technical vulnerability assessment and penetration testing of all SCS assets and implemented controls. In this section, the rules regarding the way that the previously undetected cybersecurity vulnerabilities in SCSs shall be reported and handled are presented.

SCS Providers shall make use of the provisions of ISO/IEC 30111 [20] for a reference of the steps involved for the handling of vulnerabilities. Such steps include the following main phases: preparation, receipt, verification, remediation development, release, post release. New vulnerability information can become available in a variety of ways. The most common ways of receiving information about new vulnerabilities include:

- From the SCS provider and or the SCS partners of according to Article 55.1.(c) of the EUCSA;
- there is a new publicly disclosed vulnerability on the referenced online repositories (e.g. NIST) according to Article 55.1.(d) of the EUCSA;
- the SCS provider finds out a related vulnerability to its certified SCS in any other way (e.g. Dark Web).

SCS providers may use the ISO/IEC 29147 standard [21] as a reference for the general rules related to vulnerability disclosure. For the duration of the vulnerability analysis process, the SCS provider may apply an embargo period, meaning that the possible vulnerability is not further disclosed for a period no longer than ninety (90) days. Once a remediation strategy has been defined by the SCS provider and approved by the assessor, information related to the confirmed vulnerability shall be disclosed to the NCCA (in case of Substantial/High AL SCS), in accordance with the reporting standards established by the NCA. The NCCA shall make the reported information available to other NCCAs which may also decide to further investigate the vulnerability. The final step of the disclosure process of a new vulnerability occurs when a correction has been brought to the SCS to mitigate the risk introduced by such vulnerability.

Conclusions

The proposed CYRENE-EUSCS candidate scheme tackles the challenges identified towards the certification of supply chain services, such as a diverse set of relevant SCS stakeholders involved in the life cycle of the certificate (as well as in the life-cycle of the SCS, complex systems and a constantly evolving threat landscape of supply chain services, as well as the existence of different schemes in Member States by calling for cybersecurity best practices across three levels of assurance and by allowing for a transition from current national schemes in the EU. The proposed scheme can be used by a self-assessor or by a CAB depending upon the assurance level of the SCS.

Our future research work aims to apply the proposed scheme in different SCS from various sectors (e.g. maritime, health).

Acknowledgment

The authors are grateful for the financial support provided by the European Commission for the Horizon 2020 under grant agreement No 952690 project CYRENE; and from the national programme, EPAnEK, in the No. T2EΔ/03488 project CYSMET [22]. Special thanks to the partners of these projects for their contributions.

References

[1] CYRENE EU H2020 project. Online available: https://www.cyrene.eu, accessed on May 14, 2021.

[2] ENISA, “Cybersecurity Certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS”, v1.0, July 2020, Online available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme, accessed on April 29, 2021.

[3] ENISA, “EUCS – Cloud Service Scheme: a candidate cybersecurity certification scheme for cloud services”. Online available: https://www.enisa.europa.eu/publications/eucs-cloud-service-scheme, accessed on April 29, 2021.

[4] European Parliament and Council, Regulation (EU)2019/881 on ENISA and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), April 2019.

[5] The Directive on security of network and information systems (NIS Directive). (2020, December 16). An official website of the European Union. Retrieved July 18, 2021, from https://ec.europa.eu/digital-single-market/en/directive-security-network-and-information-systems-nis-directive

[6] P. Kyranoudi, E. Kalogeraki, A. Michota, D. Polemi, “Cybersecurity Certification Requirements for Supply Chain Services”, 26th IEEE Symposium on Computers and Communications (ISCC 2021), Athens, Greece, September 5-8, 2021

[7] CYRENE EU H2020 project. D2.1 - Supply Chain Analysis and Requirements, 2021.

[8] ENISA, “Methodology for a Sectoral Cybersecurity Assessment”, Online available: https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment, accessed on September 13, 2021.

[9] ISO/IEC 27000-series on Information Security. Online available: https://www.iso.org/news/ref2266.html, accessed on April 29, 2021.

[10] ISO/IEC 15408-1/2/3:2008-09, international standard, “Information technology-Security techniques-Evaluation criteria for IT security”.

[11] ISO/IEC 18045:2008 international standard, “Information technology-Security techniques- Methodology for IT security evaluation”, online available: https://www.iso.org/standard/46412.html, accessed on April 29, 2021.

[12] ISO 28000:2007 international standard, “Specification for security management systems for the supply chain”, 1st Edition 2007-09. Online available: https://www.iso.org/standard/44641.html, accessed on April 20, 2021.

[13] ISO/IEC 27005:2018, Information technology — Security techniques — Information security risk management.

[14] NIST Special Publication 2000-02, Conformity Assessment Considerations for Federal Agencies, online available at: https://doi.org/10.6028/NIST.SP.2000-02

[15] K. Kioskli, D.Polemi “Psychosocial Approach to Cyber Threat Intelligence”, International Journal of Chaotic Computing (IJCC), Volume 7, Issue 1, 2020

[16] CYRENE EU H2020 project. D3.1 - Conformity Evaluation Process & Multi Level Evidence Driven Supply Chain Risk Assessment, 2021.

[17] ISO/IEC 17065:2012. Conformity assessment — Requirements for bodies certifying products, processes and services

[18] ISO/IEC 17021-1:2015, Conformity assessment — Requirements for bodies providing audit and certification of management systems — Part 1: Requirements

[19] International Standard on Assurance Engagements (ISAE) 3402 Assurance reports on controls at a service organization, in [IAASB Handbook], Vol. 2, pp. 217-264]

[20] ISO/IEC 30111, Information technology — Security techniques — Vulnerability handling processes

[21] ISO/IEC 29147:2018, Information technology — Security techniques — Vulnerability disclosure

[22] CYSMET EU H2020 project. Online available: accessed on May 14, 2021.

Nineta Polemi is a cybersecurity Professor in the University of Piraeus-UNIPI- (Cyber Security Lab, Dept. of Informatics) and CTO/ Co-Founder of trustilio. She served (2017-2020) as Programme Manager and Policy Officer in the European Commission DG (CONNECT H1 Unit entitled 'Cybersecurity Technologies and Capabilities'). She has obtained her Ph.D. in Applied Mathematics (Coding Theory) from The City University of New York (Graduate Center). She held teaching and research positions in The City University of New York (Queens & Baruch Colleges), State University of New York (Farmingdale), Université Libre de Bruxelles (ULB)-Solvay Brussels School-. She has over 150 publications in security (e.g. port security, maritime security, maritime supply chain security) has organised numerous scientific and policy international cybersecurity scientific events. She has received many research grants (NATO, IEEE) and awards (NSA, MSI Army Research Office IEEE, CYNY, Hellenic Ministry of Maritime, Hellenic National Defense General) and has participated as Project and Technical Manager in more than 60 cybersecurity international, EU and national R&D and commercial projects. She serves as external expert/reviewer/consultant in ENISA, E.C.(DG CNECT, DG HOME), FORTH, Focal Point.

Dr Alexandra Michota is an ICT Security and Privacy Auditor at the Hellenic Data Protection Authority (HDPA). Before joining HDPA, Alexandra had been working as an Officer in Network and Information Security at the European Union Agency for Cybersecurity (ENISA) in the areas of EU Cybersecurity Certification, Privacy and Data Protection, and Supporting the Fight against Cybercrime: Cooperation between Computer Security Incident Response Teams (CSIRTs) and Law Enforcement. She also has more than 10-year experience spanning across different ICT activities and fields linked to cybersecurity like 'Government services', 'Education and training', 'Governance Risk Compliance and Audit' both in the private and public sector. Alexandra holds a BSc in Digital Systems, an MSc in Network-Oriented Information Systems and a Ph.D. in Privacy in Online Social Networks from the Department of Digital Systems, University of Piraeus, Greece. She also worked as a Post-Doctoral Researcher at the same University. Her research interests lie in the areas of information and communication systems security and privacy. She has authored and co-authored research papers and scientific reports and participated in international, EU and national R&D projects in these areas. Currently, she also serves as external expert/consultant in Focal Point.

Prof. Sotiris Ioannidis (M) received a BSc degree in Mathematics and an MSc degree in Computer Science from the University of Crete in 1994 and 1996 respectively. In 1998 he received an MSc degree in Computer Science from the University of Rochester and in 2005 he received his Ph.D. from the University of Pennsylvania. Ioannidis held a Research Scholar position at the Stevens Institute of Technology until 2007 and a Research Director at the Foundation for Research and Technology – Hellas (FORTH) until 2020. He is currently Associate Professor at the School of Electrical and Computer Engineering of the Technical University of Crete (TUC) and Director of the Microprocessor and Hardware Laboratory.

He was a Member of the ENISA Advisory Group (AG) from 2017 to 2020, and is a Member of the National Infrastructures for Research and Technology (GRNET) Advisory Committee (AC). He is also Chairman of the Committee of Ethics and Deontology of Research of FORTH and Member of the Advisory Committee for National Infrastructures for Research and Technology. His research interests are in the area of systems and network security, security policy, privacy, and high-speed networks. Ioannidis has authored more than 200 publications in international conferences and journals, as well as book chapters, and has both chaired and served on numerous program committees in prestigious conferences, such as ACM CCS and IEEE S&P. Ioannidis is a Marie-Curie Fellow and has participated in numerous international and European projects. He has been the PI of more than 40 European, National and DARPA projects, attracting funding in excess of 12 million euros for his organization, and has been Project Coordinator in 14 of them. Currently, Prof. Ioannidis is the Deputy Coordinator of CONCORDIA, one of the four EU Cybersecurity Pilots.

CV

https://docs.google.com/document/pub?id=1qofU6ya50i_uSCipszWbxUgYyUMQFRoute3FV4s6sFw

5th NMIOTC CONFERENCE ON CYBER SECURITY IN MARITIME DOMAIN

Situational Awareness of Cyberspace on Maritime Military Operations

by Lt Françoa Taffarel, OF-2, (Brazilian Navy), taffarel@marinha.mil.br
Cdr Salvador Mota, OF-4, (Brazilian Navy), salvador.mota@marinha.mil.br

ABSTRACT

Embedding cybersecurity into operational naval assets implies a much greater technological and economic challenge than securing such networks in facilities at ground military installations. Cyber systems used in naval ships are more oriented towards operational technology (OT) logic than information technology (IT). In the maritime domain, military units increasingly rely on satellite data communication technologies to provide connection between joint commands for monitoring and optimizing propulsion systems, sensors and weapons. Military ships are becoming increasingly automated, the risks associated with attacks on a ship's information subsystems are becoming increasingly defined, directly impacting the Naval Task Force's mission. Therefore, it is necessary for Commanders to know how to use situational awareness of cyberspace to assist the decision-making process in order to protect the cyberspace of their Naval Task Forces. To contribute to this purpose, this article discusses how providing situational awareness from defensive operations in cyberspace at the tactical level can help decision making at the operational level. For this discussion, an analysis of works related to the theme of situational awareness of cyberspace is carried out, then we highlighted characteristics of a computational asset that allow the construction of this situational awareness and finally we present a Cyber Exercise in Real Operations at Sea that contributes to promoting situational awareness in cyberspace in the decision-making process.

Keywords: situational awareness, cyberspace, decision-making process, cyber exercise.

Introduction

The shipping industry is the driving force of the global economy. Through an enormous network of ships, ports, logistical and administrative infrastructure, around 90% of the world's cargo is transported by ships every year. Like most industries, the maritime industry has become increasingly automated, interconnected and remotely monitored. Maritime commerce has also become the main target of cyber-attacks, due to its dependence on technologies for navigation, communication and logistics. In this context, the growing use of cyberspace in military operations reached a critical point of dependence, allowing an increase in the probability of interruption or degradation of resources in the operating systems of a naval environment [1].

Cyber operations have created a new operational space for military action. For the navies, the effect of cyber warfare can be seen in maritime superiority, in the loss of maritime domain in a given region, by denying information about the position of ships or even by the degradation of supply chains.

The naval assets increasingly use satellite information to fulfill their missions, these technologies have become especially vital for communication networks ensuring that Force Commands are always connected [2]. The ability to communicate and exchange information is critical to the success of an operation as it allows for shared situational awareness and faster command decisions.

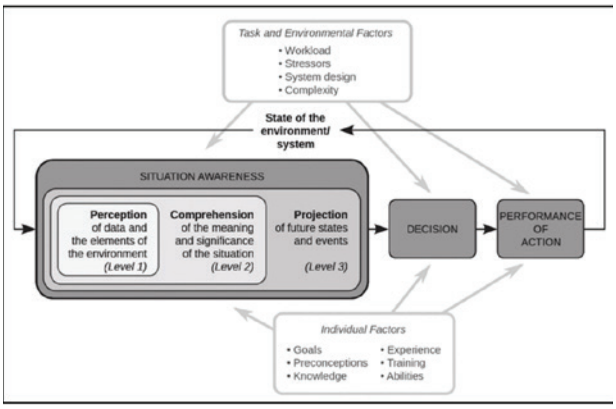
During an operation in the maritime environment, satellite communication, within each naval asset, needs to be constantly monitored by computational assets. These assets must provide their operators with the ability to perform threat detection and management actions, allowing the Maritime Task Force (MTF) Commander to have situational awareness of the cyberspace of their naval assets in order to facilitate their decision-making.

In addition to this first section, this article is divided into four sections, in the second section, through an analysis of related works, we discuss about what is situational awareness in cyberspace, in the third section we present what characteristics a computational asset acting at the tactical level must have to generate situational awareness in cyberspace at the operational level. Finally, we present a model Cyber Exercise in Real Operations at Sea that contributes to promoting situational awareness in cyber space in the decision-making process.

Definition of situational awareness of cyberspace

According to the NATO Glossary of Terms and Definitions (2020), Situational Awareness is defined: "The knowledge of the elements in the battlespace necessary to make well-informed decisions." [3]. The situational awareness is part of decision-making in dynamic environments and takes into account objectives, expectations and factors related to the task and the system used.

In searches for existing literature that cite the situational awareness (SA) of cyberspace it was noted that most authors choose to quote or adapt Endsley's definition. According to Endsley (1995) [4], it is possible to build SA that allows decision making and consequent performance of actions, using the model exposed in Flowchart 1, which presents a three-step process based on: Perception of the elements in the environment; Comprehension of the current situation; and projection about what the environment might look like in the near future.



Task and Environmental Factors
• Workload
• Stressors
• System design
• Complexity
State of the environment/ system
SITUATION AWARENESS
Perception of data and the elements of the environment (Level 1)
Comprehension of the meaning and significance of the situation (Level 2)
Projection of future states and events (Level 3)
DECISION
PERFORMANCE OF ACTION
Individual Factors
• Goals
• Preconceptions
• Knowledge
• Experience
• Training
• Abilities

Flowchart 1 – Endsley's Model of Situation Awareness. [4]

For [5] the situational awareness of cyberspace is the set of all data about the state of operating systems that make up cyberspace for a given operation. For [6], when in military operations consisting of one or more means, situational awareness of cyberspace is the effective understanding of everything that is associated with the domain of cyberspace that can impact the security of personnel and material involved in the missions.

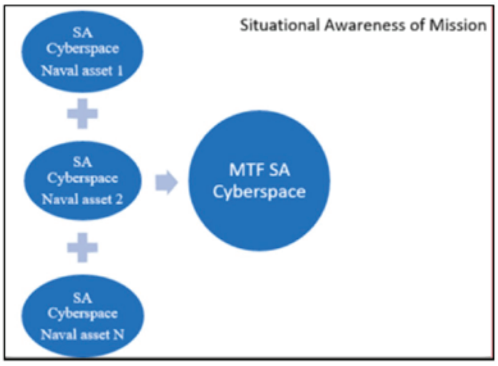
For [7] a definition of situational awareness of cyberspace in a military environment as: "the requisite current and predictive knowledge of the environment upon which operations depend — including physical, virtual, and human domains — as well as all factors, activities, and events of friendly and adversary forces across the spectrum of conflict."

Thus, it can be inferred that situational awareness of cyberspace supports military decision makers in relation to knowledge about the state of an operational environment and the relevant operational means within it.

In order to find a definition of the situational awareness of cyberspace, this article adopted the definition of cyberspace as set out in AJP-3.20, Allied Joint Doctrine for Cyberspace Operations (2020): "The global domain consists of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data." [8]

Note that the operational environment involved in the definition of cyberspace mentioned above is permeated by computer network communication. According to [9], a definition of situational awareness of cyberspace in line with the thinking of the authors of this article: "the perception of network events and data, the understanding of their meaning in terms of mission, resources, connectivity, threats and vulnerabilities and the projection of its status in the near future".

Thus, combining the Endsley model with the above definition, we concluded that cyberspace situational awareness is the subset of all situational awareness needed to work in and across cyberspace in all naval assets, as shown in Figure 1. The situational awareness of cyberspace is



Situational Awareness of Mission
SA Cyberspace Naval asset 1
SA Cyberspace Naval asset 2
SA Cyberspace Naval asset N
MTF SA Cyberspace

Figure 1 - Situational awareness of cyberspace Maritime Task Force

not an end in itself; but based on constant analysis of the computer network situation, it is a means used to support decision-making, allowing a Maritime Task Force Commander to achieve his objectives in the maritime domain.

A digital asset to support as constructor of situational awareness of cyberspace

With this understanding of the situational awareness of cyberspace, we seek to understand how the maritime domain interacts with cyberspace. We initially identified NATO's definition of Maritime Situational Awareness (MSA) as "The understanding of military and non-military events, activities and circumstances within and associated with the maritime environment that are relevant for current and future NATO operations and exercises where the Maritime Environment (ME) is the oceans, seas, bays, estuaries, waterways, coastal regions and ports" [10]

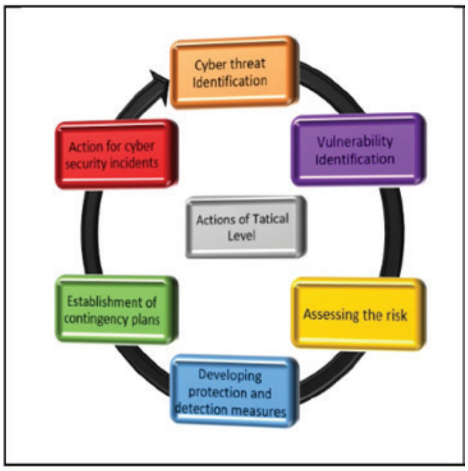
Analyzing the text above, we realize the need to compile a wide range of information that allows the MTF Commander to make the correct decision. Achieving situational awareness in the maritime environment requires continuous data collection and analysis from all available sensors and computational assets.

Considering that, in most cases, communication between ships of a Task Force is carried out via satellite band and that cyberspace is everywhere in the maritime domain, it appears that the data mentioned in the previous paragraph, mostly, are encapsulated and transmitted internally by naval media through the computer network.

In this context, to identify the computational asset that allows creating situational awareness of cyberspace through, we cite below which actions and questions must be carried out at the tactical and operational level by the defensive teams and by the MTF Commanders, respectively.

At the tactical level, situational awareness of cyberspace focuses on threats that target existing vulnerabilities of specific networks and systems, as well as the consequences arising from such compromises.

Flowchart 2 exposes tactical level defensive actions in or through cyberspace to preserve friendly freedom of action in cyberspace [8]. These actions are aligned with three documents related to defensive cyberspace operations: AJP-3.20, Allied Joint Doctrine for Cyberspace Operations, National Institute of Standards and Technology (NIST) Cybersecurity Framework [11] and The Guidelines on Cyber Security Onboard Ships [12]:


Cyber threat Identification
Vulnerability Identification
Assessing the risk
Developing protection and detection measures
Establishment of contingency plans
Action for cyber security incidents
Actions of Tatical Level

Flowchart 2 - Actions of Tactical Level

Analyzing the operational level, this article considers that the Commander cited in the referenced publications can be correlated with the Commander of the MTF. Thus, according to [8], at the operational level, the MTF Commander should consider the following operational factors:

- Effects in cyberspace - They contribute to the creation of tactical, operational and strategic effects that lead to the achievement of military objectives. These effects are directly related to software, data and protocols. However, they can occur from kinetic levels in other domains;
- Joint functions - Provide a framework to help integrate and synchronize capabilities and activities in joint operations; and
- Principles of operation - the principles of joint operations also apply to those that take place in cyberspace; however, the interpretation of these principles may differ due to the nature of this domain. They are: Security; Surprise; Concentration of force; Maintenance of morale; Freedom of action.

At the operational level, improving decision-making processes must: persistently monitor portions of the cyberspace domain and identify potential cyber threats in a timely manner. Therefore, a tool capable of operationalizing all information is needed, which also provides a reasoned view of current conditions or future situations in cyberspace. This tool can be installed in each MTF naval assets, and must be able to:

- Give real-time visibility of threats to the entire cyberspace domain;
- Identify threats quickly;
- Search and analyze logs to investigate a possible incident;
- Decrease response time.

Conducting Cyber Exercise in a Real Operations at Sea

This paper proposes the execution of Cyber Exercise in a Real Operations at Sea as a way to assess whether the increase in situational awareness of cyberspace is helping the decision-making process. This exercise can be composed of two opposing teams operating in MTF cyberspace, one team performing cyberspace defense and the other attacking. As shown in Figure 2, during the exercise the defense and attack teams should report to the MTF Commander, what were the effects of their actions in the MTF cyberspace.

According to [13], the MTF Commander should be able to answer some questions to improve the decision-making process through the situational awareness of cyberspace, we list two of them: “1. What operations exist in cyberspace? 2. What is the impact of cyberspace effects on the mission?”. We consider the following questions: 3. How many Operating Technologies (OT) are rendered inoperative by a cyber incident? 4. To what degree is the mission’s naval assets informational infrastructure compromised after an incident?

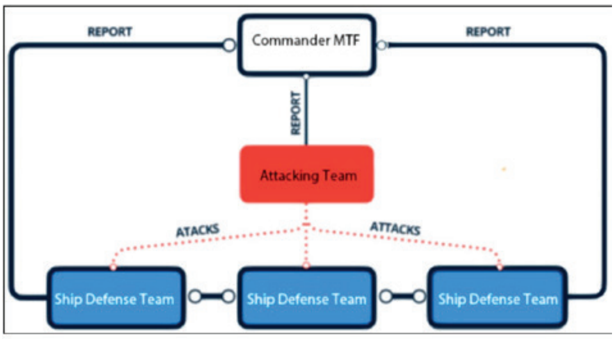


Figure 2 - Cyber Exercises

The actions must be conducted in the same satellite band of communication of the means of navigation performed. Each ship’s defense team must collect, analyze, identify data from the network and look for any critical cyber incidents involved in the MTF, providing the Commander with a cyberspace situational awareness that allows him to make a comprehensive, reliable and timely decision to comply with the mission. Attacking team can perform offensive actions by applying a Cyber Kill Chain created by members of Lockheed Martin [14] across MTF’s cyberspace, shown in Figure 3.

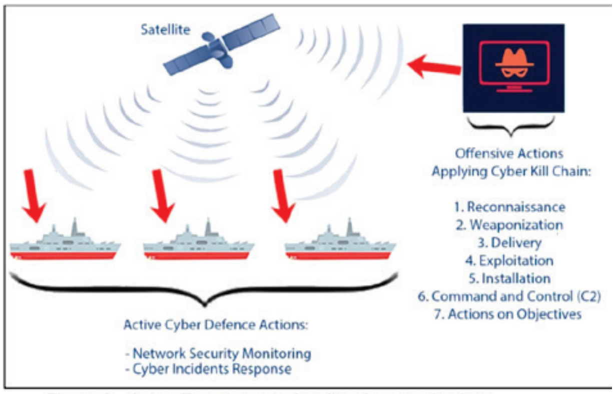

Satellite
Offensive Actions
Applying Cyber Kill Chain:
1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command and Control (C2)
7. Actions on Objectives
Active Cyber Defence Actions:
- Network Security Monitoring
- Cyber Incidents Response

Figure 3 - Cyber Exercises via Satellite Communications.

Due to the exercises take place in an actual operations at sea against cyberspace of MTF, it is suggested that there are verifiable measures for all of the actions for each of the teams involved:

● Defense ships team - can be evaluated by the number of cyber incidents detected, blocked and reported to MTF Commander.

● Attack team - can be evaluated by the number of discoveries of vulnerability or degradations of the OT/IT embedded in naval assets.

Conclusion

As previously stated, cyber-attacks have become increasingly common, and with that, cyber security has been recognized as a growing concern around the world. Military operations in the maritime domain can be targets of cyber-attacks and it is vital that MTF Commanders know how to use the situational awareness of cyberspace in the decision-making process of their actions. Success in future military conflicts will depend on which side can collect, process and share information to make better decisions faster than its adversary.

In conclusion, we emphasize that network security is a global challenge. A nation can remain indifferent and take care of itself, as it should be the responsibility of the international community to provide a secure network. As future work, we intend to carry out Cyber Exercise in Real Operations at Sea and quantify the risks and impact that the offensive teams caused to maritime domain in military operations.

References

1. Kuehl, D.T., (2009), “From cyberspace to cyberpower: Defining the problem,” in Cyberpower and national security, ed. Kramer, F. D., Wentz, L.K. & Starr, S. H. (Dulles, VA: Potomac Books, Inc., 2009).
2. U.S. Department of Defense. Joint Publication 3-32 Joint Maritime Operations. 08 June (2018).
3. NATO Glossary of Terms and Definitions (English and French): AAP-06. Edition 2020. NATO Standardization Office.
4. Endsley, M. R., “Toward a theory of situation awareness in dynamic systems,” Human Factors: The Journal of the Human Factors and Ergonomics Society, 37(1), (1995), 32-64.
5. Stone, Steve (2015) “Data to Decisions for Cyberspace Operations,” Military Cyber Affairs: Vol. 1 : Iss. 1 , Article 6.
6. Tyworth, M., N. A. Giacobe, and V. Mancuso, F. 2012. “Cyber situation awareness as distributed socio-cognitive work.” Cyber Sensing - Proceedings of SPIE, 8404.
7. Conti, G., J. Nelson, and D. Raymond. 2013. “Towards a cyber common operating picture.” In K. Podins, J. Stinissen, and M. Maybaum (Eds.), International Conference on Cyber Conflict (pp. 1–17). Tallinn: NATO CCD COE Publications.

8. AJP-3.20, Edition A, Version 1, Allied Joint Doctrine for Cyberspace Operations.2020

9. Levin, D., Tenney, Y. and H. Henri. 2001. "Issues in human interaction for cyber command and control." DARPA Information Survivability Conference, (1)141–151.

10. Kościelski, M., Miler, R.K., Zieliński, M., 2007. Maritime Situational Awareness (MSA). Zeszyty Naukowe Akademii Marynarki Wojennej, R. 48 nr 4 (171), pp. 79–88.

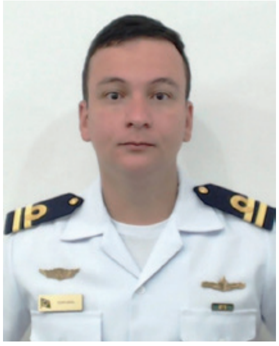
11. Barrett, M. (2018), Framework for Improving Critical Infrastructure Cybersecurity Version 1.1, NIST Cybersecurity Framework, [online], https://doi.org/10.6028/NIST.CSWP.04162018, https://www.nist.gov/cyberframework

12. The Guidelines on Cyber Security Onboard Ships, Baltic and International Maritime Council, Version 4.0, 2021.

13. Alberto Domingo et. al. (2021). Enabling NATO Cyberspace Operations by Building Comprehensive Cyberspace Situational Awareness. In Dr Juan Lopez Jr, Dr Kalyan Perumalla, Dr Ambareen Siraj (Eds.), ICCWS 2021: Proceedings of the 16th International Conference on Cyber Warfare and Security (pp. 509-518).

14. Hutchins, Eric & Cloppert, Michael & Amin, Rohan. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.

Commander SALVADOR MOTA JUNIOR is actually Head of Brazilian Navy Cyber Defense Division in working with Planning, organizing and coordinating the execution of Cyber Operations. Graduation in Naval Sciences at Brazilian Navy Academy, Master's Degree in Naval Sciences at Naval Warfare College, Postgraduate in Cybersecurity and Ethical Hacker at UNICIV, VIII Course of Cybersecurity and Crises Management in Cyberspace at National Defense Institute (Portugal).



Lieutenant Françoa Taffarel Rosario Corrêa is actually officer in Brazilian Navy Red Team section of Cyber Defense division working with Planning, organizing and coordinating the execution of Cyber Operations. Graduation in Naval Sciences at Brazilian Navy Academy, Postgraduate in Cyberwarfare at Brazilian Army Center Instruction.

Visit of the State Secretary of the Slovakian Ministry of Defence

On Monday 12th of July 2021, the State Secretary of the Slovakian Ministry of Defence, Mr Marian Majer and Her Excellency the Ambassador of the Slovak Republic in Greece, Ms Iveta Hricova, escorted by Staff of the MoD of Slovakia and the Embassy of Slovakia in Greece, visited the NMIOTC premises.

Visit of the Chair of NATO Military Committee, Admiral Rob Bauer (RNN)

On Friday 17th of September, the Chief of General Staff, General Konstantinos Floros, and the Chairman of the NATO Military Committee, Admiral Rob Bauer (CMC), visited the NATO Maritime Interdiction Operational Training Center (NMIOTC).

CyberHOT Summer School

From 27 to 28 of September 2021, the CyberHOT Summer School, co-organized by University of Piraeus and Technical University of Crete, under the auspices of the NATO Maritime Interdiction Operational Training Centre (NMIOTC), took place in NMIOTC premises. It was attended by 24 participants from 4 Nations.

5th Cyber Security Conference in the Maritime Domain

From 29 to 30 September 2021, the 5th Cyber Security Conference in the Maritime Domain was held at NMIOTC, attended by 98 participants from Allied and Partner Nations, International Organizations, the international academic community, representatives from the shipping and IT industry.

Visit of Defence Attachés Accredited to Greece

On Wednesday 6th of October 2021, the Foreign Defence Attachés accredited to Greece, (Albania, Australia, Austria, Bulgaria, Canada, Germany, Hungary, Netherlands, Romania, Russia, Saudi Arabia, Serbia, Spain, U.A.E., U.K., USA, and Zambia) visited NMIOTC's premises.

Visit of the Operation Commander of EUNAVFOR MED IRINI

On Wednesday 13th of October 2021, the Operation Commander of EUNAVFOR MED IRINI, Rear Admiral Stefano Turchetto, visited NMIOTC's premises.

Individual Training And Education Program Planning Board (IPB) II And Department Head Forum

From 26 to 28 October 2021, the Annual Department Head forum as well as the second Individual Training and Education Program Planning Board (IPB II) for 2021, organized by ACT, were hosted sequentially at NMIOTC's premises with 47 in person and 16 virtual participants from NATO relevant Organizations and entities.

NATO Nuclear Policy Symposium

From 3 to 4 November 2021, the NATO Nuclear Policy Symposium organized by NATO Nuclear Policy Directorate and supported by the General Directorate of National Defence Policy and International Relations of the Hellenic Ministry of Defence, was hosted at NMIOTC's premises with 89 participants coming from NATO capitals, Headquarters and relevant Organizations.

6th International Senior Course of Hellenic National Defence College: "Contemporary Maritime Security Threats" Module

The students of the 6th International Senior Course of the Hellenic National Defence College (HNDC) attended the "Contemporary Maritime Security Threats" module delivered by NMIOTC SMEs, during their educational week trip from 8 to 12 of November 2021 at NMIOTC premises.

Visit of the Deputy Chief for Operations and Training of the Romanian Naval Forces

On Saturday 13th of November 2021, the Deputy Chief for Operations and Training of the Romanian Naval Forces, Rear Admiral (LH) Cornel-Eugen Cojocaru, escorted by the Deputy Chief of the Maritime Component Command Captain (N) Marcel Neculae, visited NMIOTC's premises.

Multilateral Exercise "MEDUSA 11"

In the context of the Multilateral Exercise "MEDUSA 11" and under the auspices of HNDGS, a tailored training package was delivered to exercise participants from 14 to 16h of November 2021 at NMIOTC premises.

Visit of the Commander of Hellenic Special Warfare Command

On Tuesday 30th of November 2021, the Commander of Hellenic Special Warfare Command of Greece, Lieutenant General Georgios Tsitsikostas, visited NMIOTC premises.

Course 10000 "MIO in Support of Countering Illicit Trafficking at Sea"
July 5 - 9, 2021

Course 21000 "Medical Combat Care in Maritime Ops"
September 6 - 17, 2021

Underwater Post Blast Investigations Course
September 20 - 24, 2021

Course 23000 “Weapons Intelligent Team (WIT)
Supplement in the Maritime Environment
September 27 - October 1, 2021

Course 18000 "Maritime Biometrics Collection & Tactical Forensic Site Exploitation"
November 1 - 5, 2021

Training of 1st Paratroopers Regiment
November 7 - 11, 2021

Training of Egyptian SOF Team during Exercise MEDUSA 11
November 14 - 16, 2021

Course 7000 “MIO in Support of Counter Piracy”
November 15 - 19, 2021

Container Inspection training, German BTU Team
November 22 - December 3, 2021

Training of ESP RAYO
November 23 - 24, 2021

Visit of His Excellency Mr David Dondua,
Ambassador of Georgia in Greece
July 1, 2021

Visit of the American Hellenic Institute
July 2, 2021

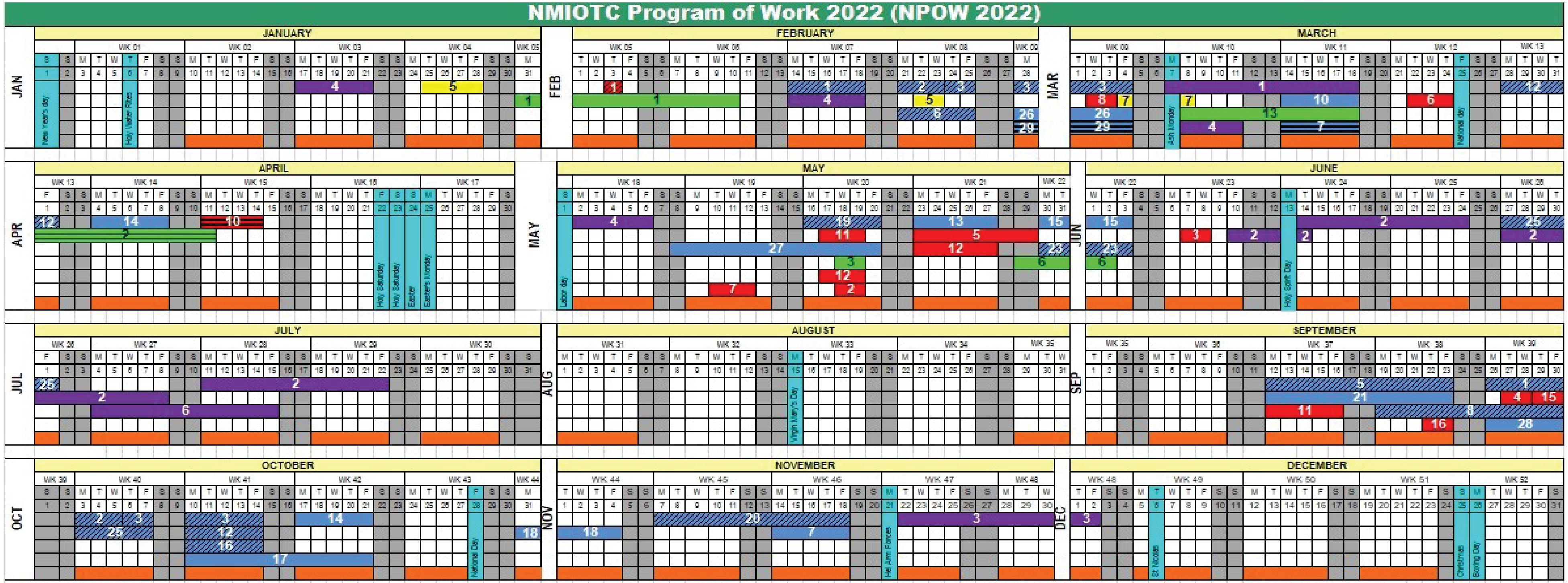
Visit of NATO HUMINT CoE Director,
Colonel Florin-Vasile Tomiuc (ROU A)
July 13, 2021

Visit of Defence Attachés accredited to Greece
October 6, 2021

Visit of His Excellency,
the Ambassador of the United Mexican States in Greece,
Mr Daniel Hernandez-Joseph
October 15, 2021

Visit of Her Excellency,
the Ambassador of Italy in Greece,
Ms Patrizia Falcinelli
November 17, 2021

NMIOTC Program of Work 2022 (NPOW 2022)



COURSES (ETOC ID.)

1	Course 1000 - Command Team MIO Issues (MOP-MO-31201)
2	Course 2000 - Boarding Team Theoritical Issues (MOP-MO-51203)
3	Course 3000 - Boarding Team Practical Issues (MOP-MO-41205)
4	Course 4000 - MIO Final Tactical Exercise (MOP-MO-41207)
5	Course 5000 - Maritime Operational Terminology Course (MOP-MO-21208)
6	Course 6000 - Weapons of Mass Destruction in MIO (MOP-MO-31209)
7	Course 7000 - MIO in support of Counter Piracy and Armed Robbery at Sea Ops (MOP-MO-31210)
8	Course 8000 - C-IED Considerations in Maritime Force Protection (IED-ED-31679)
10	Course 10000 - MIO in Support of Countering Illicit Trafficking at Sea (MOP-MO-32012)
12	Course 12000 - C-IED in MIO (IED-ED-31904)
13	Course 13000 - Command Team Issues in MIO in support of International Efforts to Manage the Migrant and Refugee Crisis at Sea (MOP-MO-22015)
14	Course 14000 - Maritime IED Disposal (IED-ED-32008)
15	Course 15000 - Migrant Handling Team Issues in MIO in support of International Efforts to Manage the Migrant and Refugee Crisis at Sea (MOP-MO-36765)
16	Course 16000 -Maritime Aspects of Joint Operations (MOP-MO-22078)
17	Course 17000 - Train the Trainers Technical Instructor (ETE-IT-34432)
18	Course 18000 - Maritime Biometrics Collection and Tactical Forensic Site Exploitation (MOP-MO-32373)
19	Course 19000 - Cyber Security Aspects in Maritime Operations (COP-CD-22104)
20	Course 20000 - MIO in Support of Managing Perilous Security Incidents on Coastal Critical Sites (SOF-SO-36734)
21	Course 21000 - Medical Combat Care in Maritime Operations (MED-MS-34411)
23	Course 23000 - WIT Supplement in Maritime Operations (IED-ED-35437)
25	Course 25000 - Drafting, Production and Maintenance of NATO Standards Course (ETE-IT-35477)
26	Course 26000 - Tactical Combat Causalty Care/ Combat Lifesaver in Maritime Operations (MED-MS-36748)
27	Course 27000 - Maritime Sniper Course (SOF-SO-35603)
28	Course 28000 - Radiological Search in Maritime Environment (WMD-CD-35614)
29	Course 29000 - Detection and Identification of Weapons of Mass destruction (CBRN materials) in Maritime Interdiction (WMD-MD-35660)

EVENTS

1	NAB (NMIOTC)
2	NCB (HNGS)
3	NMIOTC Annual Conference
4	NMIOTC Cyber Security Conference
5	NATO Maritime Operations Law Course
6	AWWCG meeting
7	PfPC ADL WG meeting
8	CCD COE Delegation Visit
9	EEZ Course (TBD) (Cancelled)
10	IP CaT Meeting
11	MMTT WG /Medical Support ADC
12	UPX Training
13	CPTM of Steadfast Interest-23
14	MPC for NOSP 22 and TC&S WS
15	Cyber Hot
16	ESDC Cyber Course

EXERCISES / METTs

1	CUTLASS EXPRESS-22 METT
2	SEA SHIELD-22 METT
3	ADRION-22 METT
4	BREEZE (TBD)
5	SEA BREEZE (TBD)
6	NIRC TRAINING
7	DYNAMIC MESSENGER (TBD)
8	PHOENIX EXPRESS METT (TBD)
9	OSG FOCOPS (TBD)
10	MEDUSA (TBD)
11	NIRIIS (TBD)
12	NORTHERH SPIRIT -22 (TBD)
13	ARIADNE-22

TAILORED TRAININGS

1	GER Teams
2	USA Teams
3	IRE Teams (TBD)
4	GRC Teams
5	GRC Naval Units
6	EST Teams
7	ESP Naval Units

► **Updated 01 April 2022**

☰ Cancelled

🟦	Training Courses
🟪	Tailored Trainings
▨	NATO Events
🟩	Exercise / MTTs
🟩	Trial Courses
🟥	Events
🟨	Naval Unit Training
🟦	National Holidays
🟧	Available Period for Training
🟪	Evaluation of Courses / Maintenance

NMIOTC
Souda Bay 732 00 Chania
Crete, GREECE

Phone: +30 28210 85710
Email: studentadmin@nmiotc.nato.int
nmiotc_studentadmin@navy.mil.gr

Webpage: www.nmiotc.nato.int