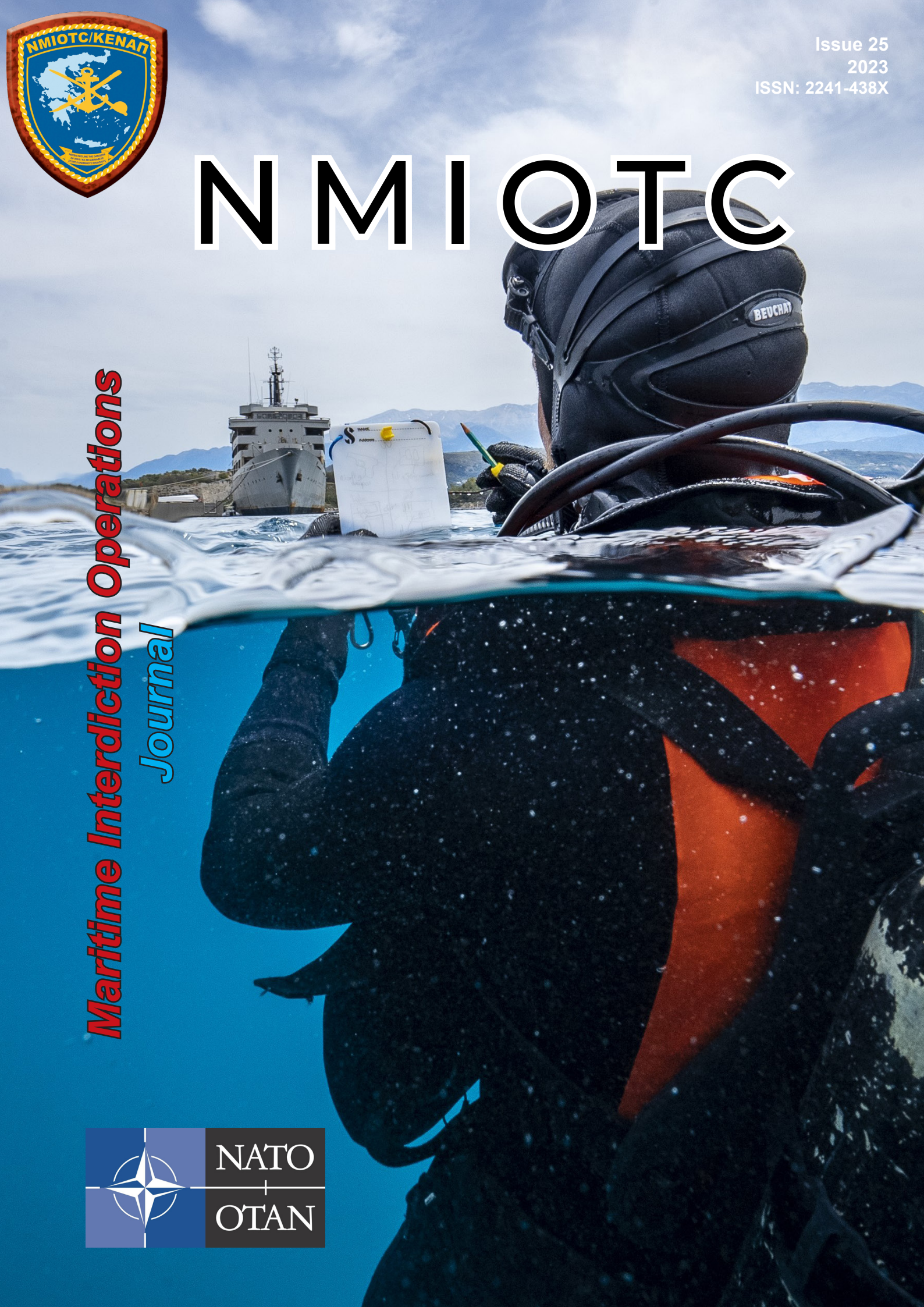
Issue 25
2023
ISSN: 2241-438X

NMIOTC



Maritime Interdiction Operations Journal

NATO OTAN

NATO
Maritime Interdiction Operational Training Centre

SAVE THE DATES

15th NMIOTC Annual Conference
4 - 5 June 2024

"Risks and Challenges in a Dynamic Maritime Domain: Strategy Adaptations, Technology Innovations and the Operational Landscape of the Future"

4&5 JUNE 2024 — 15TH NMIOTC ANNUAL CONFERENCE

8th Conference on Cyber Security in the Maritime Domain
18 - 19 September 2024

CONTENTS

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Cdre T. Papadimitriou GRC (N)
Commandant NMIOTC

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

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

Layout Production
Lt Cdr I. Giannelis GRC (N)
Lt. Ath. Perdikopoulos GRC (J)
Journal Assistant Editors

Cover Photo: Evan Possley

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

NMIOTC
Commandant's Editorial

Maritime security is key to our peace and prosperity.
The importance to protect maritime lines of energy transportation and, in a broader sense, Maritime Critical Infrastructure has increased all over the world during the last decade and the conflict between Russia and Ukraine ultimately highlighted the risks and the possible consequences related to energy security.

The critical maritime infrastructures, like oil platforms, pipelines or harbor facilities, are strategically relevant and, by nature, difficult to be protected. An attack to these facilities would have a dreadful outcome.
Major changes in the international security environment and energy landscape have brought increased strategic attention, resulting in a pragmatic energy security agenda, that provides tangible and added value to the Allies and partner countries.
As stated in the NATO 2022 strategic concept, the Allies will invest their ability to prepare for, deter and defend against the coercive use of energy.
Nowadays, top priority for NATO is the Energy Security and the protection of Critical Infrastructure, above or under the sea surface, especially since Russia uses energy as the means to achieve political goals and to support its foreign policy.

The use of new technologies can be considered an opportunity, providing a support to monitor and to protect, but also a risk, when used with malicious purpose.
A change in mentality and a new coherent and genuine collaboration between Allies and Partners is deemed necessary to share the awareness and to reduce the potential common weakness.
Hybrid warfare represents also a challenge to the Energy Sector and have the potential to disrupt, apart from the national security, the NATO's political and military effectiveness and cohesion. It will take time and effort to counter these threats.
Therefore, the Alliance has to address dependencies and collaboration among its members and act as a platform, to build

a common picture of complex operational risk and vulnerabilities.
Due to the size and scale of the maritime enterprise cyberspace, where various stakeholders (industry, commercial, civilian, military) are operating and interacting, makes it a particular advantageous environment for potential cyber malicious actors who are becoming more and more sophisticated in technics and tactics.

Again, ongoing armed conflicts like Ukraine's have shown us that cyberspace operations are being actually conducted in support of strategic objectives, by disrupting the availability of critical national services and infrastructures.
Cyber threat information sharing, cyberspace situational awareness, enterprise approach in cyber security policies and measures, and finally collaborative cyber incident response and handling are therefore considered paramount for resilience and require a coherent network of civilian, industrial, commercial and military cyber defense strategies and operations.

Consequently, on the upcoming years we will see an even stronger focus on education and training in Energy Security. More energy – related injects will be incorporated in the tabletop exercises and more scenarios will be related to the protection of critical Maritime energy infrastructure.

The bridge building between the military, industry and the private sectors, the fusion of different approaches and the development of common understanding, must lead to productive cooperation and synergies.
All the maritime enterprises need to undermine and oppose to nefarious activities against maritime energy infrastructures in all the domains, weather they come from terrorists, organized crime or hostile states having in mind the global threats changing landscape.

It is needed an extensive transformation to the classical approach to the problem in order to develop a multi domain strategy that involves governmental and civilian entities, collaborating and standing together to face, deter and defend from current and potential future adversaries.

In that vein, the role of the related NATO Education and Training Facilities, as NMIOTC, will be equally important and therefore, we expect NMIOTC to assume a pivotal role also in that field, as the maritime interdiction operations are not only closely related to, but also a critical enabler to mitigate the risks and counter those threats.

Themistoklis Papadimitriou
Commodore GRC (N)
Commandant NMIOTC

NMIOTC
14th Annual Conference, 2023

by Dinos Kerigan-Kyrou

The following is a summary, with reflections and analysis, of the 14th NMIOTC Annual Conference. The event focused on energy and critical infrastructure security. The summary will begin by highlighting the Keynote speeches addressing the challenges we face across NATO, Partner Nations, and the European Union. It will then cover the presentations and panel discussions which took place during the two days of the conference, before drawing some conclusions and reflections.[1]

The conference covered four key areas of maritime critical infrastructure security:
+ Security of Critical Sea Lanes of Energy Transportation.
+ Critical Underwater Infrastructure Challenges.
+ Protecting Critical Maritime Infrastructure.
+ Emerging Technology Trends in Energy Security.

Keynote Addresses

NMIOTC Cdre Themistoklis Papadimitriou highlighted that as NMIOTC is the NATO accredited facility for training in the maritime domain, its role is essential for our security - both maritime security and critical infrastructure security. Critical Maritime Infrastructure (CMI) faces substantial security challenges from hostile states, terrorists, and criminals. However, infrastructure such as harbours are difficult to protect from determined adversaries. The consequences of failing to protect these critical infrastructures can potentially lead to disastrous outcomes. Because of this, protecting critical infrastructure has become a central NATO priority. Nonetheless, we need to continually increase awareness and address weaknesses in the protection of CMI. Indeed, NMIOTC is preparing a new critical infrastructure and energy protection course for NATO, EU, and Partner Nations.
To address these challenges we need to better develop our information-sharing, and build and continually develop collaborative relationships within and across NATO, the European Union, and with partners, including industry.
While we need to develop methods to protect our CMI, we also need to adapt to the new strategic landscape.
NMIOTC will continue to bring together stakeholders including academia, military, and other experts. This collaboration will develop a common understanding and develop synergies, raising awareness to prevent catastrophic maritime events. NMIOTC will support the central role of NATO Allied Command Transformation (ACT) in these challenges going forward. NMIOTC is ready for these challenges, concluded Cdre Papadimitriou.

[1] Many thanks to CDR Caoimhin MacUnfraidh, Commandant of the Irish Defence Forces Naval College & Associate Head of the National Maritime University of Ireland, for his invaluable contribution to this summary analysis of the 2023 NMIOTC Annual Conference.

Lt Gen Georgios Kyriakou, Chief of Staff, Hellenic National Defense General Staff stated Europe is presently totally dependent on imported energy; supply disruptions directly affect security across Europe. We need therefore to diversify the energy mix and the energy market. Nonetheless, we rely increasingly on critical infrastructure in the maritime domain; for example, specialised floating storage units, ports, and platforms. Protecting these assets from existing and emerging threats is essential.

We therefore need to develop strategy, training, and cyber resilience. We need to improve intelligence and information sharing - this requires cooperation between government, military, the energy sector, NATO and the EU. It also requires a change of mindset in how we go about addressing these challenges.

Greece is a pillar of stability in the Mediterranean Sea and indeed in the wider region. The Hellenic Armed Forces are constantly building relations bilaterally and multilaterally with partner nations; NMIOTC has led much of the necessary training which further develops this stability and progress.

Finally, the functioning of NMIOTC is made possible by its sponsor nations. NMIOTC invites NATO and Partner Nations to play a central sponsoring role in NMIOTC's invaluable and critical work securing the maritime environment.

David van Weel, NATO Assistant Secretary General for Emerging Security Challenges said that energy security has a hugely significant maritime dimension. Moreover, new pipelines and suppliers, hydraulic fracturing, deep drilling, and Liquefied Natural Gas (LNG), have all dramatically changed the global energy market. Moreover, we are slowly moving away from Fossil Fuels. Wind power, solar, hydrogen fuel cells and biofuels do indeed promise new clean energy. However, the full potential of renewable, clean energy can only be fully realised by tackling the real and major security challenges we now face. There are three main concerns and challenges:

A) New energy will increase reliance on maritime security. For example, LNG transported by sea comprises 40% of European Union gas demand.

B) We need to pay much more attention to our critical energy infrastructure, especially the undersea infrastructure. This importance will increase as offshore power production multiples by over 300% over the next few years. However, the transmission of this energy will often depend on a single vulnerable cable.

C) We need to be working closely with the companies responsible for the infrastructure as they are the experts on its design, maintenance, and operation; they are best placed to monitor their own infrastructure. But our navies have world-leading knowledge in maritime security, including application of deterrence, and when needed, interdiction. NATO and Partner Nations need to be working closely with the commercial companies, combining our knowledge of security with their expertise in the actual infrastructure and its operation.

Training takes on a much bigger importance. We must be able to test and improve realistic exercises in the protection of maritime critical infrastructure. NMIOTC plays the central, critical role in the pursuit of maritime security excellence.

Indeed, NATO has always been a maritime alliance. Today, energy challenges have transformed the way we need to invest in our maritime environment to ensure that we have capabilities which combine both military security and energy security.

Prof James Bergeron, Political Advisor to the Commander, NATO Allied Maritime Command (MARCOM), stated that MARCOM has never been as busy or robust as since the February 2022 horrific, unprovoked, and illegal invasion of Ukraine. A pan area responsibility is critical for coordination between NATO nations at sea. 50 frigates and destroyers and 30 minesweepers were deployed by NATO in 2022. The USS *Harry Truman* [Nimitz-Class aircraft carrier], is under NATO command, as is HMS *Prince of Wales* [Queen Elizabeth Class aircraft carrier], the aircraft carrier flagship of France *Charles De Gaulle,* and the aircraft carrier flagship of Italy *Cavour.*

MARCOM is fully resourced with 485 military and civilian personnel at Northwood, UK. Its coordination with NATO national commands is crucial for its ability to deliver deterrence.

In 2022, shortly after the invasion of Ukraine there was an uncertainty as to how far Russia would go in targeting NATO. Command and coordination, and understanding of the maritime domain is vital for MARCOM and NATO's security. MARCOM needs information and knowledge from experts such as NMIOTC.

MARCOM's analysis is that closer liaison between the military and civilian realms is vital. Indeed, the Critical Undersea Infrastructure Coordination Cell at NATO Headquarters will take on increasing importance. NATO needs to increasingly work with the European Union in the defence, protection, and resilience of critical maritime infrastructure.

But our ongoing task of maritime situational awareness is under threat, so we need to be leveraging new technologies such as Artificial Intelligence (AI). Airborne surveillance in the visible magnetic spectrum, such as drones, and the Airbus surveillance services are increasingly important.

Presently MARCOM is lacking specific info about sea networks. There may be areas of technology we simply do not know about. Thus, anything that can help make sense of the information we receive - including analysis - will very much help NATO's maritime security.

In the subsurface undersea environment there is a need to increase the detection of the presence of potential saboteurs. Unmanned Underwater Vehicles (UUVs), acoustic sensing, and other sensors have great potential to develop understanding of the subsurface environment.

Communications and the role of NATO StratCom will become increasingly significant to the security of the maritime environment. Many attacks and security challenges we face will be denied by our adversaries. We need to develop the ability to 'Deny the deniability', to prevent successful false communication by our adversaries.

In addition, we need to reduce to zero our use of Russian gas, and increase imports of LNG from allied states. We need to further decarbonise and develop new energy technologies including wind from the North Sea and Baltics. But the cables connecting these facilities are vulnerable. We need training, expertise, and exercises. The nature of interdiction has changed to include counterterrorism, counterpiracy, and countertrafficking, but we are now having to defend static infrastructure at sea. Prof Bergeron concluded by stating the main issue we face: How do we take these decades of tactical knowledge and apply them to these new challenges?

RADM Stefano Turchetto, Operational Commander European Union (EU) NAVFOR MED Operation IRINI emphasised the importance of IRINI in monitoring and enforcing the Libyan arms embargo. EU IRINI is also identifying illegal oil transfers from Libya, and supporting the detection, monitoring, and prevention of human-trafficking. IRINI is building capacity and providing training, law enforcement, information-sharing, and search-and-rescue activities. All of these tasks are part of an EU coordinated approach within EU EEAS (European External Action Service).

IRINI identifies and disrupts nefarious activities, and plays an essential role in safeguarding the maritime domain. (For example, IRINI has intercepted several ships and cargos, including armoured personnel carriers destined for Libya in violation of United Nations sanctions).

Creating strategic maritime awareness through operational ability and training is indispensable; the European Union is working closely with EU member Greece and NMIOTC in order to achieve this.

While EU IRINI's mandate is focused specifically on Libya, IRINI also monitors and disrupts a range of nefarious activities. This engagement at sea - enchaining the maritime domain's security - is critical to our entire security.

Brig Gen Bart Laurent, Director of Operations, EU Military Staff (EUMS), spoke about the new EU Maritime Security Strategy and its connection to energy security of

the maritime domain, from the perspective of the EUMS.
Brig Gen Laurent emphasised the wide scope and scale of EU military CSDP (EU Common Security and Defence Policy) Operations and Missions, stating that there are presently nine military CSDP Operations and Missions and 13 civilian Missions. Indeed, there have been a total of 41 EU CSDP Operations and Missions in the past, including missions as far afield as the Gulf of Guinea and the Northwest Indian Ocean.
EUMS tasks include Military Planning at the political-strategic level, Concept and Capabilities development, supporting the MPCC (Military Planning and Conduct Capability), and supporting activities across the world. Early warning, situational assessment, and strategic partnerships are key to EUMS. The EU Military Staff Intelligence Directorate (EUMS INT) is directly involved in this work. Information collection and sharing is of critical importance.
Brig Gen Laurent stated that the EU has recently updated its Maritime Security Strategy. We are therefore looking at a combination of traditional threats, hybrid threats and cyber-attacks, as well as security challenges from climate change and enhancing environmental protection.
99% of data traverses undersea cables. 2/3 of the world's oil and gas is transported via the maritime environment, and over 80% of global trade is transported across the sea. Trafficking of humans, drugs, and piracy are all new and emerging threats. The use of unmanned sea vehicles is changing the threat landscape.
EU Maritime Security Strategy Objectives include stepping-up EU activities at sea. These include organising yearly naval exercises, developing coastguard operations, and designating new maritime areas of interest (MAI). Cooperation with partners, especially EU-NATO cooperation is absolutely imperative.
The EU is rapidly developing its maritime domain awareness capabilities. For example, the Common Information Sharing Environment, the European Defence Agency's MARSUR (Maritime Surveillance), and integrating space-based technologies are all vital in achieving this.
It is crucial to manage risks and threats by enhancing live maritime exercises, enhancing capabilities, and developing common requirements for defence technology. This is in addition to developing education and training to incorporate cybersecurity and hybrid threat qualifications. This education and training is key to protecting critical infrastructure.
Hybrid Centre of Excellence Helsinki is of great importance to maritime critical infrastructure security and its Handbook on Maritime Hybrid Threats is hugely relevant to the work of NMIOTC.
Brig Gen Laurent added that increased investment in platforms such as the EU patrol ship projects being advanced by the EU EDA (European Defence Agency) and in other PESCO (EU military Permanent Structured Cooperation) programmes relating to sub-sea capabilities, harbour protection, and information sharing is required.

Panel Discussions

Summary of Panel The Security of Critical Sea Lanes of Energy Transportation[2]
The changing nature of Black Sea Security, especially in the light of Russia's illegal invasion of Ukraine, and how technology is transforming our approach in countering Russia in the Black Sea region was emphasised throughout this panel. Presentations focused on the motivation of Russia in seizing the Crimean coast, showing that the corresponding Exclusive Economic Zone (EEZ), now claimed by Russia, is a substantial portion of the entire Black Sea. Russian forces have hit 10 merchant ships during the conflict, and a further 94 merchant ships are immobilised in ports.
Artificial Intelligence (AI), including Natural Language Processing is changing how we approach maritime security. Deep Learning AI will transform the maritime security landscape. Indeed, AI will be essential for the mapping and data-crunching that enables the analysis of maritime critical infrastructure incidents.
Cooperation in intelligence-led infrastructure assessments (particularly focusing on the infrastructure nodes), in order to make informed decisions about deterrence and protection needs to be deepened across NATO and Partners so we can make informed decisions. In addition to naval tactical requirements (ships at sea, aircraft, etc), there is a need to increase the persistence and presence of subsea assets including subsea sensing; for example, Sound Surveillance Systems and Autonomous Underwater Vehicles (AUVs). Information-sharing and cooperation between all partners must continually improve. The panel discussed and stressed the critical importance of Egypt's Role in the security of the Mediterranean and further afield.

Summary of Critical Underwater Infrastructure: Current and Future Challenges[3]
While there has been a huge increase in the number of communication subsea cables there has actually been a reduction in the number of oil and gas pipelines. So it is communications and internet cables that are becoming an increasing target for those that wish to cause harm.
Subsea cables carry US$ / Euro 8-10 trillion in daily financial transactions. Moreover, subsea infrastructure - Criti-

[2] Speakers on The Security of Critical Sea Lanes of Energy Transportation: CDR Sameh Mohamed Abdelkhalek Elkelany, Egyptian Naval Liaison Officer, Egyptian Embassy, Greece; Captain Chirea Nicu, Dep Commander of the Romanian Fleet; Dr Siyana Lutzkanovam, Head of the National Security Dept at Nikola Vaptsarov Naval Academy. Moderator: Dinos Kerigan-Kyrou.

cal Underwater Infrastructure (CUI) - is needed for facilitating global cloud computing and AI. Demand doubles for subsea infrastructure every two years.

Patrolling the pipeline environment at sea and limiting the threat faced is a formidable process. The concentration of static infrastructure in hubs and nodes presents a significant target for nefarious actors, making protection difficult. A great deal of information about this CUI is available online for anyone to discover. Because of this, information-sharing between stakeholders is very much needed for the secure operation of cables and critical infrastructure. However, poor coordination between the large number of stakeholders - owners, insurers, reinsurers, operators, contractors, specialists and others - makes achieving agreement on security measures a considerable challenge.

There is an increased use of automation and online connection for the operation of critical infrastructure at sea (for example offshore oil and gas platforms and wind turbines), and of CUI. While this interconnection produces huge efficiencies, it also raises the risk of cyberattacks, and of technical failures.

However, accidents and negligence are actually the biggest cause of problems to undersea cables rather than sabotage or attack. For example, trawler fishing accounts for 80% of undersea cable damage. Nonetheless, Russian 'research vehicles' interfere and disrupt sea based critical infrastructure regularly. Indeed, the seafloor and the cables they 'discover and research' can be exploited for espionage and data gathering. For example, the Russian vessel Yantar can operate subsea vehicles at depths of up to 6 km, so it is able to reach almost all CMI regardless of depth.

Attacks on critical infrastructure can be made under the cover of plausible deniability. Moreover, these attacks can also be directed by non-state actors, be they terrorists, mercenaries, or combinations of both.

Resilience and redundancy, developing joint undersea infrastructure repairs, joint naval protocols in the subsea environment, supporting R&D, and developing common standards are all important. But these can only happen with much more coordination between stakeholders. Working with partners, such as insurance companies, the flag states, the shipping and logistics companies, is vital.

MARCOM can potentially act as the 24/7 point of contact for nations in managing CUI awareness and coordination of operations. To do this we need a better understanding of what the CUI actually does. What sector are we trying to protect? What are the choke points / key nodes of the CUI? We need to be able to Assure, Deter, Detect, and Respond to known and unknown threats and challenges in the subsea environment.

We should also be learning from the success of what happened with preventing piracy at sea: Navies enabled and encouraged the commercial shipping industry to be much more resilient. And this is relevant because many organisations and companies are looking to develop ocean resources, but not many are looking at their actual protection. We need to raise awareness and develop information-sharing to protect these assets. The great successes we have achieved against piracy have come about through cooperation, rather than militarization, it was suggested. Indeed, a question was raised "Are we at risk 'over militarizing' challenges to Critical Maritime Infrastructure?"

The subsea cables around the African continent are located at a critical juncture for the world's communications and internet. The protection of these assets is not only key for Africa, but for the economy and well-being of the entire international community. For example, '2Africa' is a 45,000 km subsea cable system (encircling the entire continent, connecting the whole of Africa with the EU, as well as the Gulf States, Pakistan, and India), and the largest cable project in the world that will facilitate communications for over three billion people.

Likewise, the energy pipelines linking the African continent and Europe are a prime example of critical, yet potentially vulnerable, CMI. These pipelines are in relatively shallow waters, and thus more exposed to threat. For example, the TransMed gas pipeline (from Algeria, through Tunisia to Italy), is only 145 km long with a maximum depth of 600m. TransMed transports a vast amount of gas (over 30 billion cubic metres per annum), from north Africa to Europe. Likewise, the Greenstream gas pipeline from Libya to Sicily is critical for European energy supply and the Libyan economy - but it is also potentially susceptible to nefarious activity. To help secure this infrastructure the Italian Ship Anteo, a submarine rescue ship of the Italian Navy, is tasked with protecting CMI. Divers can reach 30m, while its remotely operated vehicles can reach a depth of up to 1500m. It was reported (although not confirmed), that the Italian Navy recently discovered a submarine - possibly a submersible belonging to a hostile actor - beside a pipeline near Trapani. The incident highlighted the lack of a legal framework to allow intervention in such circumstances. The presence of the submersible - although potentially threatening - was not technically illegal.

We need to combine our ability to operate in the underwater environment with our ability to operate against opponents on the seabed. The Italian Navy proposes to clas-

[3] Speakers on Critical Underwater Infrastructure: Current and Future Challenges (Panel 1): Ognyan Savov, Bulgarian Maritime Training Centre; Ben Caves and Charlotte Kleberg, RAND Europe; Capt Niels Markussen DNK (N), Director of NATO Shipping Centre, NATO MARCOM. (Panel 2): Capt Navy (Retd), Mark Blaine. Institute for Governance & Leadership in Africa, Stellenbosch University, Cape Town; CDR Antonio Manno, Italian Navy General Staff; Dr Georgi Georgiev, Maritime Capabilities Support EU European Defence Agency. Moderator: Prof James Bergeron, NATO MARCOM.

sify this activity as a new fifth physical domain i.e. land, sea, air, space and now, seabed. Italy will propose Seabed Warfare as a new physical domain to NATO that lies beyond the traditional anti-submarine and mine warfare of the sea domain. This new form of warfare is developing and moving on from submarine and mine warfare. Seabed Warfare includes the protection of critical infrastructure. Protecting these assets, monitoring the environment, and neutralising threats is central to our security. The use of sensors and possibly special forces to do this will become necessary. But we need to develop these soon as presently we have 'Subsea Blindness.'

For the EU the priority for the European Defence Agency (EDA), is maritime situational awareness, harbour protection, and the developing issue of Seabed Warfare. Threats identified by the EU include smuggling, illegal fishing, terrorism, espionage, the vulnerability of huge data traffic flows, trade, energy supply, and digitization of the maritime environment. However, there are very few repair ships in the EU or ways of dealing with both security and technical problems; this needs to be addressed.

Siloed governance between state, security services, and commercial companies is harmful for the security of our maritime environment - especially when combined with the emergence of new security challenges. Breaking down silos which prevent collaboration must start at the lowest levels.

Critical Maritime Infrastructure is vulnerable, and the threats are increasing; we must be expanding control capability into the deep sea. No actor can face these threats alone; military and industry have significant roles to fulfil. The EDA is continuously studying this environment, running tabletop exercises, and is organising a second symposium on CMI. The EDA lists six PESCO projects active in relation to CMI, demonstrating concern at the EU level for the vulnerability of CMI and an awareness of the impact on society of its disruption.

The panel also emphasised the importance of infrastructure security assessments. But for these assessments and audits to be effective we need to start determining and defining what actually constitutes Critical Maritime Infrastructure. Because without working definitions we cannot possibly make accurate assessments of vulnerabilities, nor can we propose effective security solutions.

Summary of The Protection of Critical Maritime Infrastructure[4]

The Nord Stream situation was discussed by several of the panellists. It was agreed that Nord Stream has substantially increased focus and awareness, particularly regarding CMI resilience.

The panel proposed that we need to define CMI not as critical points 'on the map' but as critical entities. Moreover, developing security means developing redundancy. Communications critical infrastructure offers redundancy via its networks. Energy pipelines, however, have no redundancy.

We need to Detect, Deter, Identify and Neutralize threats to CMI. Acoustic sensing on the seabed is of great importance to help do this, as is civilian / military cooperation in seabed protection.

The threat to critical CMI is real - major incidents are going to occur. Therefore, we need to do much more to align national procedures. Military and civilian exchanges of information need improving, and the role of NATO and the EU is critical. We need a multinational approach involving the owners of the infrastructure. We need common and realistic life-like exercises - such as the EU coastguard exercise COASTEX in Italy, organised by the EU border agency FRONTEX.

Moreover, many of these problems are not new. A map from 1901 that was displayed showing critical undersea cables did not look dissimilar to undersea infrastructure maps of today. Indeed, undersea cables were targeted extensively in WW1. And the panel also mentioned the 1981 Operation Ivy Bells which intercepted Soviet communication off the Kamchatka Peninsula. But today everything we do involves the internet and cyberspace. Subsea cables carry all the information we need every day. And since the 2022 invasion of Ukraine sea transport of energy has hugely increased making us all more dependent than ever on Critical Maritime Infrastructure.

Current monitoring of Critical Underwater Infrastructure is not sufficient; the result of this is that we identify problems much too late. Moreover, we need to be changing the questions we ask. For example: Do the security challenges of the seabed actually start and end with the seabed? We may need a much more holistic approach; underwater situational awareness may well be essential in achieving this. We need to use technology such as sensors, smart cables, and distributed acoustic sensing, as well as working with commercial partners. We may need a more comprehensive effort combining surveillance, reconnaissance, Anti-submarine Warfare, Anti-Surface Warfare, and a much broader strategy to address these challenges. In international law we are missing a protection that expressly protects subsea critical infrastructure.

The Eastern Mediterranean presents new energy opportunities, but there are also security challenges, the panel stated. Enhancing regional cooperation, diplomacy and conflict resolution, incorporating UNCLOS (United Nations Convention on the Law of the Sea), is of great importance.

[4] Speakers on The Protection of Critical Maritime Infrastructure: CDR K De Winter Bel (N) Director of Maritime Ops Center, Admiralty BENELUX; Ltr Cdr S CANARUTTO, Italian Navy General Staff; Capt Athanasios Moustakis Hellenic Navy General Staff. Moderator: Dr Iosif Progoulakis, Dept of Shipping, Trade and Transport University of the Aegean, Chios, Greece.

We need to cooperate internationally and to cooperate with industry. Industry has always focused on safety, but now needs to focus much more on security.

Summary of Emerging Technology Trends in Energy Security[5]

A number of key questions, as well as possible solutions were raised in this final panel.

We depend on electricity for our economies; without it our economies collapse. Protecting the supply of electricity is fundamental for our security. Remote Inspection techniques of CMI are vital: we need to develop how we do these - but we have not adequately done this yet. Unmanned boats are being used by drug smugglers and terrorists. The US Navy Digital Horizon 2022 project seeks how to address such threats, especially by utilising - and possibly countering - Unmanned Surface Vehicles. We need to build on programmes and initiatives such as Digital Horizon 2022.

Each year a substantial number of oil and gas facilities are boarded illegally, sometimes by hostile state actors. And in addition to hostile states, we have the threat of terrorism, extreme activism (including extreme environmental activism), criminals, and disgruntled employees or contractors (insider threat), who want to cause harm to infrastructure. The effects of these illegal activities lead to a substantial number of deaths and injuries each year.

We need to think about our supply routes for energy and communications. Are these supply routes resilient? Probably not. Likewise, there is a need to re-think cybersecurity. How can we do this to protect against evolving threats? What about the way we perceive risk to CMI? Are we analysing these risks correctly? What assumptions might we be making which are possibly dangerous to us and simultaneously of benefit to our adversaries?

Overall Summary and Ways Forward

To address Critical Maritime Infrastructure security, we need to develop our information-sharing, and build much improved collaborative relationships within and across NATO, the European Union, and with industry. We need to develop operational methods to protect our CMI, but we also need to adapt to the new strategic landscape. That landscape has changed, possibly forever, following the horrendous and illegal invasions of Ukraine in 2014 and 2022.

In many ways it is the threat of interference to our CMI that must be addressed. The interference itself when it occurs is much harder to fight because the initiative, over a vast geographic area, lies with the attacker, not the defender. It is the 'concentration of vulnerability' that differentiates CMI from shore-based critical infrastructure. Indeed, onshore infrastructure is more dispersed, has intrinsic redundancy, and is usually much more easily and quickly repaired following damage - whether that damage is accidental or deliberate.

Protection means we must Assure, Deter, Detect and Respond. Protection also involves a clear StratCom communications strategy to 'Deny Deniability.' Naval deterrence is critical; demonstrating that we understand the adversary is a threat and that their actions can - and will - be exposed. In other words, making the adversary's 'deniability' far less plausible and of less value to them than at present. This is a central security aspect of CMI, in addition to the kinetic military actions that NATO, the EU, and NATO's Partner Nations can deploy.

Critical Maritime Infrastructure protection requires us to prevent - as far as possible - detrimental situations to our CMI from occurring in the first place. While deterrence is indeed a traditional naval task spanning centuries, it is given far greater urgency and relevance by the current situation. We need to be rethinking and reevaluating our naval deterrence broadly and holistically to address new and emerging security challenges to our Critical Maritime Infrastructure.

Dinos Kerigan-Kyrou PhD CMILT

Dinos leads and coordinates the cybersecurity and hybrid threats education for the Irish Defence Forces Joint Command & Staff Course. Dinos is a NATO Defence Education Enhancement Programme (NATO DEEP), instructor (for cybersecurity and hybrid security challenges), and a military educational advisor at the Partnership for Peace Consortium of Defense Academies (PfPC), based at the George C. Marshall Center, Garmisch-Partenkirchen. He is a co-author of the NATO/PfPC Cybersecurity Reference Curriculum and the new Hybrid Threats & Hybrid Warfare Reference Curriculum. He coordinated and instructed the initial military education on critical infrastructure security and resilience at the NATO School Oberammergau from 2011 to 2015. Dinos was an inaugural member of the PfPC Emerging Security Challenges Working Group (ESC WG), when it was established in 2013 to liaise with NATO's Emerging Security Challenges Division, and is today a Subject Matter Expert member of the ESC WG. He is a member of the PfPC Advanced Distributed Learning (ADL) Working Group, developing blended and hybrid learning for NATO and Partner Nations. Dinos is an editor of the PfPC journal *Connections*, published by USEUCOM. He is an Associate Member of the Royal Institution of Naval Architects, and a board member of Digital Business Ireland.

[5] Speakers on Emerging Technology Trends in Energy Security: Prof. Dimitrios Dalaklis, Assistant Professor, World Maritime University, Sweden; Tafsir Johansson, World Maritime University; Asst. Prof. George Stergiopoulos, University of the Aegean (GR); Marios-Theodoros Kampolis, TMS Cardiff Gas Ltd (TMS Group) (GR); Michalis Michaloliakos, TMS Cardiff Gas Ltd (TMS Group) (GR) CAPT (ret.) Edward Lundquist, U.S. Navy; Dr. Iosif Progoulakis, University of the Aegean. Moderator: Prof Dimitris Gritzalis, Dept of Informatics, Athens University of Economics and Business.

State accountability in seabed extraction of oil*

by Ognyan Savov

Introduction

Each country, being the owner of its natural resources, has the right to exploit them as it wishes. However, this right is associated with the duty to prevent significant transboundary harm unless an agreement to the contrary exists. In other words, it does not mean no pollution at all, but that the polluter does not cause significant pollution[1]. Thus, a total ban on pollution prevention would not be necessary especially when the burdens in avoiding it are excessive compared to the results achieved[2]. However, having in mind the long history of oil pollution incidents as well as the existing number of marine compensation treaties relating to oil pollution, one could be right in concluding that no matter the quantity of spilt oil, the polluting substance is the precursor for the presence of the element of significance.

The purpose of this article is to argue that regardless that the transboundary victims from seabed extraction activities have a number of options to enforce their rights following transboundary pollution, in reality this task is very hard and the loss would lie where it falls. Moreover, against all odds, the engaged States shy away from their obligations to rectify the situation and, thus, tend to avoid accountability.

Liability and responsibility

Seabed oil extraction is a legal activity. Nonetheless, lacking an agreement to the contrary, the transboundary pollution consequences of an otherwise legal activity are illegal. The consequences of a legal activity raise liability while an illegal one – responsibility[3]. Responsibility triggers restitution, compensation or a combination of the two[4]. And since the general position is that State accountability in

* This article is based on a presentation the author made during the 14th NATO Maritime Interdiction Operational Training Centre (NMIOTC) Conference in Souda Bay, Crete, Greece (June 7-8 2023)

[1] Tanaka Y 'Regulation of Land-based Marine Pollution' (2016) vol. III *IMLI Manual on International Maritime Law* 139 at 143

[2] Guiding Principle A(a)(3) of Organisation for Economic Co-operation and Development (OECD) *Recommendation of the Council on Guiding Principles concerning International Economic Aspects of Environmental Policies*, 1972 (OECD/LEGAL/0102)

[3] ILC *Draft Articles on Responsibility of States for Internationally Wrongful Acts* (2001), ILC *Draft Articles on Prevention of Transboundary Harm from Hazardous Activities* (2001)

[4] *Ibid*

transboundary seabed oil pollution is unregulated by hard law[5] or that the existing soft law, whatever detailed it may be, does not impose any legal obligations[6], the wrongdoing State is still responsible for its omission to introduce adequate legislation on the process of dealing with the transboundary pollution. Therefore, it is to restitute and/or compensate the transboundary victims. In other words, a gap in law leads to State responsibility.

It is to note that in this research the term 'accountability' and its derivatives are used instead of liability and responsibility since its purpose is not to differentiate whether an action is legal or illegal but rather who is to bear the consequences.The Actors in question would be fairly consistent; an international terrorist group that had the wherewithal to plan and and conduct a maritime transit, whether that group was fully non-state or state-sponsored, would by definition be highly organized and capable. This fact, along with the definitional intention of terrorist actors to conduct or facilitate violent attacks, would leave state actors with no option but to organize for a highly-focused operation using their highest-end and most capable forces, acting based upon shared information and intelligence between participating coalition partners.

It is to note that in this research the term 'accountability' and its derivatives are used instead of liability and responsibility since its purpose is not to differentiate whether an action is legal or illegal but rather who is to bear the consequences.

State-investor relationship in seabed oil exploitation

Regardless that the wrongdoing State is to bear the consequences for transboundary pollution, a process that seems straightforward, in reality this is not so. It is so because in bringing one to justice, one is to ask the question who the wrongdoer is, what the law is and what its application in reality is.

Due to the nature of the seabed extraction activity, most States, known as the host States or licensors, are not able to conduct it on their own. Rather, they grant concession to a private company (the licensee, investor or operator) which may be domiciled in another State (home State). The investor may also be subject to multiple jurisdictions if consisting of different branches spread in different countries, in which case, the home State is the domicile of the holding company[7]. This structure is commonly known as a multinational company[8].

If the home State and the host State coincide, the relationship between the investor and the State are governed by the national law. However, should the investor be a foreign company, international investment regulations take precedence over domestic law. Moreover, the companies are sufficiently strong to influence the contractual terms to their advantage. Thus, while the host States may introduce national provisions benefiting their subjects, the same may be considered detrimental to the investors which may seek redress through litigation. In other words, the international companies are less accountable for the consequences they cause in the host State than at home.If the home State and the host State coincide, the relationship between the investor and the State are governed by the national law[9]. However, should the investor be a foreign company, international investment regulations take precedence over domestic law[10]. Moreover, the companies are sufficiently strong to influence the contractual terms to their advantage. Thus, while the host States may introduce national provisions benefiting their subjects, the same may be considered detrimental to the investors which may seek redress

[5] Regardless that there are two global treaties that relate to seabed oil exploitation which step in once pollution has occurred, they are unconcerned with the pollution itself but with the consequences of the intervention activities; see Convention on Limitation of Liability for Maritime Claims, 1976 (London, 19.11.1976)) [UNTS 970 (p 211)] and International Convention on Oil Pollution Preparedness, Response and Co-operation (London, 30.11.1990) [UNTS 1891 (p 78)]; It may be argued that the Convention on Limitation of Liability for Maritime Claims provides for the transboundary victims but it is of very limited application and its compensation cap is highly insufficient. Moreover, unlike the former two conventions, it is silent on the accountability of the States; see Convention on Limitation of Liability for Maritime Claims, 1976 (London, 19.11.1976) [UNTS 1456 (p 221)]; On a regional scale, States have been more active, but the result is also flawed. Within EU, those are Directive 2004/35/CE of the European Parliament and of the Council of 21 April 2004 on Environmental Liability with Regard to the Prevention and Remedying of Environmental Damage *OJ L 143, 30.4.2004, p. 56*, Directive 2013/30/EU of The European Parliament and of the Council of 12 June 2013 on Safety of Offshore Oil and Gas Operations and Amending Directive 2004/35/EC *OJ L 178, 28.06.2013, p. 66*, Directive 2008/56/EC of the European Parliament and of the Council of 17 June 2008 Establishing a Framework for Community Action in the Field of Marine Environmental Policy (Marine Strategy Framework Directive) *OJ L 164, 25.6.2008, p. 19*, Directive 2014/89/EU of the European Parliament and of the Council of 23 July 2014 establishing a framework for maritime spatial planning *OJ L 257, 28.8.2014, p. 135*

[6] International Union for the Conservation of Nature and Natural Resources *Draft International Covenant on Environment and Development* (2015); ILA *Rules on Transnational Enforcement of Environmental La*w (Res 6/2006, 07.06.2006); United Nations Environmental Programme 'Environmental Guidelines and Principles: Offshore Mining and Drilling' (31.05.1982)

[7] UNCTAD 'World Investment Report 2007: Transnational Corporations, Extractive Industries and Development' (2007) at 245 available https://unctad.org/en/docs/wir2007_en.pdf (20.06.2023)

[8] UN 'Draft United Nations Code of Conduct on Transnational Corporations' (1984) 23(3) *International Legal Materials* 626 at 626; UNCTAD/TDR/17 – 'World Investment Report 1997: Transnational Corporations, Market Structure and Competition Policy' (1997)

[9] Leal-Arcas R and Nadule V 'Multilateral and Bilateral Energy Investment Treaties' in Chaisse J et al (eds) Handbook of International Investment Law and Policy, 1st ed (2021) Springer 3 at 4; Sornarajah M The International Law on Foreign Investment, 3rd ed (2010) Cambridge University Press 60; Eberhardt P et al 'One Treaty to Rule Them All' (June 2018) Corporate Europe Observatory (CEO) and Transnational Institute (TNI) available https://energy-charter-dirty-secrets.org/wp-content/uploads/2019/12/One-treaty-to-rule-them-all.pdf (20.06.2023)

[10] Ibid

through litigation[11]. In other words, the international companies are less accountable for the consequences they cause in the host State than at home[12].

Furthermore, because the investor is not a subject under international law and does not have legal personality[13], lacking an agreement, it cannot be a party to an international dispute[14].

And since there is no universal interpretation of the obligations of the companies for their overseas activities[15], different opinions exist as regards making them directly accountable in international law. Some argue for their treatment as subjects[16] due to the influence they have[17]. Others, it is the home State to be vicariously accountable since it is its duty to serve as a compliance watch-dog[18]. In third instances, it may be claimed that the host State is the one to blame for anything happening on its territory. Fourth, the host and home States are to be jointly and severally accountable.

As evidenced in case law[19] and elaborated on in soft law[20], there is a tendency that the duties of the investors increase in international law. Furthermore, nowadays, the host States are apt to renegotiate outdated investment treaties taking more into consideration their social and environmental obligations[21]. And depending on the language of the investment agreement, the ascertainment of investor's accountability may be referred to either the host[22] or home State legislation[23] or the international investment agreement, while litigation – to the court of the home or host States as well as an international tribunal[24].

Where there is a dispute, the judicial forum may take into consideration the fact that the company has not complied with the international standards and the social responsibility guidelines[25]. And it is almost certain that even in the absence of social policies in the investment agreement and the non-application of the principle of *stare decisis* in investment litigation, where the investment agreement has been concluded with the sole purpose of

[11] Red Carpet Courts 'Dirty Oil Attacks Action on Fossil Fuels: Rockhopper vs Italy' available https://10isdsstories.org/cases/case9/ (20.06.2023); For more on ongoing environmental litigation, see Verheecke L *et al* 'Red Carpet Courts – 10 Stories of How the Rich and Powerful Hijacked Justice' (June 2019) *Friends of the Earth, TNI and CEO* available http://10isdsstories.org/wp-content/uploads/2019/06/red-carpet-courts-WEB.pdf (20.06.2023); Provost C and Kennard M 'The Obscure Legal System that Lets Corporations Sue Countries' (10.06.2015) *The Guardian* available https://www.theguardian.com/business/2015/jun/10/obscure-legal-system-lets-corportations-sue-states-ttip-icsid (20.06.2023); Chasek P *et al Global Environmental Politics – Dilemmas in World Politics,* 7th ed (2018) Routledge 22

[12] Wenar L *Blood Oil: Tyrants, Violence, and the Rules that Run the World* (2016) Oxford University Press 216

[13] *Urbaser S.A. and Consorcio de Aguas Bilbao Bizkaia, Bilbao Biskaia Ur Partzuergoa v. The Argentine Republic*, ICSID Case No. ARB/07/26 para. 1195

[14] For a succinct overview of the host State-foreign investor relations, see Brabandere E and Van den Herik L 'Non- state Actors and Human Rights Obligations: Perspectives from International Investment Law and Arbitration' in Blokker N *et al Furthering the Frontiers of International Law: Sovereignty, Human Rights, Sustainable Development: Liber amicorum*, Nico Schrijer (2020) Brill 37 at 43-4

[15] Tzevelekos V 'In Search of Alternative Solutions: Can the State of Origin Be Held Internationally Responsible for Investors' Human Rights Abuses that Are Not Attributable to It?' (2010) 35 *Brooklyn Journal of International Law* 157 at 158

[16] *Ibid* at 227; De Jonge *A Transnational Corporations and International Law: Accountability in the Global Business Environment* (2011) Edward Elgar 83-4

[17] Benvenisti E 'Sovereigns as Trustees of Humanity: On the Accountability of States to Foreign Stakeholders' (2013) 107(2) *American Journal of International Law* 295 at 301

[18] Ryngaert C 'Jurisdiction: Toward A Reasonableness Tort' in Langford M (ed) *Global Justice, State Duties: The Extraterritorial Scope of Economic, Social and Cultural Rights in International Law* (2012) Cambridge University Press 192 at 208

[19] *Interamerican Court of Human Rights Advisory Opinion OC-23/17 of November 15, 2017 Requested by the Republic of Columbia* available https://www.corteidh.or.cr/docs/opiniones/seriea_23_ing.pdf (20.06.2023)

[20] Chapter 30 of Agenda 21 of 1992 Rio Declaration on Environment and Development in A/CONF.151/26/Rev.I (Vol. I) – 'Report of the United Nations Conference on Environment and Development Rio de Janeiro, 3-14 June 1992'; E/C.12/2011/1 – 'Committee on Economic, Social and Cultural Rights: Statement on the Obligations of States Parties regarding the Corporate Sector and Economic, Social and Cultural Rights' (20.05.2011) ; E/C.12/GC/24 – 'Committee on Economic, Social and Cultural Rights: General Comment No.24 (2017) on State Obligations under the International Covenant on Economic, Social and Cultural Rights in the Context of Business Activities' (10.08.2017); International Labour Organization 'Tripartite Declaration of Principles Concerning Multinational Enterprises and Social Policy, 5th ed' (2017); UN 'Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework'(2011)

[21] UNCTAD 'World Investment Report 2018' (2018) at 104; Brabandere E and Van den Herik L 'Non-state Actors and Human Rights Obligations: Perspectives from International Investment Law and Arbitration' in Blokker N *et al Furthering the Frontiers of International Law: Sovereignty, Human Rights, Sustainable Development: Liber amicorum, Nico Schrijer* (2020) Brill 37 at 37-8

[22] Art 9 of Agreement between the Government of the Sultanate of Oman and the Government of the Republic of Bulgaria on the Promotion and Reciprocal Protection of Investments (03.02.2007) available https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5433/download (20.06.2023)

[23] Art 20 of Reciprocal Investment Promotion and Protection Agreement between the Government of the Kingdom of Morocco and the Government of the Federal Republic of Nigeria (Abuja, 03.12.2016) available https://investmentpolicy.unctad.org/international-investment-agreements/treaty-files/5409/download (20.06.2023)

[24] Dabrowski L 'Arbitration Procedure in Bilateral Investment Treaties – Interactions between National, European and International Courts' in Teles P and Ribeiro M (eds) *Case-law and the Development of International Law: Contributions by International Courts and Tribunals* (2022) Brill 246 at 253-4

[25] Levashova Y 'The Accountability and Corporate Social Responsibility of Multinational Corporations for Transgressions in Host States through International Investment Law' (2018) 14(2) *Utrecht L Rev* 40 at 45

going against fundamental principles, the investor would be unsuccessful during litigation[26]. But still, as exemplified by the *Moorburg* saga, the investor-State relations are not always that clear-cut[27].

Moorburg is a village located on the coast of the Elbe in the vicinity of which a coal-powered factory was built in the 1980s. In 2008, the owner of the factory, Vattenfall, a Swedish-owned company, was granted a permit to use the Elbe's resources. However, the permit was associated with stringent conditions. Vattenfall succeeded in its claim for breach of the investment treaty[28] because the permit amounted to indirect expropriation. And this is regardless that the treaty specifies that the host State should take into consideration the environmental aspects[29]. Thus, the local authority rectified the permit by imposing less stringent duties on Vattenfall. But in 2017, the Court of Justice of EU found Germany accountable for granting the permit to Vattenfall because, by doing so, Germany had violated its duties under EU environmental law[30].

What is certain is that presently direct application of the international law norms on State accountability regarding the activity of the company does not seem to be contested only in those instances where its actions may be attributed to the State[31].

Since transboundary pollution never exists individually but is rather pollution occurring within the boundaries of a particular country developing later into transboundary, it is worth studying first how the host State and its communities may enforce their rights.

Claims against the licensee/ home State by the host State and its communities

The available options against the licensee and home State are the following: 1) should the host State wish to institute proceedings in an international court, they are to be initiated against the home State for its failure to control the licensee; 2) the licensor may bring a claim in its own courts; 3) the licensor may bring a claim in the courts of the home State; 4) the licensor may bring a claim in a third State having assets of the licensee or home State.

There is a fifth option created particularly for investment disputes. In order to govern their relations free from the influence of the changing political environment within the host State and bring certainty, specialised international fora have been created[32]. In other words, the international investment agreements follow more or less uniform international law providing the litigants with direct access to specialised international tribunals[33], thus avoiding haphazard litigation[34].

As regards the nationals of the host State, they may enforce their rights following options 2)–4) against the licensee as well as against the home and host States for their failure to exercise diligent control over the licensee. The claim against the latter two may also be initiated in an international court of human rights, such as the European Court of

[26] Metal-Tech Ltd v The Republic of Uzbekistan, ICSID Case No. ARB/10/3
[27] Provost C and Kennard M (n 11)
[28] Energy Charter Treaty (Lisbon, 17.12.1994) [UNTS 2080 (p 95)]
[29] Arts 18&19 of Energy Charter Treaty
[30] European Commission v Germany CJEU (Case C-142/16)
[31] See ARA Libertad (Argentina v. Ghana), Provisional Measures, Order of 15 December 2012, ITLOS Reports 2012, p. 332 on the difference between commercial and non-commercial activities carried out by the State
[32] Convention on the Settlement of Investment Disputes between States and Nationals of Other States (Washington, 18.03.1965) [UNTS 575 (p 159)]
[33] Sornarajah M (n 9) at 38
[34] At 62

Human Rights (ECtHR) should they have subscribed to its jurisdiction[35]. However, this option becomes available[36] once options 2) and 3) have been exhausted[37]. The exhaustion of options 2) and 3) is commonly known as 'exhaustion of local remedies'. As regards option 5), since the communities are not part of the investment agreement, they are not able to avail themselves to it.

In interstate litigation before an international court, one is to be aware of its bizarre status. The court does not have the power to hold the litigating States to its decision unless they have agreed to its jurisdiction which may be explicit or implied. If explicit, most probably the defendant State would comply with the order. If implied – for instance, from previous litigation to which it has been a party – the execution of the order might be impossible. In a 1973 nuclear dispute, New Zealand and Australia brought France to the International Court of Justice (ICJ) arguing that via its nuclear tests, France threatened their populations with the poisonous fallout[38]. However, France did not appear before ICJ[39] and ignored its interim order to cancel the tests[40].

Claims by the Victim States

In transboundary pollution, in addition to the licensing and home States, it is also the other States that are affected by it. The most obvious instance of the consequences is the accidents caused by installations located in border areas[41] or air pollution. Although the 1986 Chernobyl nuclear reactor blast did not attract any international litigation, several European States declared their firm intention to sue USSR[42]. Nonetheless, it was only the citizens that claimed in their domestic courts against their countries and USSR[43] while the victim States did not dare bring a single claim against USSR either domestically or internationally. Ultimately, for various reasons did the courts state that the claims against USSR were invalid and it was the victim States that dealt themselves with the consequences of the accident[44]. Following the present analysis, one is to be aware that should the State of origin or home State be brought to the court of the victim State, their own courts or the courts of third States with their assets, there is a tendency that a verdict against them would not be upheld since it is viewed as interference with State sovereignty as well as against the principle of equity[45]. However, this rule is not cast in stone and depends on the national legislation[46]. Moreover, due to the same reasons (sovereignty and equity), the victim States[47] are not willing to pursue international court litigation against the other States regardless that the extensive quantity of law shows that the victim States are within their rights to claim violation of rights. On the other hand, the victim State has the same options against the licensee as the host State with the exception of option 5). All in all, it is submitted that litigation against the licensee is the preferrable option in enforcing one's rights. Further evidence of the preference for the unsettled character of the interstate relations regarding the transboundary pollution consequences of seabed oil exploitation is the text of the 2019 Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters[48]. Unlike its 1971 predecessor[49], which is silent on its relation to transboundary issues, it enjoys a vast number of States

[35] ECtHR has pronounced in a number of cases that States have the obligation to take care of the protection of non-nationals whose rights may be violated by the nationals of the State in a third country; For a summary of ECtHR case law, see ECtHR 'Environment and the European Convention on Human Rights' (July 2022) available https://www.echr.coe.int/documents/fs_environment_eng.pdf (20.06.2023); However, while those ECtHR has pronounced in a number of cases that States have the obligation to take care of the protection of non-nationals whose rights may be violated by the nationals of the State in a third country; For a summary of ECtHR case law, see ECtHR 'Environment and the European Convention on Human Rights' (July 2022) available https://www.echr.coe.int/documents/fs_environment_eng.pdf (20.06.2023); However, while those cases refer to nationals suing their governments, in *Al-Skeini and Others v. the United Kingdom* (Application no. 55721/07), ECtHR upheld the claim of Iraqi citizens for violation of their rights by UK soldiers. And although the litigation was for the wrongful deaths of the applicants' relatives, this case nonetheless proves of the extraterritorial obligations of the States, which in light of the environmental jurisprudence of ECtHR should also mean violation of the rights to clean environment of non-citizens outside national borders; For a summary of the Al-Skeini case and its implications, see Human Rights Watch 'UK: Landmark Ruling in Iraq Case – European Court Says UK Violated Rights of Iraqis in Killings Case' (07.07.2011) available https://www.hrw.org/news/2011/07/07/uk-landmark-ruling-iraq-case (20.06.2023)

[36] Art 35 of Convention for the Protection of Human Rights and Fundamental Freedoms, (Rome, 04.11.1950) [UNTS 213 (p 221)] (ECHR)

[37] Trindade C 'Exhaustion of Local Remedies in International Law and the Role of National Courts' (1978) 17(3/4) *Archiv des Volkerrechts* 333 at 334; Nollkaemper A 'Cluster-Litigation in Cases of Transboundary Environmental Harm' in Krishna P (ed) *Transboundary Environmental Harm: Emerging Legal Regime* (2010) Amicus Books 30 at 32

[38] *Nuclear Tests (New Zealand v France)* 1974 I.C.J. Reports, p. 457; *Nuclear Tests (Australia v France)* 1974 I.C.J. Reports, p. 253

[39] *Nuclear Tests (New Zealand v France)* (ibid) at 461 (para 15)

[40] Merrill T 'Golden Rules for Transboundary Pollution' (1997) 46(5) *Duke LJ* 931 at 958

[41] For instance, a smelter factory *(Trail Smelter Case (United States, Canada),* 16 April 1938 and 11 March 1941, RIAA Vol. III pp. 1905–1982) or an upstream State having a nuclear facility using the river for cooling activities

[42] Rest A 'Need for an International Court for the Environment: Underdeveloped Legal Protection for the Individual in Transnational Litigation' (1994) 24(4) *Envtl Pol'y & L* 173 at 174-5

[43] *Ibid* at 175-9

[44] In more recent times, the Chernobyl consequences may be compared to two oil spills from seabed activities in 2009 and 2010 discussed later in this research where it had been argued that they have caused transboundary pollution

[45] The so-called 'clean hands doctrine'

[46] Greenwood C 'Unity and Diversity in International Law' in Andenas M and Bjorge E (eds) A Farewell to Fragmentation: Reassertion and Convergence in International Law (2015) Cambridge University Press 37 at 49-50 comparing Italian and UK case law

[47] It might be argued that this tendency is changing as evidenced by the number of environmental cases decided in recent times by the international tribunals

[48] the Hague, 02.07.2019

[49] Convention on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters (the Hague, 01.02.1971)

parties and is not applicable to transboundary marine pollution (Article 2(2)(g)). Moreover, between 2010 and 2017 the International Maritime Organization and its members missed the opportunity to clarify the rights and obligations of the States in seabed oil exploitation.

Communities of the transboundary victim States – the example of two oil spills

In 2010, the oil rig 'Deepwater Horizon', while engaged in the production of oil from the Macondo oil field on the US Gulf of Mexico continental shelf, exploded and sank causing a large environmental damage with oil leaking for several months to both US and Mexican shores. The oil rig was under the control of British Petroleum (BP) – a company with extensive experience in seabed oil production. Following a US suit, BP was found accountable for the loss suffered by the US citizens. As regards the Mexican victims, it took almost ten years to reach out-of-court settlement. However, it was concluded between the Mexican federal government and BP and there is a claim that the Mexican victims would not be compensated at all[50]. The second case, the 2009 Montara oil spill, took place in the Pacific Ocean offshore Australia resulting from lost well control of the Montara oil field operated by a subsidiary of a Thai company[51]. The Australian shores did not suffer environmental damage but the subsidiary was found accountable under the Australian legislation. At the same time, on the other side of the ocean, along the shores of the Indonesian islands, the local fishermen suffered extensively from oil pollution. The Indonesian government initiated actions against the subsidiary and holding companies accusing them of 'falsely claiming that oil never reached the Indonesian coast [and] of negotiating in bad faith'[52] in the Indonesian court. However, this claim was soon withdrawn and not brought again regardless that the reason for this was not an intention not to sue the operator and the holding company but an amendment of

the claim[53]. Thus, one of the remaining alternatives was the class action by the Indonesian citizens in the Australian court against the Australian subsidiary[54]. The claim was successful and led to an out-of-court settlement[55].

Potential hurdles in enforcing the rights of the communities of the transboundary victim States

Although the interests of the States and their nationals seem to be inseparable, sometimes the actions to be undertaken by the former are inadequate or not timely. As seen above, in such a case, the latter may take the matters in their hands and enforce their rights unilaterally against the licensee, the host or home States in their domestic courts or the courts of third States. The communities or their governments acting on their behalf may also refer to the international human rights courts against the State

[50] 'BP quietly Paid just US$25.5M to Mexico after the Worst Oil Spill of the Century' (02.10.2018) Kaieteur News available https://www.kaieteurnewsonline.com/2018/10/02/bp-quietly-paid-just-us25-5m-to-mexico-after-the-worst-oil-spill-of-the-century/ (20.06.2023); Janowitz N 'BP Paid Mexico $25.5M After the Deepwater Horizon Oil Spill, But Victims Didn't See a Peso' (17.12.2020) Vice World News available https://www.vice.com/en/article/m7a383/mexicos-government-got-millions-after-deepwater-horizon-so-where-did-all-the-money-go (20.06.2023)

[51] Hayes J 'A New Policy Direction in Australian Offshore Safety Regulation' in Baram M and Renn O (eds) Risk Governance of Offshore Oil and Gas Operations (2014) Cambridge University Press 188 at 189

[52] Henry T 'A Thai Oil Firm, Indonesian Seaweed Farmers and Australian Regulators. What Happened after the Montara Oil Spill?' (14.02.2017) Mongabay available https://news.mongabay.com/2017/02/a-thai-oil-firm-indonesian-seaweed-farmers-and-australian-regulators-what-happened-after-the-montara-oil-spill/ (20.06.2023); see also 'Indonesia Sues Thailand's PTT, PTTEP for $2 billion over Oil Spill'(06.05.2017) Reuters available https://www.reuters.com/article/uk-indonesia-thailand-oil-idUKKBN182068 (20.06.2023); 'Indonesia Files $2B Lawsuit against PTTEP over 2009 Oil Spill' (08.05.2017) Offshore Energy available https://www.offshore-energy.biz/indonesia-files-2b-lawsuit-against-pttep-over-2009-oil-spill/ (20.06.2023); 'Indonesia Launches Bt70-bn Lawsuit against PTTEP over Oil Spill off Australia' (06.05.2017) The Nation Thailand available https://www.nationthailand.com/in-focus/30314455 (20.06.2023)

[53] Mahawongtikul P 'The Revocation of Indonesian Lawsuit Relating to the Montara Incident' (07.03.2018) available https://www.pttep.com/en/Investorrelations/Regulatorfilings/Setnotification/Therevocationofindonesianlawsuitrelatingtothemontaraincident.aspx (20.06.2023)

[54] Sanda v PTTEP Australasia (Ashmore Cartier) Pty Ltd (ACN 004 210 164) [NSD 1245/2016]; Business&Human Rights Resource Centre 'PTTEP Australasia Lawsuit (re Montara Oil Spill in Indonesia)' available https://www.business-humanrights.org/en/latest-news/pttep-australasia-lawsuit-re-montara-oil-spill-in-indonesia/ (20.06.2023); Maurice Blackburn Lawyers 'Montara Oil Spill Class Action' available https://www.mauriceblackburn.com.au/class-actions/join-a-class-action/montara-oil-spill-class-action/ (20.06.2023)

[55] 'PTTEP Agrees $127m Montara Oil Spill Settlement' (22.11.2022) Energy Voice available https://www.energyvoice.com/oilandgas/462388/pttep-agrees-127m-montara-oil-spill-settlement/ (20.06.2023); Ryan R and Parry E 'The Montara Class Action Decision and Implications for Corporate Accountability for Australian Companies' (2021) 6(3) Business and Human Rights Journal 599

of origin or the home State[56]. However, what one has to take into consideration is that the victim States' nationals, unlike the nationals of the licensing State, might be far away from the source of the accident, thus facing the difficulty to prove the causal link between the activity of the oil producer and the pollution[57]. The further hurdles are forum non conveniens, non-recognition of foreign court verdicts[58], unfamiliarity with the foreign court process, language issues, time consuming, more expensive in comparison to domestic litigation and prescription of claims.

Lessons learnt from the two oil spill cases

Following the 2010 Deepwater Horizon oil spill, the local governments of the Mexican states that had been affected by it filed claims against the companies linked to the exploitation of the oil rig before the US courts[59]. The latter rejected them on the basis that it was the federal government of Mexico that had proprietary interest in the oil-damaged property[60]. In the same year, a class action lawsuit was launched in the Mexican courts against the local BP subsidiaries[61] but the proceeding was not allowed until September 2019[62].

The claims could also have been filed against the US government officials for failure to comply with their professional obligations, having in mind the investigation report by the US authorities finding lack of due diligence on the US control organs[63]. However, it is hardly likely to believe that the claim would have been successful. As seen from the US case law on Deepwater Horizon, the judiciary relies on the ex post control and personal criminal liability of managers[64] but not criminal sanctions against the State officials[65].

According to this study, there are 14 options that could be used by the transboundary victims for potentially successful claiming violation of their rights. As a role model, Mexico and the Mexican claimants in the Deepwater Horizon are used in summarising them.

Instead of USA, the defendant could also be the home State of BP for failure to exercise sufficient control over the activity of the holding company.

The second is that the Mexican citizens bring individual or class action claims in the US courts against BP similar to what was done in the wake of the 1986 Bhopal incident where the Indian claimants argued violation of their rights by a US subsidiary in India in the US courts[66].

The third is to bring USA and/ or the BP home State to international human rights court after the exhaustion of the local remedies. However, while the home State, the UK, is part of ECtHR, USA is part of neither it nor the Inter-American Court of Human Rights which in 2017 delivered

[56] Commentary to Article 14 of International Law Commission (ILC) 'Draft Articles on Diplomatic Protection with Commentaries, 2006' Yearbook of the International Law Commission, 2006 (vol II, Part Two) 26 at 44 (para 1); Art 35(1) of ECHR; Barcelona Traction, Light and Power Company, Ltd, Preliminary Objections (1964) ICJ Reports 6 at 19; Kidanemariam M 'Assessing the Ethiopian House of Federation in the Light of the Exhaustion of the Local Remedies Rule under the African Charter' in Benedek W et al (eds) Implementation of International Human Rights Commitments and the Impact on Ongoing Legal Reforms in Ethiopia (2020) Brill 326 at 327; Banda M 'Regime Congruence: Rethinking the Scope of State Responsibility for Transboundary Environmental Harm' (2019) 103 MINN. L. REV. 1879 at 1953-4

[57] Henry T (n 52); Sutinen J et al 'A Framework for Monitoring and Assessing Socioeconomics and Governance of Large Marine Ecosystems' (2005) 13 Large Marine Ecosystems 27 at 54

[58] For instance, the court of the home State or the court of the third State might not recognise the decision of the court of the victim State; see the 2019 Convention on the Recognition and Enforcement of Foreign Judgments, in particular Articles 2(1)(g) excluding transboundary marine environmental claims and 19 giving leeway to the State parties to exclude the application of the Convention where one of the litigants is a State or State representative

[59] In re Deepwater Horizon, 784 F. 3d 1019 - Court of Appeals, 5th Circuit 2015 available https://scholar.google.com/scholar_case?case=11903941093620094261&q=784+F.3d+1019&hl=en&as_sdt=3,39 (20.06.2023); In Re Oil Spill by the Oil Rig "Deepwater Horizon" in the Gulf of Mexico, Dist Court, ED Louisiana 2018 available https://scholar.google.com/scholar_case?case=5646660986383371742&q=784+F.3d+1019&hl=en&as_sdt=3,39 (20.06.2023); In fact, the actions of the Mexican states could be matched to the role the affected States play in providing disaster relief as per Article 10 of ILC Draft Articles on the Protection of Persons in the Event of Disasters (2016)

[60] Hill-Cawthorne L 'Dispute Settlement in the Aftermath of Disasters' in Breau S and Samuel K (eds) Research Handbook on Disasters and International Law (2016) Edward Elgar 501 at 519

[61] Lakhani N 'BP Faces Mexican Class Action Lawsuit over Deepwater Horizon Oil Spill' (11.12.2015) The Guardian, available https://www.theguardian.com/environment/2015/dec/11/bp-gulf-oil-spill-mexico-lawsuit-deepwater-horizon (20.06.2023)

[62] Lakhani N 'Deepwater Horizon: 'We've Been Abandoned': a Decade Later, Deepwater Horizon still Haunts Mexico' (19.04.2020) The Guardian available https://www.theguardian.com/us-news/2020/apr/19/deepwater-horizon-mexico-10-years-on (20.06.2023)

[63] National Commission on BP Deepwater Horizon Oil Spill and Offshore Drilling 'Deep Water – the Gulf Oil Disaster and the Future of Offshore Drilling' (US) Report to the President (2011) Washington D.C. at 243 and 291 available https://www.govinfo.gov/content/pkg/GPO-OILCOMMISSION/pdf/GPO-OILCOMMISSION.pdf (20.06.2023); Boyle A 'Transboundary Air Pollution: a Tale of Two Paradigms' in Jayakumar S et al (eds) Transboundary Pollution: Evolving Issues of International Law and Policy (2015) Edward Elgar 233 at 239-40

[64] Micklitz H 'Risk, Tort and Liability' in Grundmann S et al Grundmann S et al New Private Law Theory: A Pluralist Approach (2021) Cambridge University Press 272 at 296

[65] US Environmental Protection Agency (EPA) 'Summary of Criminal Prosecutions' (fiscal year 2013) available https://cfpub.epa.gov/compliance/criminal_prosecution/index.cfm?action=3&prosecution_summary_id=2468 (20.06.2023); The search on the US EPA website for criminal prosecutions linked to the search words 'Macondo' or 'Deepwater Horizon' showed that no governmental official were held criminally accountable; see https://cfpub.epa.gov/compliance/criminal_prosecution/index.cfm (20.06.2023)

[66] Hanqin X Transboundary Damage in International Law (2006) Cambridge University Press 27-8

an advisory opinion in a similar case.

A subcategory that is indirectly linked to the enforcement of rights is the recourse to various international commissions or courts that may recommend on the proper behavior of the States[67].

The fourth option is that Mexico brings a civil claim against the BP subsidiaries in its domestic courts. However, one is to be aware that the defendants might argue that the court verdict in favour of the plaintiffs would amount to expropriation of their assets, thereby breaching their rights under the investment agreement between Mexico and the home State as what happened in the Moorburg case.

In the fifth, sixth and seventh options, the Mexican federal government could lodge a claim against the polluting State and/ or the home State in an international court not on behalf of its citizens but on its own behalf. In this course of events, it would not be necessary to exhaust initially the local remedies[68] unless an agreement to the contrary exists[69]. And as regards USA as defendant, there is a chance of success based on the investigation report by the US authorities concerning the complicity of the US control organs.

The eighth path is that the Mexican federal government files a claim against the company linked to the exploitation of the oil rig before a US court.

The remaining alternatives are to be brought by the victim communities or the victim State in a third State having assets of the defendant as follows: against the home State, host State or the investor.

Of course, one may argue that some of the 14 alternatives are of scholarly importance only and of little or no value since the States discharge their obligations by simply making the investor carry out an insurance policy. And even though after the 2009 and 2010 incidents, the insurance companies worked towards introducing one, specifically designed to cover the risks associated with seabed oil activity[70], there is always a chance that the coverage would not be sufficient to meet the pollution challenges. Moreover, since legislation is generally either silent on how to deal with this insufficiency or has not been explicit in holding that the outstanding loss would lie where it falls, the accountable State would still become responsible for the transboundary pollution consequences regardless that the claim is not against it but the licensee – State accountability that should be classified as vicarious accountability. The same conclusion would apply to claims in a third State.

Conclusion

Regardless of the multitude of options to enforce rights, they fall under two main categories – channeling accountability to the operator of the seabed activity or making the States directly accountable. Presently, in ascertaining the wrongdoer and its duties, preference is given to the first category, thus tentatively alleviating the States from their obligations. However, since this process caters only in part, the latter are therefore not exculpated from accountability.

There is only one treaty which, although of regional application, unconditionally imposes the obligation on the States to cater for the transboundary pollution consequences – the Nordic Convention[71]. However, its shortcoming is that it has not dealt with the obligations of the home State which may be not part of the convention.

Without imposing an unconditional obligation on the States benefiting from the seabed oil exploitation, that is, the home and host States, to cater for the transboundary victims, treaty law may not be a panacea should the treaty extend only to its parties. In order everybody to get what it deserves, States are to cooperate in introducing legislation providing for individual and shared accountability of the home and host States extending to all transboundary victim States regardless of whether they are party to it.

About the Author

Ognyan Savov is a full time lecturer in nautical studies and STCW courses at the Bulgarian Maritime Training Centre. He is also part time lecturer in Maritime law at the Bulgarian Naval Academy 'N. Vaptsarov'.

Having graduated from the Bulgarian Naval Academy in 2002, he worked aboard ships reaching the rank of Chief Officer. His interest to delve deep into the issues surrounding the marine industry brought him to South Africa where he obtained a Bachelor in Laws from the University of Cape Town in 2007 and Sweden where he got his Master's in Maritime Law from the University of Lund in 2011.

Although in his work he deals with all aspects of maritime law, his principal field of interest is protection of the marine environment and States' relations on global and regional levels.

[67] e.g. Inter-American Commission on Human Rights, United Nations Human Rights Committee

[68] Payne C 'Negotiation and Dispute Prevention in Global Cooperative Institutions: International Community Interests, IUU Fishing, and the Biodiversity beyond National Jurisdiction Negotiation' (2020) 22 International Community Law Review 428 at 435-6

[69] In M/V "Virginia G" (Panama/Guinea-Bissau), Judgment, ITLOS Reports 2014, p. 4 at 53-4 (para 153) and 54-5 (paras 157-8), the tribunal holds that it is 'established in international law that [in the absence of an agreement to the contrary] the exhaustion of local remedies rule does not apply where the claimant State is directly injured by the wrongful act of another State'

[70] Abraham K 'Catastrophic Oil Spills and the Problem of Insurance' (2011) 64 Vanderbilt Law Review 1769; King R 'Deepwater Horizon Oil Spill Disaster: Risk, Recovery, and Insurance Implications' (2010) Congressional Research Service (R41320); Cameron P 'Liability for Catastrophic Risk in the Oil and Gas Industry' (2012) 6 International Energy Law Review 207; Noussia K 'Environmental Pollution Liability and Insurance Law Ramifications in Light of the Deepwater Horizon Oil Spill' in Basedow J et al (eds) The Hamburg Lectures on Maritime Affairs (2009 & 2010) vol 23 Springer 137

[71] Convention on the Protection of the Environment (Stockholm, 19.02.1974) [1092 (p 279)] with Denmark, Finland, Norway and Sweden parties

7th NMIOTC Conference on Cyber Security in the Maritime Domain, 2023

by Dinos Kerigan-Kyrou

There follows a summary, with reflections and analysis, of the 7th NMIOTC Conference on Cyber Security in the maritime domain. The conference addressed multifaceted aspects of maritime cybersecurity[1].

Cybersecurity is the security of cyberspace - the online environment in which everyone now lives and works. Cybersecurity is central to our personal security, the security of our families, societies, organisations, businesses, governments, and our militaries. Today, cybersecurity underpins our security across NATO, the European Union, and NATO's many Partners across the world. Cybersecurity is central to the Maritime environment. As NMIOTC Cdre Themistoklis Papadimitriou states, the sheer scale of the maritime environment, combined with a multitude of actors, makes the maritime a particularly advantageous environment for potential cyber malicious actors who are becoming increasingly sophisticated in their techniques and tactics.
The summary will begin by highlighting the Keynote speeches addressing the challenges we face across NATO, Partner Nations, and the European Union. It will then highlight the presentations and panel discussions that took place over the two days of the conference before drawing some conclusions[1].

The conference covered six key areas of maritime cybersecurity:
+ The Impact of Emerging Cyber Risks in Maritime Security.
+ Maritime Cybersecurity Technologies and Industrial Products.
+ Maritime Enterprise Cyber Security Challenges.
+ Assessment, Certification and Training in Maritime Cyber Security.
+ The Security of Maritime Value and Supply Chains, Infrastructure, and Services.
+ Research and Innovation in Maritime Cyber Security and Cyber Defence.

[1] Many thanks to Dr Rois Ni Thuama for her invaluable advice in regard to the conclusions and analysis.

Keynote Addresses

NMIOTC Cdre Themistoklis Papadimitriou stated that NMIOTC is the only NATO quality assured educational facility dedicated to training and research in the maritime domain. NMIOTC's core aim is to enhance capabilities and awareness in maritime interdiction. The key enabler for maritime security is defined by the '3Ds': Delay. Disrupt. Destroy. And these '3Ds' are as crucial in cyberspace as they are in the physical realm. All asymmetric and hybrid threats - including threats in cyberspace - must be delayed, disrupted or destroyed before they become a threat to ourselves or our friendly forces. Highlighting the very specific and unique cybersecurity challenges in the maritime environment, Cdre Papadimitriou emphasised that the new cyber environment presents us with an imperfect and incomplete informational picture, making decision-making hugely challenging. It is data that is driving new communications networks, artificial intelligence led technologies and remotely connected robotics.

Complexity is the new normal, and surprise events are much more likely, including against critical national services and infrastructures. Indeed, for years the sea was a guarantee of wellbeing and prosperity. And yet in the wake of recent vast technological progress, there are a growing number of challenges and risks that threaten the very core of this global security and prosperity. Ongoing armed conflicts, such as the illegal Russian invasion of Ukraine, have shown us that cyberspace operations are being conducted to support strategic objectives.

Cdre Papadimitriou stated that we need an 'enterprise approach' to cybersecurity, consisting of information-sharing, cyberspace situational awareness, collaborative cyber incident response, and strategic policies and measures. This approach will require a coherent network of civilian, industrial, commercial, and military cyber defence operations and strategies. Cybersecurity challenges will be with us for the next decade and beyond. Because of this, it is critical we establish a comprehensive approach for maritime cybersecurity, concluded Cdre Papadimitriou.

Chief of Staff of the Hellenic Navy General Staff, RAdm Georgios Floros

RAdm Georgios Floros stated that our oceans have become a key theatre of Cyberware. This fact has major implications for our military and security operations.

NATO faces daily challenges in the maritime cyberspace environment, especially in information-sharing and situational awareness. Because of this, challenges need to be dealt with across NATO, especially as cybersecurity problems in the maritime environment have broad and profound implications for the whole Alliance.

Shipping companies, port authorities, and all of our civilian and military maritime infrastructure is at risk. Addressing cybersecurity in the maritime domain requires a completely united front. Maritime nations need mandatory regulations for ports, shipping companies, and all involved in the maritime environment - at sea and ashore. Ensuring our supply chains in the maritime environment are secure, and developing certification to ensure these cybersecurity standards, is vital.

Information-sharing is crucial to mitigate new and emerging threats. While new technology such as Artificial Intelligence (AI), Machine Learning and blockchain present security challenges, they also present substantial opportunities to protect us and our critical infrastructure.

RAdm Floros emphasised that warships are highly connected, digital platforms. This interconnectivity enables huge advantages, but also presents new and substantial vulnerabilities such as unauthorised data access and threats to our ships and Critical Infrastructure. The legacy computer systems so many of us continue to use were not designed with security in mind. While patching and upgrades to these systems are of course vital, they are not enough; insider threats can also produce substantial cybersecurity challenges. A disgruntled or compromised

employee - in the military or civilian environments - can easily introduce vulnerabilities into a network. And all of us can accidentally click a phishing or spear phishing link, rapidly introducing vulnerabilities into our systems. Moreover, warships rely on complex supply chains. Sophisticated adversaries can target naval assets - stealing information and data, and planting malware. It is therefore critical to update these supply chains to prevent vulnerabilities. The cybersecurity challenges facing modern ships are ever evolving. It is essential to develop and continually secure our ships. Failure to do this will make us extremely vulnerable.

We need to ensure Confidentiality, Integrity, and Availability of information. The development and enforcement of cybersecurity regulations is crucial. Proactive defence is key to staying ahead of adversaries. Preparing for worst case scenarios by developing response plans is imperative for our navies to be able to address new challenges.

RAdm Floros concluded by saying that we must follow a holistic approach to maritime cybersecurity - cybersecurity is everyone's responsibility. Cybersecurity is not an option, it is a necessity - we must secure our naval assets, secure supply chains, and secure our economies.

Mr Mario Beccia, Deputy Chief Information Officer, NATO OCIO (Office of the Chief Information Officer), NATO HQ stated that in July 2020 a decision was made to appoint a CIO (Chief Information Officer), at NATO. The goal was to create better ICT (Information, Communications, and Technology) coherence and structure.

The CIO's role is to oversee NATO's cybersecurity, consisting of 57 entities and 55,000 individual civilian and military users. NATO's cybersecurity should be viewed in the context of NATO's function of portfolio management[2]. The CIO became the single point of authority for cybersecurity in NATO. The CIO constantly assesses and scans the cybersecurity risk posture. The CIO is responsible for the Defensive Cyber Operations (DCO) planning and coordination cell, and Defence Cyberspace Operations. The CIO also has a crucial liaison and external role, communicating directly with Military Operations, Intelligence, the NCIA (NATO Communications and Information Agency), and with external partners. Mr Beccia stated there are four elements or goals in this approach:

1) Reducing risk of cyber attack. This requires intelligence, and working with industry and academia, helping NATO understand the overall cyber risk.

2) Mitigating Insider Threats. Liaising with the NATO Office of Security, helping to prevent attacks from within the organisation.

3) Managing the Risk of Obsolescence. The risk of obsolescence is a real and actual security risk to NATO and Allies. Many layers of IT have accumulated over the last 50 years in an uncoordinated way. The NATO IT environment is now complex and vast, but much of it is in danger of becoming outdated, and is therefore increasingly vulnerable.

4) Addressing the Risk of Lack of Cybersecurity Skills. Not having a workforce with the right abilities and skills means that NATO's adversaries will have an advantage. It is therefore crucial to ensure NATO is recruiting effectively, and for NATO staff and contractors to constantly update their education and training to face the new cyber threat environment.

Collaboration with all NATO Allies and Partners is key to addressing these cybersecurity risks and challenges going forward, concluded the NATO Deputy CIO.

Panel Discussion Summaries

Summary of Panel The Impact of Emerging Cyber Risks in Maritime Security[3]

Machine Learning and Artificial Intelligence (AI), will transform the maritime cybersecurity threat landscape. Machine Learning provides us with ways of handling enormous complexities of data. We can leverage these technologies for both defensive and offensive capabilities. 'Adversarial Machine Learning' is a challenge we need to prepare for; hostile states and other nefarious actors, be they terrorists or organised criminals, will adapt Machine Learning and AI for their own ends. However, if used at the right time and in the right place Machine Learning can give NATO Allies and Partners a strategic advantage.

Moreover, the Radio Access Networks (RANs), on which we rely for communications are increasingly vulnerable and can be breached by adversaries. It is crucial to develop new standards, best practices, monitoring, and implementation to ensure that our communications continue to be as secure as possible.

New standards in cybersecurity for the maritime environment - which are currently lacking - are very much needed. It was stated that a cybersecurity 'baseline' standard has recently been developed which can be applied to maritime organisations. A baseline standard is invaluable because research has shown that if people can start with an achievable level of cybersecurity they are very likely to go on and do more. But it is important that this baseline is met, even for vessels and crew that are new to the concept of cybersecurity. One of the main problems of cy-

[2] Portfolio Management: the selection, prioritisation and control of programmes and projects, in line with NATO's strategic objectives and capacity to deliver these objectives.

[3] Speakers on The Impact of Emerging Cyber Risks in Maritime Security: Dr Barton P. Miller and Dr Elisa Heymann, National Science Foundation Cybersecurity Center of Excellence, University of Wisconsin-Madison, USA; Peter Thomas and Dr Paul Rohmeyer, Palindrome Technologies, New Jersey, USA; Emma Philpott MBE and Craig Wooldridge, IASME Consortium, Malvern, UK. Moderator: Dinos Kerigan-Kyrou.

bersecurity certification is that the entire process appears overwhelming; this issue has to be addressed if we are to achieve effective cybersecurity certification and standards, according to IASME. Basic cybersecurity controls will - for certain - prevent a vast number of cybersecurity incidents.

Summary of Maritime Cybersecurity Technologies and Industrial Products[4]

The criticality of being able to identify potential threats in our rapidly changing technological environment was the main message of the panel. Challenges to our ability to do this (sometimes referred to as signature vulnerabilities), need to be addressed. AI will both help us develop solutions, but will also create problems for us. Nonetheless, AI is likely to be an integral part of maritime cyberspace in the very near future.

Challenges to the transition to AI include social, technical, and behavioural issues. User trust, training, and ethical considerations should be part of this evolution. When considering progression of AI, NATO and Partner Nations need to place human factors and user interface of AI as paramount in planning and strategy.

Indeed, Cyber Defence may well need to be re-thought of as a 'Reinforcement Learning Process' i.e. continuous learning and adaptation. Addressing these challenges is crucial for improving the efficiency, safety, and reliability of maritime operations and naval warfare. This entails balancing automation with human control, fostering trust, and ensuring robust cybersecurity measures.

Moreover, AI needs to be built-in to a realistic network environment for simulations and training. There is increased interest and research not only in detecting malicious cyber activities but in early recognition, and being able to stop them before they cause harm - thus making the network resilient. The main problem we face however in achieving this goal is the massive number of 'false positives' (incorrect identification of threats), producing millions of false alerts each day. In order to address this problem DARPA's CASTLE[5] project explores defensive actions to stop ongoing Advanced Persistent Threats (APTs). CASTLE utilises purple, red, and blue teams[6] to test, evaluate and adapt cybersecurity for the new AI environment. CASTLE aims to utilise AI technology in order to identify cybersecurity challenges early - while minimising the problem of false positives - thereby producing far more efficient cybersecurity.

Summary of Maritime Enterprise Cyber Security Challenges[7]

Our adversaries' seabed capabilities are increasing enormously. These include their offensive capabilities, as well as their ability to reduce and degrade our cyberspace intrusion detection systems. Because of this, NATO MAR-

[4] Speakers on Maritime Cybersecurity Technologies and Industrial Products: Dr Kitty Kioskli, Trustilio B.V, UK / Netherlands, and Henri de Foucauld, ATHANOR, France; Tejas Patel, DARPA, USA; Benjamin Azoulay and Joffrey Guerry, OLEDCOMM, France. Moderator: Prof Christos Douligeris, University of Piraeus, Greece.

[5] DARPA CASTLE Project: Cyber Agents for Security Testing and Learning Environment.

[6] Red Teams are offensive cybersecurity experts acting the part of adversaries. Blue Teams are expert incident responders who act as defenders of networks and systems. Purple Teams are both offensive and defensive cybersecurity experts working together; Purple Teams can be used in multiple scenarios such as exercises, simulations, and real-world operations.

[7] Speakers on Maritime Enterprise Cyber Security Challenges: Captain Yann Bozec (FRA-N), NATO Allied Maritime Command MARCOM, Allied Command Operations; Tsvetelina Shabanska (Bulgaria), and Joanna Sliwa (Poland), NATO Cyber Security Centre at the NATO Communications and Information Agency; Mark Milford (Singapore), and Stephen Mills (US), Wärtsilä, Finland; Jacob Syta, Maritime Cybersecurity Centre, Polish Naval Academy, Gdynia, Poland. Moderator: Dr Iosif Progoulakis, University of the Aegean, Chios, Greece.

COM will continue to adapt, improve, anticipate and develop best practices and processes to face the growing maritime cybersecurity threats and challenges.
Like AI, Quantum Computing will revolutionise cybersecurity - not only for ourselves, but also for our adversaries. Because of this, the NATO Science & Technology Organisation aims to work with external partners (in industry, academia and research), in addition to governments and the military, in order to develop our approach to these new and emerging technological challenges.
The panel emphasised that when building ships and equipment it is imperative that the customer and the supplier consider cybersecurity early in the process, working together to incorporate the highest cyber standards.
The horrific Russian invasion of Ukraine has created new 'lessons learnt' about cybersecurity and protecting our cyberspace. Ukraine has rapidly learnt how to protect its Critical Infrastructure (CI), - learning in particular from other countries, such as Poland, whose CI has been constantly targeted by Russia over a long period of time. Some of these Russian attacks against Polish CI have been sophisticated; others less so. But these Russian cyberattacks are continuous and ongoing. They are targeted at ports, shipyards, naval equipment, marine brokerages, and maritime manufacturers. CI such as power, telecoms, financial services, and transport have all been targeted.
Cyberspace is increasingly an enabler of adversaries. Nefarious actors including hostile states and terrorists are able to utilise drones in the air, on the sea and under the sea, and we must be aware of these threats. Cyberspace is utilised for human trafficking, disinformation, smuggling of drugs, and hiding shipping containers, often containing items which can cause us great harm. It was emphasised that war crimes committed by Russia in cyberspace, or where cyberspace is an enabler, must not escape war crimes investigations.
The panel concluded that the key factor in the protection of our CI across NATO is 'fixing the cybersecurity basics'. Without this, we are unable to conduct the more complex cybersecurity tasks.

Summary of Assessment, Certification, and Training in Maritime Cybersecurity[8]

The panel opened by stating that if we are to retain the security of our domain of operations at NATO, we must continually be ahead of our adversaries. Cybersecurity is essential for us to fulfil the mission.
But some systems we use, such as the Automatic Identification System (AIS), are now 'broken', it was claimed. We need to identify such systems which are no longer satisfactorily working, address these issues and fix them. We also need to update and develop NATO STANAGs (NATO Standardization Agreements).
The panel emphasised that maritime cybersecurity is critically important due to its role in global transportation, the global economy, and for the military. Ransomware and spyware has hit maritime activities globally. Increasing digitalization and automation introduce complex cyber threats. Our ships and contractors are being compromised. Cyber Ranges can develop integrated IT (Information Technology), and OT (Operational Technology), attack-defence scenarios to enhance maritime cybersecurity training. We need to have 'Security by Design'; training, simulation and 'virtual cyber ranges' are essential to achieve this.
The EU's CYRENE Consortium of 14 industrial and academic partners from 10 EU countries, who are establishing an EU cybersecurity standard certification framework[9], emphasised how important it is to develop 'whole process' certification in supply chains. The new EU NIS2 (Network and Information Systems) Directive, introduced new standards in supply chain security and cybersecurity vulnerability management. In addition to NIS2 there are likely to be more EU cybersecurity standards and certification requirements in the near future.

Summary of Secure Maritime Value and Supply Chains, Infrastructure and Services[10]

Cybercriminals can target maritime assets to steal sensitive data, disrupt operations, or cause physical damage.
Software vulnerabilities leave our civilian and military naval fleets with severe gaps in their cybersecurity. Unfortunately, our adversaries can quickly capitalise on this, utilising these vulnerabilities to develop and improve their attack vectors. The panel addressed the substantial skills gap in cybersecurity. This problem includes a lack of cybersecurity awareness, as well as a shortage of technical skills and expertise to respond to cyberattacks.
The need for 'zero trust' in software supply chains was emphasised. But the shipping companies have had a substantial challenge in forcing suppliers to become secure

[8] Speakers on Assessment, Certification and Training in Maritime Cyber Security: Dr Soultana Ellinidou, Thales, Belgium; Henri de Foucauld, ATHANOR, France; Dr Eleni Maria Kalogeraki, Maggioli Group / EU CYRENE Project, Greece. Moderator: CAPT (Ret), Emmanouil Christofis GRC (N), NATO SHAPE J6, Cyberspace - Strategic Plans and Policy, Mons, Belgium.
[9] CYRENE is part of the EU Commission's CORDIS programme, 'Certifying the Security and Resilience of Supply Chain Services'.
[10] Speakers on Secure Maritime Value and Supply Chains, Infrastructure & Services: Eric Hill, Eastern Mediterranean Business Cultural Alliance, USA; Dr Anna Vazintari, Unisea Shipping, Greece; Margaux Blandel-Coquet, SOPRA STERIA, France; Prof Christos Douligeris, Theodoros Karvounidis, and Despina Polemi, University of Piraeus, Greece, and Prof Paresh Rathod, Laurea University, Finland (representing CyberSecPro, EU). Moderator: Konstantinos Sakellakos, AMMITEC - Navarone SA, Greece.
[11] Speakers on Innovative Research in Maritime Cyber Security and Cyber Defence: Dr Britta Hale, Postgraduate School (NPS), Monterey, California, USA; Stelios Kavalaris, Netcompany-Intrasoft, Piraeus, Greece; CDR (Res.) Fulvio Arreghini (Italy) and CAPT (Res.) Paolo Pezzola (Italy), INFODAS, Cologne, Germany. Moderator: Dr Eleni Maria Kalogeraki, Maggioli Group, / CYRENE (EU) Project, Greece.

because of the lack of certification and standards. The Association of Maritime Managers in Information Technology and Communications (AMMITEC) stated that threats have been multiplying against shipping. These include ransomware and malware caused by phishing and spear-phishing attacks targeting the port authorities, port operators, and manufacturers.

CyberSecPro, an EU supported coalition of universities and companies, stated that its goal is to enhance the role of Higher Education Institutes in cybersecurity education and training. The European Commission's Joint Research Centre and CyberSecPro stated that cybersecurity is a multidisciplinary science that involves all sectors of academia, business, government, and the military. Hands-on and working-life skills in digital transformation in critical sectors of the economy, including the maritime sector, are being developed by establishing an EU Cybersecurity Skills Framework. CyberSecPro concluded by emphasising that cybersecurity is a cross-sector discipline, stating "Let's cooperate, not compete, to consolidate cybersecurity for good."

Summary of Innovative Research in Maritime Cyber Security and Cyber Defence[11]

There has been a 400% increase in attempted cybersecurity breaches of the maritime sector since 2020. The maritime environment presents a high surface area for attack, and a large window of opportunity in time and space for attackers. The costs to the maritime community can be staggeringly high, consisting of economic, environmental, and financial costs, in addition to the risk of deaths and serious injuries.

Technology is rapidly developing. Encryption is the foundation of cybersecurity, but it is changing and altering the way in which we address cybersecurity. Cryptography is not static, but an ever-changing process, and new developments and progress can provide gains in security and of the functionality of what we do online. New forms of cryptography may enable early detection of attack and cybersecurity breaches. Examples of this new technology include 'Quantum 2FA (Two-Factor Authentication), and much stronger identity management, including Quantum Key Distribution. We need to enhance and utilise the opportunities that quantum computing presents us. Quantum potentially provides new ways in which today's encryption can be breached. We therefore need to be utilising the potential advantages that it presents us with, before our adversaries do. We need to use it for new forms of encryption. Likewise, we should take advantage of the new technology for the protection of our maritime assets and Critical Infrastructure at sea. For example, quantum may vastly improve the sensors we use for detecting adversarial activity, as well as pollution and environmental issues.

In summary, the panel concluded that these new technologies can be utilised by us across NATO, the EU and Partner Nations to enhance and develop our own security. If we do not employ them for our own advantage, those who wish to cause us harm will use these technologies against us. In order to stay ahead we must research and apply these new technologies.

Conclusions

The 7th NMIOTC Conference on Cyber Security in the Maritime Domain revealed many of the new challenges we are facing. Fortunately, the outstanding and enlightened presentations, as well as the formal and informal discussions over the two days, provided a wealth of answers to address the complex issues we face now and well into the future. Foremost among these solutions is ensuring that everyone has a role in cybersecurity - everyone must be part of the defense of NATO, the EU, our Allies and Partner Nations.

Cybersecurity Education and Training: The presentations on cybersecurity education, training and simulations demonstrate a major problem in cybersecurity training. Largely consisting of 'Did you click the link?' phishing tests, present-day cybersecurity training is counterproductive and out of touch with the threats we actually face in cyberspace. It was made clear that training must not create a 'blame' environment where we constantly fear being 'caught out'. Rather, cybersecurity training must become an immersive process where everyone feels involved as part of the cyber defence. Unfortunately, cybersecurity education and training has clearly developed in the wrong way over the past 10 years, and the presentations made clear just how much this needs to change. And developing our cybersecurity education will result in minimising accidental cybersecurity errors, and it will also help us identify malicious insider threats when they occur. (Unfortunately all large organisations will have some intentional insider threat actors, and we must train our personnel to identify these threats early before they cause real harm to our organisations). We need to totally and completely transform our approach to cybersecurity education - at sea and ashore.

[12] The phrase 'Quantum' is very broad. It includes quantum cryptography, quantum mechanics, and quantum computing. Moreover, there is wide debate as to whether any type of practical quantum computer has yet been developed, at the time of writing. However, there are developments occurring in several forms of quantum technology, particularly Quantum Key Distribution.

[13] It would require an operating temperature of minus 273 celsius, among many other specific conditions. However, it is possible that we may be able to access such a machine from a ship, in the cloud online, via an onboard remote terminal.

Certification: Ships and naval assets (including maritime CI, sensors, platforms and drones), are becoming technological platforms. IoT - the Internet of Things - today increasingly comprises every part of a ship's systems, controls, and operating technology; indeed every part of a ship that sends or receives data. For this IoT and Operating Technology to be secure we need to develop (and constantly update), robust - but manageable and workable - certification and standards for the maritime industry and our supply chain networks. Those working in the civilian and military maritime sector need to be able to work effectively with this certification. Standards must not become 'tick box' exercises but must be integrated into the maritime environment. Standards and certifications must exist to enhance and improve the maritime cybersecurity environment for everyone.

Technology: It will not wait for us. We need to develop and work with Quantum Computing, Artificial Intelligence, Machine Learning and Blockchain. It is of course not clear what direction these progressions will take; we have no timeframe for the introduction of a workable quantum computer or indeed for the widespread use of blockchain (beyond today's 'cryptocurrencies'). Indeed it is highly unlikely we will ever have a quantum computer onboard a vessel. But this uncertainty does not mean that these new technologies - or others we have yet to become aware of - will not have a profound impact on the future of our maritime cybersecurity. Indeed, Artificial Intelligence and Machine Learning are already starting to change the way we interact with cyberspace. Moreover, quantum cryptography and Quantum Key Encryption are starting to be utilised. While no one knows the specific direction this will take us, we can unfortunately be certain that hostile states, terrorist organisations and criminal networks will make use of all technological advancements, as they have done so in the past. We must make sure that our research and utilisation of new technology is always ahead of theirs.

The main message throughout the conference was that of Resilience in Maritime Cybersecurity. RAdm Floros correctly described this as 'Proactive Defence'. We can never stop all cybersecurity breaches. We can however achieve the resilience goal of minimising these breaches to as close to zero as we possibly can. But some will occur in our organisations. So in tandem with this we must make certain that when breaches do occur - which they for sure will - we address problems when they are minor before they become major issues. Information-sharing and a holistic approach to cybersecurity - the 'enterprise approach' described by Cdre Papadimitriou - is critical for this to happen. And by doing this we will ensure that our maritime cybersecurity is as robust as it can possibly be.

Dinos Kerigan-Kyrou PhD CMILT

Dinos leads and coordinates the cybersecurity and hybrid threats education for the Irish Defence Forces Joint Command & Staff Course. Dinos is a NATO Defence Education Enhancement Programme (NATO DEEP), instructor (for cybersecurity and hybrid security challenges), and a military educational advisor at the Partnership for Peace Consortium of Defense Academies (PfPC), based at the George C. Marshall Center, Garmisch-Partenkirchen. He is a co-author of the NATO/PfPC Cybersecurity Reference Curriculum and the new Hybrid Threats & Hybrid Warfare Reference Curriculum. He coordinated and instructed the initial military education on critical infrastructure security and resilience at the NATO School Oberammergau from 2011 to 2015. Dinos was an inaugural member of the PfPC Emerging Security Challenges Working Group (ESC WG), when it was established in 2013 to liaise with NATO's Emerging Security Challenges Division, and is today a Subject Matter Expert member of the ESC WG. He is a member of the PfPC Advanced Distributed Learning (ADL) Working Group, developing blended and hybrid learning for NATO and Partner Nations. Dinos is an editor of the PfPC journal *Connections*, published by USEUCOM. He is an Associate Member of the Royal Institution of Naval Architects, and a board member of Digital Business Ireland.

Assessing the Security and Resilience of ICT Supply Chain Services

by Eleni - Maria Kalogeraki[1], Danijela Boberić Krstićev[2], Sophia Karagiorgou[3], Pablo Gimenez[4], Giulio Vivo[5]

Keywords: Supply Chain Service, Risk and Conformity Assessment, Target of Evaluation, Maritime Transport, Automotive industry.

1. Introduction

A supply chain service is a collaborative service supported by a group of organizations, people, technology, activities, and information exchange, entailing an interdependent set of resources and processes (nodes) triggered by the sourcing of raw material and extended to fulfil the delivery of final products or services to the end-customer by transport means.

Within the last years of technological advent which upholds a gradual shift to remote work encouraged by the COVID-19 pandemic, the digitalization of services towards maritime transport and automotive industries is rapidly accelerated [1],[2]. To this end, the level of digital dependencies is amplified among heterogeneous interconnected infrastructures that support the provision of complex ICT Supply Chain Services (SCS), such as those related to Maritime Transport. In this vein, the disruption of such composite SCS could cause a devas-tating impact on the collaborative stakeholders that operate the assets of their cyberdependent ICT infra-structures and harm the entire supply chain environ-ment, including the markets economies that are associ-ated.

Nevertheless, the Information Technology (IT) escalation has raised attacker's capacity, knowledge and their motivation to attack on Critical Information Infrastructures (CIIs) since next generation malware toolkits are available by several web sources (e.g., via the Deep and Dark Web). Considering that SCS of critical Indus-

[1] Maggioli SPA - Greek Branch SA, Andrea Papandreou 19, 15124 Marousi, elma.kalogeraki@maggioli.gr
[2] Faculty of Sciences, University of Novi Sad, Trg Dositeja Obradovica 4, Novi Sad, dboberic@uns.ac.rs
[3] UBITECH Limited, 26 Nikou & Despinas Pattichi, Limassol 3071, skaragiorgou@ubitech.eu
[4] Fundación Valenciaport, Avinguda Moll del Turia, Valencia 46024, pgimenez@fundacion.valenciaport.com ,
[5] Fiat, Centro Ricerche Fiat, Strada Torino 50, 10043 Orbassano (To), giulio.vivo@crf.it

Acknowledgement

The work of this paper has been carried out within EU Project CYRENE, which has received funding from the European Union's Horizon 2020 research and innova-tion programme under grant agreement No 952690. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information con-tained therein.

try sectors, such as Maritime Transport and Automotive industries Services, become more connected and digitalized, the cybersecurity threat landscape of such services gradually blossoms, and new attack vectors are promoted. Subsequently, the potential of disrupting SCS or exposing sensitive data by compromising parts of CIIs (e.g., information systems, telematics, IoTs) or the entire CIIs (e.g., port infrastructures, manufacturing plants, etc.) through the implementation of sophisticated attacks (e.g., DDoS, ransomware, or adversarial at-tacks) increases exponentially [3],[4]. For instance, in July 2023, Container operations at the Port of Nagoya, the largest port in Japan, were suspended for several hours to recover from a ransomware attack on its sys-tems [5]. During January 2022, Swiss "Emil Frey", the giant EU car dealer, was hit by Hive ransomware attack, which relied on a ransomware-as-a-service model that led to restore and restart its commercial activity days after [6].

Despite the great majority of state-of-the-art security evaluation approaches and technologies, the literature reviews the difficulty and uncertainty in selecting an effective method and an appropriate tool to perform risk analysis on composite ICT processes/products/services supporting modern interconnected Supply Chains [7],[8]. There is still no easy, structured, standardized, and trusted way to forecast, prevent and manage inter-related and propagated cybersecurity vulnerabilities and threats, considering holistically the heterogeneity and complexity of today's global ICT Supply Chains. To this aim, devising methodologies, techniques and tools for comprehensive security evaluation and efficient risk management that addresses the ICT-based SCS speci-ficities is a burning issue. The CYRENE EU H2020 project [9] aims to fill this gap by developing a com-bined risk and conformity assessment methodology that evaluates the security and resilience of SCS and con-currently promotes a conformity assessment process which investigates whether the SCS is subject to cyber-security certification. The application of this methodolo-gy to realistic SCS environments, envisages raising the SCS trustworthiness and, thus, the competence to the EU digital market. To this objective, the CYRENE pro-ject has developed a software solution that implements this methodology. To validate the CYRENE solution towards SCS stakeholders' requirements, end-users from the maritime transport and automotive manufactur-ing industries tested the platform under real conditions via two focused pilot scenarios of a complex SCS. The current article presents the CYRENE solution, the two Pilots and the way forward from their outcome.

2. CYRENE H2020 Project general idea

CYRENE is EU H2020 project [9] aiming to enhance the security, privacy, resilience, accountability and trustworthiness of Supply Chains through the provision of a novel and dynamic Risk and Conformity Assess-ment Process that considers Supply Chain Services (SCS) as Targets of Evaluation[1] (SCS-TOEs) [10] and assesses their security and resilience. The evaluation mechanism takes into account the interconnections of ICT processes, ICT infrastructures and individual ICT devices and components interoperating to provide the SCS. The proposed Risk and Conformity Assessment (RCA) process follows a methodology [10] of subse-quent steps which supports an extended security model that combines both information security and conformity assessment aspects driven by EU regulation, such as the commonly known NIS 2 Directive (i.e., EU regula-tion 2022/2555) [11] and Cybersecurity Act (i.e., EU regulation 2019/881) [12]. Moreover, it relies on promi-nent international standards, such as ISO/IEC 27k [13] series, ISO 28000:2022 [14] on information security and supply chain security and resilience, respectively, and ISO/IEC 15408 [15] (representing the Common Criteria [16]), ISO/IEC 18045 [17] on IT evaluation. The RCA process supports different types of assessments with a set of incremental (evaluation) assurance levels [18], according to a proposed cybersecurity certification scheme for SCS developed by the CYRENE project [19] based on the ENISA EU Candidate Cybersecurity Certi-fication Scheme (EUCC) [20]. The combined risk and conformity assessment processes offer a dual use, utilized by two groups of actors:

- Supply Chain operators, Security Officers, and ICT experts of various industries, such as Maritime Transport, to assess and manage the SCS-risks, undertake security controls, and guide them to develop the Protection Profile[2] of the SCS (SCS-PP). In addition, it may help them to support forecasting, treatment and response to Advanced Persistent Threats (APTs) and assist in encountering privacy risks, han-dling incidents and avoiding data breaches.
- Assessors (self-assessors, e.g., manufacturers, logistics, distributors, service providers, or third-party assessors, i.e., Conformity Assess-ment Bodies (CABs), depending on the adopt-ed assurance level [10]) to conduct a conformi-ty assessment in order to evaluate the con-formance of the claims of a given SCS-PP and investigate whether the SCS is subject to cy-bersecurity certification and meets the re-quirements of the SCS cybersecurity certifica-tion scheme [19].

The RCA process evaluates the security and resilience

[1] SCS Target of Evaluation (SCS-TOE): A set of software, firm-ware, hardware and/or process possibly accompanied by guid-ance.

[2] Protection Profile is defined in ISO/IEC 15408 [7] and Common Criteria [8] as the implementation-independent statement of security needs for a Target of Evaluation i.e., the Supply Chain Service (SCS) in the CYRENE RCA process [2].

of SCS horizontally across various sectors assessing global SCS, such as the Vehicle Transport Service (VTS), which engages a set of industries (i.e., maritime transport, automotive manufacturing industries, etc.). In addition, it evaluates the security and resilience of the SCS (e.g., VTS) vertically to assess sector-specific ICT processes and assets (e.g., related to Assembly Plant or Port logistics in the context of the Automotive and Maritime Industries cooperating for the provision of the VTS). The RCA process is applicable to different SCS evaluation views [10]:

- the overall business view that scrutinizes only busi-ness aspects, such as business processes, business partners, business logic (e.g., data and information flows)
- the holistic-technical view, which assesses all ICT processes and ICT assess across the entire SCS
- the sector-specific view, which evaluates ICT pro-cesses and ICT assets of a snapshot of the SCS tech-nical view focusing on the sectorial aspects adopted by an individual business partner who participates in the SCS.

As mentioned, CYRENE promotes a Cybersecurity Certification Scheme for SCS [19], which indicates a certification process providing different certificates, according to the diverse SCS security evaluation views.

To this end, the CYRENE project has developed a software solution of collaborating components which implement the RCA process. The overall CYRENE solution is presented in the following.

3. CYRENE solution overview

The CYRENE solution follows a layered and modular approach aiming to ensure security-by-design, interoperability and continuous evolvement among all the components that implement the RCA process. The conceptual architecture of CYRENE solution is presented in Figure 1. This approach pipelines information from user authentication, secure services certification and data management to the support of seven (7) verti-cal, high-level cybersecurity services that support the risk and conformity assessment performance, i.e.:

- the Dynamic Vulnerability Management ser-vice
- the Dark Web Intelligence service
- the Threat Monitoring and Detection service
- the Forecasting and Attack Behaviour Simulation service
- the Data Protection Management and Security Declaration Establishment
- the Collaborative Risk Assessment service
- the Security and Privacy Assessment service
- the Visualization service.

The Dynamic Vulnerability Management service is supported by a set of components that provide sub-services related to vulnerability analysis to detect, assess, and quantify vulnerabilities on ICT assets and systems that compose a SCS-TOE. It provides vulnerability scanning services towards interconnected ICT systems. The vulnerability analysis is based on non-intrusive network data and meta-data analysis.

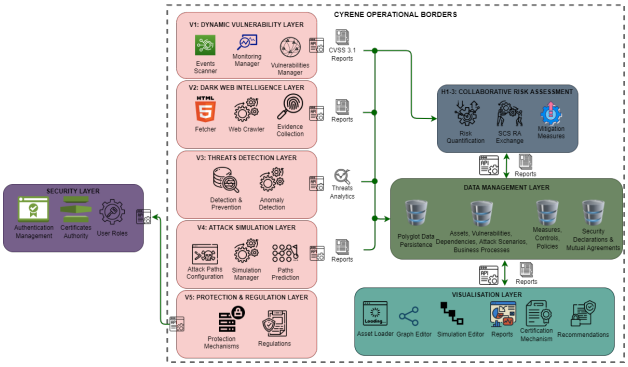


Fig. 1 Conceptual architecture of the CYRENE solution.

The Dark Web Intelligence service is responsible for the collection, mining and analysis of security, risks, threats, and personal data related information, embed-ded in User Generated Content (UGC). The CYRENE solution takes advantage of one of the most valuable applications of dark web research, i.e., identifying com-promised assets or user information by harvesting vari-ous electronic streams.

The Threat Monitoring and Detection service em-beds a bundle of services related to behavioural analy-sis and Intrusion Detection to recognize: (i) anomalies in Industrial Internet of Things (IIoT) sensory data and network traffic flows based on machine/deep learning algorithms and (ii) security threats in real-time. It reacts with dynamic decisions considering the network status and users' needs.

The Forecasting and Attack Behaviour Simulation service provides prediction capabilities supported by a bulk of services to identify potential vulnerabilities and attack patterns/paths on cyber assets of a SCS. In addi-tion, it offers a Behaviour Simulation Environment which allows users to execute simulation experiments to esti-mate the cascading effects of potential cyber-attacks over the SCS assets' network. It relies on CVSS 3.1 [21] vulnerability severity specification of FIRST and the Attack Potential metric of the Common Criteria [16] to estimate the impact to the SCS network upon sequen-tial vulnerabilities exploitation launched by an adver-sary to a series of interconnected SCS assets. The possible attack paths are visualized to the user via the generation of attack graphs.

The Data Protection Management and Security Declaration Establishment leverages data from the Data Management and serves as the evidence of the Conformity Assessment process status, validating Service Level Agreements (SLAs), Security Declara-tions and statements of application as defined in ISO/IEC 27001 [22] and ISO 28001 [23] among all SCS business partners participating in the RCA perfor-mance.

The Collaborative Risk Assessment service encom-

passes the entire lifecycle of SCS considering process modeling, asset cyberdependencies and estimating processes and assets criticality based on their impact to the SCS performance in case of their compromiza-tion. In addition, it provides a set of services related to threat assessment and vulnerability analysis, quantifi-cation of risk and estimation of its propagation across the SCS asset network. It guides Supply Chain opera-tors to enhance the security, privacy, resilience, ac-countability, and trustworthiness of their SCS.

The Security and Privacy Assessment service em-beds all the implemented mechanisms required to en-sure individual's privacy preservation and advanced user-defined access to the system per se via strong credentials, group- and role- specific accessibility rights. The Security and Privacy Assessment service communicates with all other high-level services of the CYRENE solution.

The Visualization service incorporates a group of sub-services delivering a collection of distinct dashboards with pre-selected widgets for visualizing functionalities and outcomes of other services of the CYRENE solution. Furthermore, the service: (i) showcases intrusion detections related to network connections, offering functionalities such as sorting, filtering, and drilling into the available information, (ii) depicts detected anomalies with relevant charts, (iii) presents analytics of passive and active vulnerability detection, including filtering mechanisms for more targeted results, (iv) provides a comprehensive view of security events.

4.CYRENE Pilot Demonstrations

The CYRENE project organized and coordinated the execution of two Pilots, i.e., the Port Pilot, conducted by a Port Authority and the Factory Pilot, performed by an Automotive manufacturer, to demonstrate and validate the application of CYRENE solution in real conditions. The two Pilots allowed stakeholders from different industries (i.e., maritime transport and automotive manufacturing industries) to use the CYRENE platform to assess the security and resilience of a prominent sup-ply chain service (SCS), i.e., the Vehicle Transport Service.

The Vehicle Transport Service (VTS) is a composite SCS. It engages numerous stakeholders to conduct the vehicles' transport, starting from the assembly and manufacturing of vehicles upon an importer's order request ending up with their shipment and delivery to the end-customer, executed mainly by port-to-port transportation means. The VTS is supported by an aggregation of industries, such as the Automotive Man-ufacturing and Maritime Transport industries, which are operators of essential/important services for the EU economy, respectively, according to the NIS 2 Directive [11].

The VTS was in both Pilots the Supply Chain Service Target of Evaluation (SCS-TOE). The pilot demonstrations aimed at showcasing the assessment of a specific SCS (i.e., the VTS) using the CYRENE platform under the scope of two focused threat scenarios addressing different evaluation views of the SCS (i.e., the holistic-technical and the sector-specific views), according to the RCA Methodology. To this aim, the project received feedback from different stakeholders after testing the SCS in alternative evaluation views, which provided a complementary evaluation of its security and resilience. The two CYRENE Pilots are presented in the next sections.

4.1The Port Pilot

The Port Pilot was the 1st CYRENE Pilot, carried out in Valencia Port Foundation (VPF) premises. It aimed at demonstrating the holistic-technical evaluation view of the VTS. Specifically, the port pilot scenario engages supply chain service processes and assets hosted by different business partners (i.e., Port Authority, Cus-toms, Agents) participating in the provision of the VTS. In this evaluation view, the developed asset models revealed asset interdependencies within the asset network of an end-to-end supply chain service (i.e., VTS). This Pilot targeted at testing the performance and efficiency of the CYRENE services (i.e., IDS services, Anomaly Detection analysis and Dynamic Vulnerability analysis) via a focused attack scenario and performed threat/vulnerability/risk assessment processes upon the VTS assets. The Port Pilot applied the generic steps of the CYRENE RCA methodology on and illustrated how a SCS stakeholder can be alerted via CYRENE and undertake proactive actions to meet conformity aspects and leverage the possibility of reaching cybersecurity certification.

The Port Pilot scenario: At first, the Port Pilot scenario launched a cyber-attack on critical VPF assets supporting the Port Community System (PCS) interoperating in the VTS port call requests SCS process to test how the CYRENE system can detect and analyze anomalies on the asset network and dynamically identify vulnerabili-ties that can help the user to identify malevolent actions of an attacker towards a cyber intrusion potential. After-wards, the end-users utilized the risk and conformity assessment capabilities of the CYRENE platform to evaluate the security of the VTS relevant processes related to "Port Call request" and assets involved upon a specified assurance level (substantial) defined in the Security Declaration and Application statement agreed upon the VTS business partners. Following the RCA conformity aspects: the Attack Potential metric was "Enhanced Basic" and the vulnerability analysis level of the AVA_VAN assurance class of ISO/15408 [15],[16] was AVA_VAN_3.

Table 1 depicts the Port Pilot scenar-io, including the cyberattacker's malevolent actions to disrupt maritime transport services and presents the pilot end-user's

Cyber Attacker	Pilot end-user/CYRENE services
1.The credentials of a PCS technician are published on the Dark Web, and they are eventually exposed to cyberattackers.	2. CYRENE platform detects the credentials publication through the Deep and Dark Web Crawler & Data Mining Service.
3.The attacker uses the credentials to access the PCS server.	4. The Intrusion Detection System (IDS) detects the access. 5.Then, the security staff analyses the vulnerabilities in their systems using the CYRENE's Dynamic Vulnerability Assessment and Testing services
6. The attacker tries to disrupt the port call services.	7. The service downtime is detected by the CYRENE's Data Protection and Management services.
-	8.The security staff uses the CYRENE platform to conduct a risk assessment on the supply chain service assets operating in the Port Call Request SCS process of the Vehicle Transport Service (VTS)

Table 1. The Port Pilot scenario.

subsequent actions in relation to the information provided by the CYRENE platform:

The Factory Pilot

The Factory Pilot was the 2nd CYRENE pilot realised in the Centro Ricerche FIAT (CRF) premises. It adopted the sector-specific evaluation view of the CYRENE RCA methodology, to asses the security, resilience and conformity of sectorial processes and assets of a single business partner that participates in the VTS, i.e., the Automotive Manufacturer (CRF). In this context, the business partner utilised the CYRENE platform to conduct risk assessment by performing a set of actions which instantiated all subsequent steps of the CYRENE RCA Methodology:

- Boundary and Scope Setting
- Supply Chain Service Analysis
- Threat, Vulnerability, and Impact Analysis
- Risk Assessment and Establishment of Risk
- Risk Mitigation
- Development of Overall Report

To validate the CYRENE platform's vulnerability analysis capabilities (i.e., IDS, anomaly detection, and dynamic vulnerability assessment), a focused threat IoT scenario was developed.

The Factory Pilot scenario: The Automotive Manufacturer (CRF) uses the CYRENE platform to conduct a sector-specific risk assessment on the assets operating for sectorial processes related to "Inbound Logistics" of the Assembly Plant considering all cyberdependencies with the interoperating assets of sectorial partners. To this aim, all sectorial partners interacting in the "Inbound Logistics" processes agreed to participate in the assessment under the following conformity aspects (defined via the Security Declaration and Application statement), according to the RCA Methodology: the Attack Potential metric identified as "Basic" and the vulnerability analysis level of the AVA_VAN assurance class of ISO/15408 [15],[16] was AVA_VAN_2. The following table illustrates the IoT threat scenario showcased the vulnerability analysis capabilities of the CYRENE platform.

In this threat scenario, a disgruntled employee was fired because of infringements to the company's policies of conduct and thus collaborated with cyberattackers to cause a dual harm to the company by: i) physically damaging some Electric Vehicle (EV) batteries (short-circuiting them) and ii) interrupting the Supply Chain Management (SCM) services supporting the delivery process of the automotive sensitive components.

Table 2 shows the attacker's actions, the CYRENE platform's findings and the end-user's responsive actions.

Cyber Attacker	Pilot end-user/CYRENE services
1.A disgruntled, fired, inbound logistic technician, still holds valid access credentials to the assets of the EV battery supply chain. The attacker physically accesses the Stellantis Warehouse to short-circuit some EV batteries using the valid credentials of the revengeful inbound logistics technician.	2.CYRENE detects the anomaly (thermal runaway) in the IoT sensory data.
3.The cyberattacker uses the valid access credentials of the rogue technician to access the supply chain management (SCM) assets and intrudes the supply chain Frontend Server.	4.CYRENE detects the intrusion via its IDS services.
5.The attacker stops the permanent storage and recording services by blocking the data tracking, and the data ingestion functions of the SCM.	6.CYRENE detects the interruption of the Database (DB) service, reports the events, and allows the user to monitor the system security level and anomalies. 7. The CYRENE dynamic vulnerability management services detect, analyse, and assess the vulnerabilities identified in the interconnected ICT components/systems of the sectorial (inbound logistics) process.
-	8. The user utilizes the CYRENE Forecasting and Attack Behavior Simulation services to experiment on potential cascading effects and estimate the impact to the sectorial asset network.
-	9. The user performs risk assessment on the sectorial assets involved in the inbound logistics process related to the delivery of EV batteries.
-	10. The user implements controls on the sectorial assets and reassesses them in the CYRENE platform which accurately reflects the implemented measures and excludes the corresponding mitigated vulnerabilities or threats score from the risk overall results providing the actual risk exposure after the controls' application.
-	11. The CYRENE platform creates an overall of all the above findings. The user consults the report to develop the Protection Profile of the sectorial processes and assets that participate In the Vehicle Transport Service.

Table 2. The Factory Pilot scenario.

5. Pilot outcomes and Conclusions

After each pilot execution, pilot participants evaluated the CYRENE platform, according to the experience gained and their SCS needs via filling dedicated online questionnaires and validating the CYRENE platform against specific quality variables, such as service quality, usability, satisfaction, performance efficiency based on ISO/IEC 25010 [24]. The overall feedback gained from pilot end-users was positive. Nevertheless, the end users provided suggestions for UI/UX improve-ments that drove the technical development lifecycle of the CYRENE platform until the release of its final ver-sion. The lessons learned from the pilot evaluation activities and the project results lead to the develop-ment of best practices illustrating how to perform risk assessment on complex, multi-actor supply chain envi-ronments, such as the Maritime Transport ecosystem. In addition, guidance provided, indicating to auditors how to conduct a conformity assessment to explore whether the SCS is subject to cybersecurity certification accord-ing to a given certification scheme.

Eleni Maria Kalogeraki is a Business Intelligence and Information Security researcher. She cooperates with MAGGIOLI SPA - Greek Branch S.A. providing ICT consulting services in the areas of IT security evaluation, system validation and conformity assessment in the context of EU research projects. During her career, she has been involved in more than 11 European Research and Innovation projects, applied in various industries (i.e., Maritime Transport, Energy, Health, Aviation, Privacy Sector). Ms Kalogeraki has authored more than 20 publications in cybersecurity research areas, Critical Infrastructure Protection, standardization, certification, and knowledge management. She has received a most outstanding paper award by the Operational Research Society for an article published in Knowledge Management Research & Practice journal in 2018/19. She is now completing her PhD on Critical Infrastructure Protection at the Dept. of Informatics of the University of Piraeus and she is member of the university's Cybersecurity Research Lab (CSRL). She holds a M.Sc. Degree in Informatics from the University of Piraeus and a B.Sc. Degree in Public Administration from the Panteion University of Social and Political Sciences. Throughout her career, she has worked in the private sector as an economist and business analyst (i.e., oil accounting, risk tolerance consulting, etc.) and has held Teaching Assistant positions in the Education Sector (i.e., Hellenic National School of Public Administration). She is a registered member of the Economic Chamber of Greece and a class B beneficiary Accountant-Tax Consultant.

Danijela Boberić Krsićev is an associate professor at Faculty of Sciences, University of Novi Sad, Serbia. She taught more than ten different academic courses in various areas of Computer Science and IT. Her research pursuits primarily revolve around the development of information systems. She boasts a robust background in the information technology and services sector. Lately, her focus has shifted towards the analysis of big data. Mrs. Boberić Krstićev defend her PhD thesis focused in Development of Information Systems at the Faculty of Sciences, Serbia. She has published more than 30 research papers and participated in several international projects including H2020, Erasmus, Interreg transnational and cross-border, and SCOPES. Contact her at dboberic@uns.ac.rs.

Dr Sophia Karagiorgou is currently leading the Artificial Intelligence & Machine Learning department in UBITECH, being responsible for data-driven IT projects execution and delivery. She is also an Adjunct Lecturer at the Department of Informatics and Telematics of the Harokopio University of Athens (teaching Artificial Intelligence, AI in the Web of Things, Advanced AI topics and Deep Learning). She holds a PhD in data management from the National Technical University of Athens (2014); a MSc. with honors from the Department of Electrical and Computer Engineering of the University of Thessaly and a BSc. from the Computer Science Department of the University of Crete. She has been certified with the ITIL Foundation Certificate in IT Service Management and she has demonstrated skills in Big Data & Data Analytics, Databases, Process Modeling, SOA, JAVA, Python, C++ and C#. Her research interests involve algorithms for big data management, scalable data analytics and information retrieval from structured and unstructured data.

Giulio Vivo is a senior researcher of Centro Ricerche FIAT. He graduated in Information Science in 1986 and joined CRF in 1987. From 1986-1989 he worked at Tecnopolis (Bari) dealing with innovative computer vision, inspection, robot guidance, knowledge-based vision systems, 2D and 3D pattern recognition, and dedicate applications for the FIAT group plants. He has participated to various EU RTD programs, starting with EUREKA-Prometheus, and in the 2001 to the MIT Sloan School – Managing Corporate Innovation: Linking Business & Technology Strategies in the Next Decade. Afterwards, he has worked in the domain of the preventive safety and the cooperative ITS systems, contributing to a significant number of projects on these subjects. Among the others he coordinated the largest FP6 EU initiative on V2V and V2I Communication, the SAFESPOT project. Dr. Vivo is currently involved within Stellantis as Project Manager and Senior Researcher in Advanced Product Development department and Factory Innovation activities, by promoting the adoption of the Industry 4.0 paradigms towards the modernization and digitalization of the Stellantis productive settlements in Europe and abroad.

Pablo Gimenez is an ICT Project Manager. He holds a M.Sc. degree in telecommunication engineering from the Polytechnic University of Valencia. He became a member of the Distributed Real-Time Systems research group of the Communication Department at the UPV, where he received his Ph.D. He was involved in research projects related to sensor networks for logistics services, industrial safety, and security assurance for smart grids. Pablo Gimenez works since 2015 at Fundacion Valenciaport as an ICT Project Manager in research projects related to ICT, IoT, Big Data, and cyber-security. He is also a Project Manager Professional from the Project Management Institute.

References

[1] UNCTAD (2022), "COVID-19 and Maritime Transport - Navigating the Crisis and Lessons Learned". Online available: https://unctad.org/publication/covid-19-and-maritime-transport-navigating-crisis-and-lessons-learned

[2] UNCTAD (2022), “Digitalization of Services: What does it imply to trade and development? Online available: https://unctad.org/publication/digitalization-services-what-does-it-imply-trade-and-development

[3] MarPoint (2023), “Maritime cyber-attacks on the rise”. Online available: https://marpoint.gr/blog/maritime-cybersecurity-attacks-on-the-rise/

[4] Tripwire (2023), “A Look at the 2023 Global Auto-motive Cybersecurity Report”. Online available: https://www.tripwire.com/state-of-security/global-automotive-cybersecurity-report

[5] The Maritime Executive (2023), “Ransomware Attack Stops Container Operations at Japan’s Na-goya Port”. Online available: https://www.maritime-executive.com/article/ransomware-attack-stops-container-operations-japan-s-nagoya-port

[6] ZDNet (2022), Europe's biggest car dealer hit with ransomware attack”. Online available: https://www.zdnet.com/article/europes-biggest-car-dealer-hit-with-ransomware-attack/

[7] Ralston, Patricia AS, James H. Graham, and Jef-ferey L. Hieb. "Cyber security risk assessment for SCADA and DCS networks." ISA transactions 46.4 (2007): 583-594.

[8] Tešendić T., Kalogeraki E.-M., Vivo G., Polemi N., Krstićev B.D. (2023), "Quantifying asset criticality in supply chains". In proceedings of the IEEE 9th In-ternational Conference on Engineering and Emerging Technologies (ICEET 2023) (in press).

[9] CYRENE EU H2020 project, “Certifying the Securi-ty and Resilience of Supply Chain Services”. Online available: https://www.cyrene.eu/.

[10] Polemi N., Kalogeraki E.M. et al (2021), Report “D3.1 Conformity Evaluation Process & Multi Level Evidence Driven Supply Chain Risk Assessment”, CYRENE EU H2020 project, September 2021. Online available: https://zenodo.org/records/6786244

[11] Directive (EU) 2022/2555 of the European Parlia-ment and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and re-pealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). Online available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[12] European Parliament and Council, Regulation (EU)2019/881 on ENISA and on information and communications technology cybersecurity certifica-tion and repealing Regulation (EU) No 526/2013 (Cybersecurity Act), April 2019. Online available: https://eur-lex.europa.eu/legal-con-tent/EN/TXT/PDF/?uri=CELEX:32019R0881&qid=1695663489885.

[13] ISO/IEC 27k series, Information Security Manage-ment. Online available: https://www.iso.org/standard/iso-iec-27000-family

[14] ISO 28000:2022, Security and resilience - Security management systems Requirements. Online avail-able: https://www.iso.org/standard/79612.html

[15] ISO/IEC 15408: 2022 “Information security, cyber-security and privacy protection — Evaluation crite-ria for IT security”. Online available: https://www.iso.org/standard/72891.html

[16] Common Criteria for Information Technology Secu-rity Evaluation (Parts 1-5) Rev.1 (2022). Online available: https://www.commoncriteriaportal.org/cc/

[17] ISO/IEC 18045:2008, Information technology - Security techniques - Methodology for IT security evaluation,. Online available: https://www.iso.org/standard/46412.html.

[18] Polemi N., Michota A., Ioannidis S., "A Proposed Cyber Security Certification Scheme for Supply Chain Services" Maritime Interdiction Operations Journal, 23(2), 2022, ISSN: 2241-438X

[19] Michota, A., & Polemi, N. et al (2022), Report “D2.2 A Cybersecurity Certification proposed Scheme for Supply Chain Services (EUSCS). CYRENE EU H2020 project, September 2021. Online available: https://zenodo.org/records/6786175.

[20] ENISA (2021). Cybersecurity Certification EUCC, a candidate cybersecurity certification scheme to serve as a successor to the existing SOG-IS, v1.1.1, May 2021, Online available: https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme-v1-1.1.

[21] FIRST (2019). Common Vulnerability Scoring Sys-tem (CVSS) v3.1, Specification Document, Revi-sion 1. Online available: https://www.first.org/cvss/specification-document.

[22] ISO/IEC 27001:2022, Information Security Man-agement System. Online available: https://www.iso.org/standard/27001.

[23] ISO 28001:2007, Security Management System for the Supply Chain. Online available: https://www.iso.org/standard/45654.html.

[24] ISO/IEC 25010: 2011 “Systems and software engi-neering — Systems and software Quality Require-ments and Evaluation (SQuaRE) — System and software quality models”. Online available: https://www.iso.org/obp/ui/#iso:std:iso-iec:25010:ed-1:v1:en (Last accessed: 20-09-2023).

Securing the Open Source Software Supply Chain for Critical Warfare Assets

by Eric Hill, EMBCA

Introduction

We live in a software defined world. The evolution of the Defense Industrial Base (DIB) coupled with US Department of Defense (DoD) requirements and reinforced by use cases in the battlespace of Ukraine, make it clear that we are in the era of **software defined warfare**. Software has become an axis of innovation at the speed of relevance while presenting an attack surface advantaged by adversaries.

The authors first two white papers published in the NMIOTC Journal, "Securing the Software Supply Chain for Naval Warfare Systems" and "Securing the Open Source Software Supply Chain for Naval Warfare Systems", addressed capabilities to ensure software is cyber ready & cyber resilient. However, in the context of the DoD DevSecOps Software Factory, one key aspect had yet to be addressed. Weapons systems software, or rather software classified as secret or top secret, requires security gate capabilities to be brought across 'the air gap".

This white paper will readdress some concepts in the aforementioned NMIOTC published documents while topically covering the key issue of the air gap. An attempt is made to address the subject matter in a manner contextual to legislators & policy makers yet broadening the ecosystem perspective of engineers that may be focused at a low level on specific aspects.

The impetus for this third white paper was a series of articles published in outlets following the "6th NMIOTC Cybersecurity Conference in the Maritime Domain" highlighting well known issues in US naval assets as well as restating some of the issues the author had touched on at the conference. As well, DoD and US Navy directives, that will be touched on later, gave more clarity not only to timeline of implementation but accepted Risk Management Framework parameters in a software factory configuration.

In February 2023, CIMSEC featured "Paralyzed at the Pier: Schorodingers Fleet and System Naval Cyber Compromise" highlighted issues of vulnerabilities in US naval assets; the reasons why the author originally decided to present at NMIOTC. One particular statement stood out:

"Consider two adversaries who have both compromised the software supply chains of the conventional forces of the opposing side. Each is faced with uncertainty regarding what forces will and will not be impacted at the point of initial aggression and therefore face an incalculable risk toward their respective chances of success."

Then in March 2023 an article appeared in the US Navy's CHIPS that paralleled the concepts presented in the previous white papers relating to JADC2, cyber readiness, cyber intelligence repositories, related dashboards, etc . The article called out the AEGIS Weapons System specifically; teams with which the author has had the honor to engage with on DevSecOps security gate technology relayed later in this paper:

"Our nation's critical warfare assets, such as Arleigh Burke class destroyers (DDGs) and the AEGIS Weapons System (AWS), are uniquely difficult to protect from cyberattacks. They are examples of large Systems of Systems (SoS) running multiple concurrent mission threads, presenting vast numbers of threat surfaces that include complex integrated systems, satellite communications links, sensor fusion platforms and many human/machine interfaces."

And yet as the concept of this white paper was evolving, reinforcement of its need arrived on July 31, 2023 in an article titled "Officials Found Suspected Chines Malware Hidden in Various US Military Systems" appearing in INSIDER and quoting an NSA executive:

"… unlike previous attacks, experts say the intent is more likely to disrupt rather than to surveil … Now, experts say this new wave of malicious code has the ability to disrupt US military and civilian operations.

… Last month, Rob Joyce, the director of cybersecurity at the NSA, called the nature of this malware 'really disturbing.' "

This white paper is the third in the series presented by the author at NMIOTC 2021 & 2022. The contents, while providing a bit of a conceptual review of the previous two, is intended to take the model a step further into aligning with DoD and US Department of the Navy (DON) guidance. Further, as the author stepped away for the "the 6th NMIOTC Cybersecurity Conference in the Maritime Domain" it was realized the important topic of bringing Software factory security gate capabilities across the air gap had yet to be addressed.

Thus, this white paper will present a series of interrelated concepts involved with air gapped systems. An attempt is made to "over simplify" some of the concepts, especially architecture, so that a novice in the private sector or a legislator/minister concerned with high level policy will be able to walk away with a contextual understanding of this very complex cyber topic. It is the author's hope that between the three white papers, those that are involved very intricately with projects will gain an "ecosystem understanding" while those that are non-technical stakeholders will be engaged. The impetus being that with simplicity we can begin to solve more complex scenarios.

Secret and Top Secret

The US Government has a number of data classifications (depicted in **Figure 1**); each related to the data's implications to US national security. For the sake of this white paper, it is assumed that within the air gapped environment we are working on programs that are classified as "secret" or "top secret". In other words, "critical warfare assets" as mentioned in the introduction.

Further, it is not uncommon to hear references from software teams working in enclaves speaking to the "high side" and the "low side". For the sake of simplicity in this white paper, the "high side" refers to "secret" or "top secret" within the air gapped environment and the "low side" to have full internet exposure.

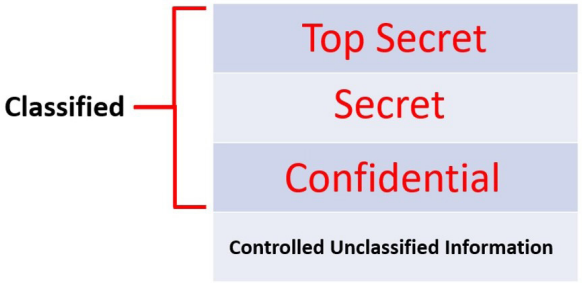


Figure 1- DoD Simplified Data Classification by author

As an aside we have in **Figure 2** a cut out from the DON's "Telework Capabilities" placemat. It depicts DoD networks, the classification and the controls related to their protection. It is worth noting that SIPRENET is the DOD's "secret" network. While **Figure 2** contains up to IL6, there is IL6+ known in the industry.

For the sake of this white paper, we will assume we are working in an air gapped enclave, such as a SCIF or SAPF (Special Access Project Facility), with IL6 & IL6+ controls. However, there is not necessarily the assumption that the enclave is connected to an IL6 or IL6+ network, such as SIPRENET or JWICS, and as such considered out of scope for this document.

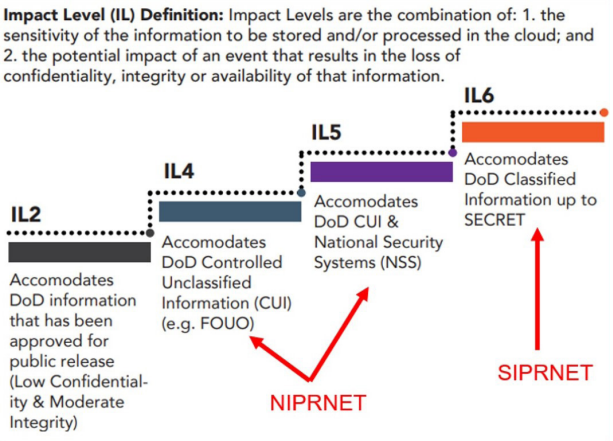


Figure 2 - US Dept of the Navy Telework Capabilities - red by author

DOD Zero Trust Strategy

Nov 2022 the DoD released the Zero Trust Strategy document. The capabilities to secure applications, and security gates in the DoD Software Factory configuration, exist in pillar 3 (see **Figure 3**) and indicated by the solid red rectangle. As we live in a "software defined world" there is a play in all pillars indicated by the dashed red rectangles.

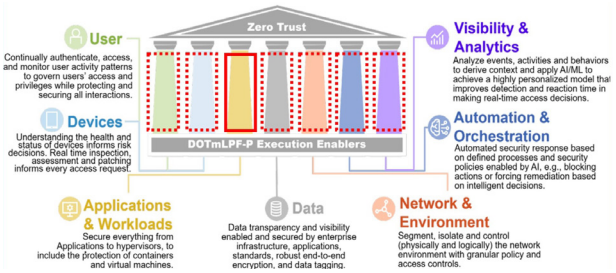


Figure 3 - DoD Zero Trust Strategy p.10, red annotations by author

Also important is the capability rollout schedule for Applications & Workloads per the DoD indicates that that full implementation of capabilties have a milestone set for 2027.

In August 2023, the DON published its "Strategic Intent to Implement Zero Trust". The memorandum include the following precise statement with the indicated year of sup-

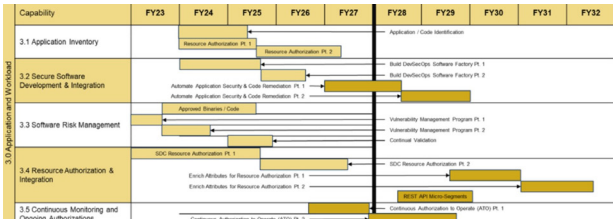


Figure 4 - DoD Zero Trust Strategy - Capability Timeline p. 24

port, 2027, correlating to the capabilities timeline in **Figure 4**.

"*The Program Executive Officer (PEO) for Digital and Enterprise Services (Digital) will continue to develop key zero trust capabilities, including NIS, Flank Speed, and the MCEN, in alignment with the DoD zero trust framework and DON technology direction, and will make target level activities available globally to enable adoption of zero-trust aligned platforms and services in as many environments and conditions as possible in accordance with reference (s) NLT the end of FY 2027.*"

RAISE 2.0

The previous year, or more precisely Oct 4, 2022, the DON published RAISE 2.0 or rather "Rapid Assess and Incorporate Software Engineering". The hand book is direct in its intent on page 1:

"The purpose of this document is to enable the Department of Navy (DON) Digital Warfighter to rapidly respond to the evolving demands of cyber warfare and achieve continuous cyber readiness …

… To accelerate capability delivery, the Rapid Assess and Incorporate Software Engineering (RAISE) process was developed with Agile & DevSecOps practices in mind …"

Further, per unclassified briefing, US Navy staff does refer to RAISE2.0 as a software factory program. Thus, this white paper takes liberty to shift some of the RAISE2.0 capabilities into the security gate context of a US DoD DevSecOps software factory.

ID	Description
GATE 1	must provide Static Application Security Testing (SAST) for available source code
GATE 2	must provide Dependency List or Software Bill of Materials (SBOM)
GATE 3	must provide Secrets/Keys Detection CWE-798
GATE 4	must provide Container Security Scanning (CSS)
GATE 5	must provide Dynamic Application Security Testing (DAST)
GATE 6	must provide a step to allow the RPOC ISSM to review
GATE 7	must sign the release container image
GATE 8	must store the release container image in an artifact repository

SCA

Figure 5- RAISE 2.0, Requirements p. 11
w/ red markup by author

Figure 5 highlights gates that must be supported in the RAISE 2.0 RMF. While the table specifically notes **SAST** (Software Application Security Testing) and **DAST** (Dynamic Application Security Testing) it does not specifically call out **SCA** (Software Composition Analysis). As highlighted in "Securing the Open Source Software Supply Chain for Naval Warfare Systems" (2022 NMIOTC Journal) **SCA** is a class of tools critical to securing any programs open source software supply chain. Thus, the author has taken the liberty to group RAISE2.0 gates **2** & **4** as functions of **SCA**. As to the importance of these security gate, the SBOM is critical to transparency of OSS in software and container image scanning important aspect of the software factory that are both included in commercial **SCA** capabilities.

Further, there are **SAST** scanners that test for secrets/keys detection or rather CWE-798 (more on CWE's in the next section). Keeping in the spirit of simplicity, RAISE2.0 gates **1** & **3** are grouped under the **SAST** capability. Furthermore, where as weapons systems programs will typically require two **SAST** scanners, only one will be considered in this paper to keep redundancy out of architecture & data flow diagrams.

CWE, CVE, CAPEC

Figure 7 shows a table matching the basic lexicon to security gate technology. To put it simply, **SCA** is utilized to scan OSS (free open source software) binary files to match against known OSS components and their CVE's. **SAST** capabilities on the other hand, scan text code for CWE's. Currently weapons systems must do extensive reporting for any CWE's that are revealed from **SAST** scanning; ideally there are zero.

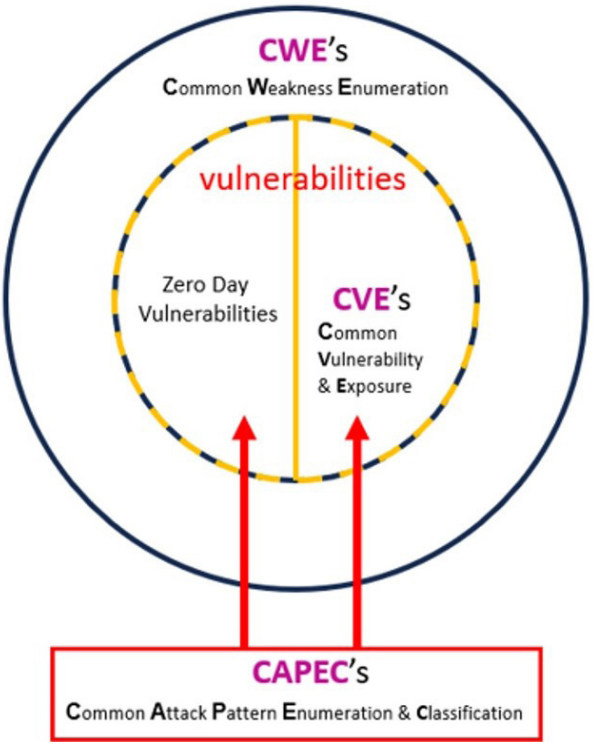


Figure 6 - CWE's, CVE's, CAPEC's by author

In reviewing **Figure 6**, a software factory's **DAST** capability is used to exercise CAPECs against code that is executing in a process such as an application server, a web service, etc. By exercising a CAPEC that exercises a CWE a vulnerability, including a zero day, may be exposed and thus fixed before deploying a container image from the software factory. In the case of a CVE against 3rd party OSS, **DAST** could possibly catch if missed by the **SCA** capability. Likewise, scanning proprietary code with **SAST** capability for CWE's helps in avoidance of zero day vulnerabilities. It is worth mentioning that data regarding vulnerabilities on specific weapons systems software is classified information.

The SCA, SAST, DAST capabilities mapping to security gates will be revisited later in this paper after bringing the

capabilities across the "air gap" has been addressed.

Security Gate Type	Action	Scans	Note
SCA	Scans binaries for FOSS (SBOM) & its related vulnerability intelligence (CVE's)	binaries	CVE
SAST	Scans source code for CWE's	code	CWE
DAST	Scans running process on a network w/ CAPECs to test for **vulnerabilities**	Running processes on network	CAPEC

Figure 7 - SCA, SAST, DAST by author

Aligning RAISE2.0 & DoD Software Factor Security Gates

Figure 8 aligns the **RAISE 2.0** gates that we matched to **SCA**, **SAST** & DAST capabilities with the software development life cycle of a DoD Software Factory. This will be walked through in example once we present the capabilities across the "air gap" in the enclave.

There are various strategies for enabling access to the public open source software (OSS) repositories (maven, npm, pypi, etc) from within an air gapped enclave for development teams. Later sections will assume that the public OSS repositories are available from within the air gapped enclave. This will simplify the discussion to focus on the security gate capabilities.

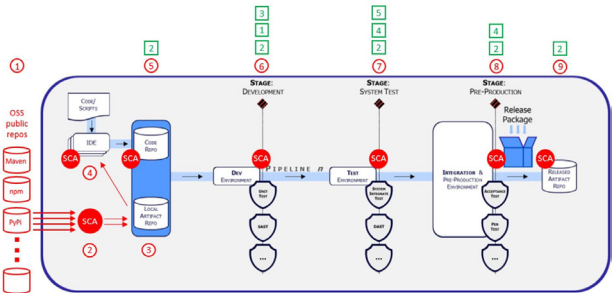


Figure 8 - Raise 2 Gates to DSO Software Factory SDLC by DoD DevSecOps guides diagram w/ red & green markup by author

Simplified Security Gate Architecture

In **Figure 9** the capability architecture is broken down into its 3 component capabilities; SCA, SAST and DAST. The assumption, per the DoD DevSecOps playbooks, is that Kubernetes (denoted as "**k8**") is being utilized. Further, the assumption is that the runtime application is composed of an OCI compliant container image executing in the container environment with cyber posture maintained; as necessary to be placed in the US Air Force's Iron Bank. There is a vast mismatch of storage requirements when comparing **SCA** to **SAST** & **DAST**. Thus, we will disregard any database requirements of the **SAST** and **DAST** capabilities and focus on the storage of vulnerability intelligence in relation to the **SCA** capability.

In the experience of the author, the storage requirements and updating of the SCA vulnerability intelligence is one of the most difficult challenges to overcome. Therefore, care is given to simplify not only the architecture but the use cases for data flow. It should also be noted that the "backend service" that composes "vulnerability intelligence' is typically composed of a number of container images executing at runtime in their own architecture. This varies in the industry and is intentionally disregarded to avoid complexing the air gap transfer use cases highlighted later.

Figure 9 - Simplified Architecture to Support Security Gate Capabilities by author

Air Gap Definition

NIST defines air gap as:

"An interface between two systems at which (a) they are not connected physically and (b) any logical connection is not automated (i.e., data is transferred through the interface only manually, under human control)."

This is the definition utilized for the next sections of the white paper. However, it is a bit misleading for mature enclave teams. In the experience of the author, using data diode technology, much actually can be automated. The implementation of "human control" is also dependent on the culture of the enclave development team and stakeholders. This is a vital point to remember.

Air Gapped Security Gate Capability Architecture

Figure 10 expands the security gate architecture into a data flow across the air gap. In "sneaker net" the diagram and accompanying use cases default to the simplest, and perhaps least mature, method of bringing & maintaining capabilities across the air gap. A team member literally transports the storage mechanism (SSD) into the enclave. Top left of the diagram is representative of capabilities' (SCA, SAST, DAST) OCI compliant images and vulnerability intelligence available in the cloud. The SSD icon represents "solid state storage". In **ETL** we have Extract-

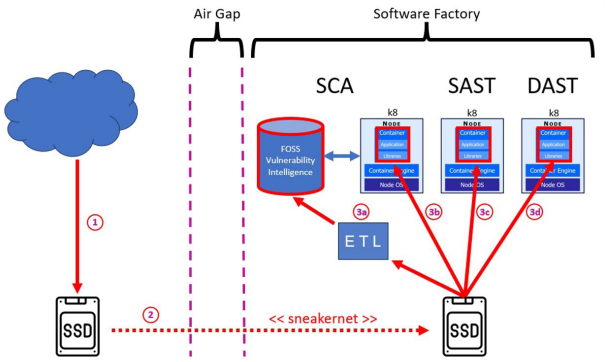


Figure 10 - Air Gapped Security Gate Architecture
by the author

Transform-and-Load functions used to transform data from a file systems (such as SSD) and upload to a database. This can be implemented in scripts or a number of commercial solutions.

In the architecture and dataflow, there are 3 main use cases to bring/maintain the 3 security gate capabilities (**SCA**, **SAST** & **DAST**) across the air gap:

1. Initial install across the air gap
2. Container image release update
3. OSS vulnerability intelligence daily update

The 3 use case outlines follow.

Initial Install Across the Air Gap:

Due to the vast amount of OSS vulnerability intelligence, this will generally take the longest amount of time. Thus, care should be taken on timing of both the initial download and transfer into the enclave as well as the ETL process applied in the enclave to populate the vulnerability intelligence database.

1. Download to SSD of DAST, SAST, SCA container images as well as all vulnerability intelligence data.
2. Transfer SSD via "sneaker net" into the enclave
3.a. Transfer large data upload via ETL of all vulnerability intelligence to the vulnerability intelligence database
b. Upload **SCA** container image to execute in a Kubernetes Node (container)
c. Upload **SAST** container image to execute in a Kubernetes Node (container)
d. Upload **DAST** container image to execute in a Kubernetes Node (container)

Container Image Release Updates:

With each new major or minor version release update of the **SCA**, **SAST** or **DAST** capabilities, the Software Factory stake holders may review and opt to upgrade the OCI-compliant image executing in the respective k8's node container. While this use case treats the capabilities in sync, this is more often not the case as the capabilities are usually provided by differing vendors. Even in the cases where the same vendor provides **SCA**, **SAST** or **DAST**, the release schedules are often independent of one another.

1. Download to **SSD** of **DAST**, **SAST**, **SCA** container images.
2. Transfer **SSD** via "sneaker net" into the enclave.
3.b. Upload **SCA** container image to execute in a Kubernetes container
c. Upload **SAST** container image to execute in a Kubernetes container
d. Upload **DAST** container image to execute in a Kubernetes container

OSS Vulnerability Intelligence Update:

1. Download daily increment of OSS vulnerability intelligence data to SSD
2. Transfer to SSD via "sneaker net" to into the enclave
3.a. Transfer daily vulnerability intelligence increment via ETL to the vulnerability intelligence database

It is extremely important that the vendor of the **SCA** capability provides daily updates to the in-enclave vulnerability intelligence. The update time duration for the vulnerability intelligence data that will be ETL'd will be much smaller than if done on weekly intervals. In addition, daily updates will minimize exposure to newly discovered OSS vulnerabilities as the intelligence will be day- relevant to the OSS components in the public OSS repositories.

This is not only true for vulnerabilities. Adversaries to the Free World have been conducting maligned operations inserting "malicious" open source components into the public OSS repositories. In these cases, exposure of an air gapped software factory, engaged in "secret" or "top secret" efforts, can be mitigated.

Air Gapped Software Factory

As RAISE2.0 documentation implies DevSecOps cultures vary among stake holders and teams working on various DSO software factory efforts. Skill sets, past experience, future timelines and budget all come into play in one way or another. Taking this into consideration, in this section we present a high level scenario mapping certain RAIS2.0 gates previously mapped to **SCA**, **SAST** and **DAST** capabilities. This relationship is depicted in **figure 11** with **SAST** and **DAST** annotated in the original DoD diagram and SCA and other annotations noted in red. RAISE2.0 gates noted previously appear in green.

As mentioned, developers for critical warfare asset software are typically required to utilize 2 **SAST** scanners. For purposes of this white paper, they are collapsed into 1 SAST capability. In addition, in the author's experience, and noted in *"Securing the Software Supply Chain for Naval Warfare Systems"* (NMIOTC 2021) SAST is normally applied by the developer before checking in code as well as (in the case of GIT) when a pull request is issued. This is disregarded in the scenario below.

The reader should also remember that copies of the pub-

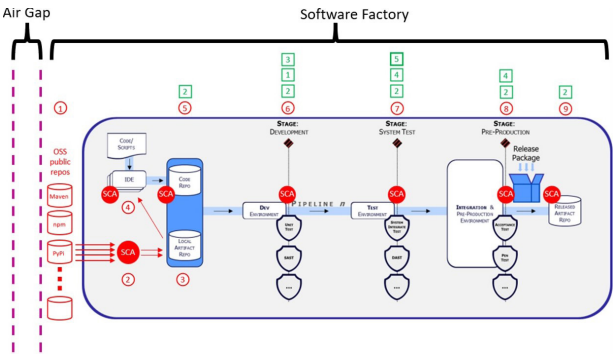


Figure 11 - DoD DSO Software factory with black, purple, red, green annotations by author

lic OSS repositories are assumed to be available within the air gapped enclave.

Note that the red numbers below map to the life cycle numbers in **Figure 11** above.

A Simple Air Gapped Software Factory Scenario:

1. – 5. No **SCA**-capability policy violations for OSS components, **CVE's** nor "malicious", pulled from the OSS public repos for use in software.

6. CI/CD performs the following:

a. **SAST**-capability to scan for CWE's in proprietary source code (including passcodes & keys in CWE-198) – If no CWE's proceed to 6.b.

i. Supports RAISE2.0 gate 1 and gate 3

b. Build of mission software using package manager technology

i. For instance in java ecosystem using the mvn package manager to build a .war

c. **SCA** capability to create SBOM and pull vulnerability intelligence on OSS – If no CVE's that exceed policy proceed to 7

i. Supports RAISE2.0 gate 2

7. CI/CD performs the following:

a. Build an OCI compliant container image

i. For instance from the java**.war** in 6.b.i

b. **SCA** capability scan to create SBOM and pull vulnerability intelligence on OSS – If no CVE's that exceed policy proceed to 7.c

i. Supports RAISE2.0 gate 2 & gate 4 – See "Securing the Open Source Software Supply Chain for Naval Warfare Systems" (NMIOTC Dec 2022) to better understand posture on deployed containers

c. Instantiate OCI compliant image to staging Kubernetes cluster

d. DAST-capability scans on container – If no CVE's/vulnerabilities proceed to 7.d.

e. Functional testing – If pass proceed to 8

8. CI/CD Performs the following:

a. As time has elapsed, **SCA**-capability to re-status SBOM for vulnerability intelligence on OSS – if no CVE's to 8.b

i. Supports RAISE2.0 gate 2 & 4

b. **SCA**-capability to Export CycloneDX or SPDX representation of SBOM & insert into *"release artifact repo"*

i. Supports RAISE2.0 gate 2

c. Sign the OCI-compliant image

i. Supports RAISE2.0 gate 7

9. CI/CD Performs the following:

a. Publish OCI-compliant container image to *"release artifact repo"*

i. Supports RAISE2.0 gate 8

b. Publish, CycloneDX/SPDX **SBOM** & other artifacts to "release artifact repo"

i. Support RAISE2.0 gate 2 & gate 8

c. **SCA** capability to place in-memory SBOM under continuous re-status of CVE posture for immediate stakeholder messaging if security policy exceeded on new CVE's in the future

i. Supports *"vulnerability management"* via situational awareness of cyber posture on container images deployed to assets - See "Securing the Open Source Software Supply Chain for Naval Warfare Systems' (NMIOTC Dec 2022) to better understand posture in assets

ASOC to Calibrate & Measure

"Securing the Software Supply Chain for Naval Warfare Systems" (NMIOTC 2021, by author) included a recommendation that ASOC tooling be utilized to calibrate software factory function and efficiency. The author has verified via unclassified briefings that in the context of RAISE 2.0 this is, in fact, being done.

Figure 12 displays for the reader a higher level ASOC diagram presented in the context of the capabilities introduced in the aforementioned white paper. Transferring ASOC capabilities across the air gap as well as usage in the enclave will perhaps be the subject of future white papers.

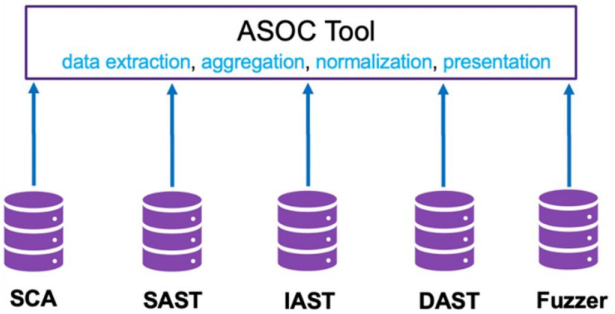


Figure 12 - ASOC tooling for DSO security gate capabilities from "Securing the Software Supply Chain for Naval Warfare Systems" – NMIOTC 2022 by Eric Hill

Summary

The US Navy has set the "DevSecOps maritime pace" with the RAISE 2.0 software factory RMF platform. Meanwhile, kinetic war that arrived in Europe 2022 is continuing unabated and supported by maligned cyber activities. The need for cyber ready and cyber resilient systems has

been proven at the tactical edge. With the resurgence of the CJADC2 (Combined Joint All Domain Command and Control) it is of utmost importance that critical warfare assets of the USA, NATO and other allies and partners are at all times cyber ready and cyber resilient. We are only as cyber ready and cyber resilient as the lowest grade system.

In composing this white paper, it is the authors hope that that the daunting topic of transfering capabilities "across the air gap" into Software Factory configurations will perhaps be more normalized and thus funding and execution on the minds of legislators, ministers and other stake holders across the Free World. The functioning of our critical warfare assets in CJADC2 configurations, and thus national security of all of these nations, will depend on it … Sea, Air, Space and Land.

About the Author

Eric Hill has a BS in Computer Engineering from the University of New Hampshire. His industry career spans 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. Throughout his career, including as the Chief Software Architect of a division of a large DIB prime, he has worked with "dual use" technologies. Eric has presented in a number of forums over the years including defense & intelligence community conferences. He has specifically presented at NMIOTC conferences 3 times. While Mr. Hill works in the defense industry, he provided this white paper for educational purposes in his capacity as a volunteer director with the Eastern Mediterranean Business Culture Alliance non-profit in New York city where he serves as a DIB SME.

LinkedIn: https://www.linkedin.com/in/eric-hill-316300b

References

DoD CIO Library
https://dodcio.defense.gov/Library/
DoD Information & Communications Technology Supply Chain Risk Management
https://www.denix.osd.mil/ict-scrm/policy-governance/
RAISE 2.0 Memo and Implementation Guide – Nov 3, 2022
https://www.doncio.navy.mil/ContentView.aspx?ID=15943
Strategic Intent to Implement Zero Trust Memo Released – Aug 14, 2023
https://www.doncio.navy.mil/ContentView.aspx?id=16397
US Navy Telework Capabilities v14 – US Navy
https://media.defense.gov/2020/May/18/2002302035/-1/-1/1/NAVY_TELEWORK_CAPABILITIES_V14.PDF
Common Weakness Enumeration - Mitre
https://cve.mitre.org/
Common Weakness Enumeration - Mitre
https://cwe.mitre.org/
Common Attack Pattern Enumeration and Classification - Mitre
https://capec.mitre.org/
Classification, Declassification of National Security Information
https://www.ecfr.gov/current/title-12/chapter-IV/part-403

Author's Previous NMIOTC White Papers

"Securing the Open Source Software Supply Chain for Naval Warfare Systems" – by Eric Hill, submitted Sep 2022
https://nmiotc.nato.int/wp-content/uploads/2022/12/24-2022.pdf#page=27
"Securing the Software Supply Chain for Naval Warfare Systems" – by Eric Hill, submitted Sep 2021
https://nmiotc.nato.int/wp-content/uploads/2022/04/23-2021-B.pdf#page=33

Other References

"Return of CJAD2: DoD Officially Moves Ahead with "combined" JADC2 in a Rebrand Focusing on Partners" – Breaking Defense, May 2023
https://breakingdefense.com/2023/05/return-of-cjadc2-dod-officially-moves-ahead-with-combined-jadc2-in-a-rebrand-focusing-on-partners/
"Officials Found Suspected Chinese Malware Hidden in Various US Military Systems"
https://www.businessinsider.com/us-officials-found-chinese-malware-hidden-in-military-systems-2023-7
"A New Cyber-Resilient Approach for Warfighting Platforms" – Mar 2023
https://www.doncio.navy.mil/chips/ArticleDetails.aspx?ID=16063
"Marine Corps Launches Software Factory" – Mar 2023
https://www.marines.mil/News/News-Display/Article/3325399/marine-corps-launches-software-factory/
"Paralyzed At the Pier: Schrodinger's Fleet and Systemic Naval Cyber Compromise" – Feb 22, 2023
https://cimsec.org/paralyzed-at-the-pier-schrodingers-fleet-and-systemic-naval-cyber-compromise/
"How Software Factories Help the DoD Scale DevSecOps" – April 29, 2022
https://fedtechmagazine.com/article/2022/04/how-software-factories-help-dod-scale-devsecops-perfcon
"NAVWAR Launches First Secret-Level DevSecOps Pipeline" – July 28, 2021
https://www.navy.mil/Press-Office/News-Stories/Article/2710817/navwar-launches-first-secret-level-devsecops-pipeline/
"Small Companies Can't Access Classified Work Without a Secure Space to Work In" – Aug 3, 2023
https://www.forbes.com/sites/erictegler/2023/08/03/small-companies-cant-access-classified-work-without-a-secure-space-to-work-in/amp/

NMIOTC Annual Information Meeting & Advisory Board 2023

NMIOTC's Annual Information Meeting (AIM) and Advisory Board (NAB), chaired by NMIOTC Commandant, were held at the Center's premises on Thursday 2nd February 2023.

33rd Cryptographic Services Capability Team (CryptoCaT) Meeting

From 6th to 8th March 2023, the "33rd Cryptographic Services Capability Team Services Conference" (Crypto CaT) meeting was conducted atthe NMIOTC premises. The meeting was attended by 67 participants, coming from NATO HQ, Strategic Commands ACT and ACO, Military Committee Agencies, NCIA, NATO Chief Information Office (CIO) and 25 NATO and Partners countries.

Course 27000 “Maritime Sniper Course”

From 7 to 19 May 2023 the NMIOTC Maritime Sniper Course was conducted at NMIOTC premises and in the broader area of Chania, Crete.

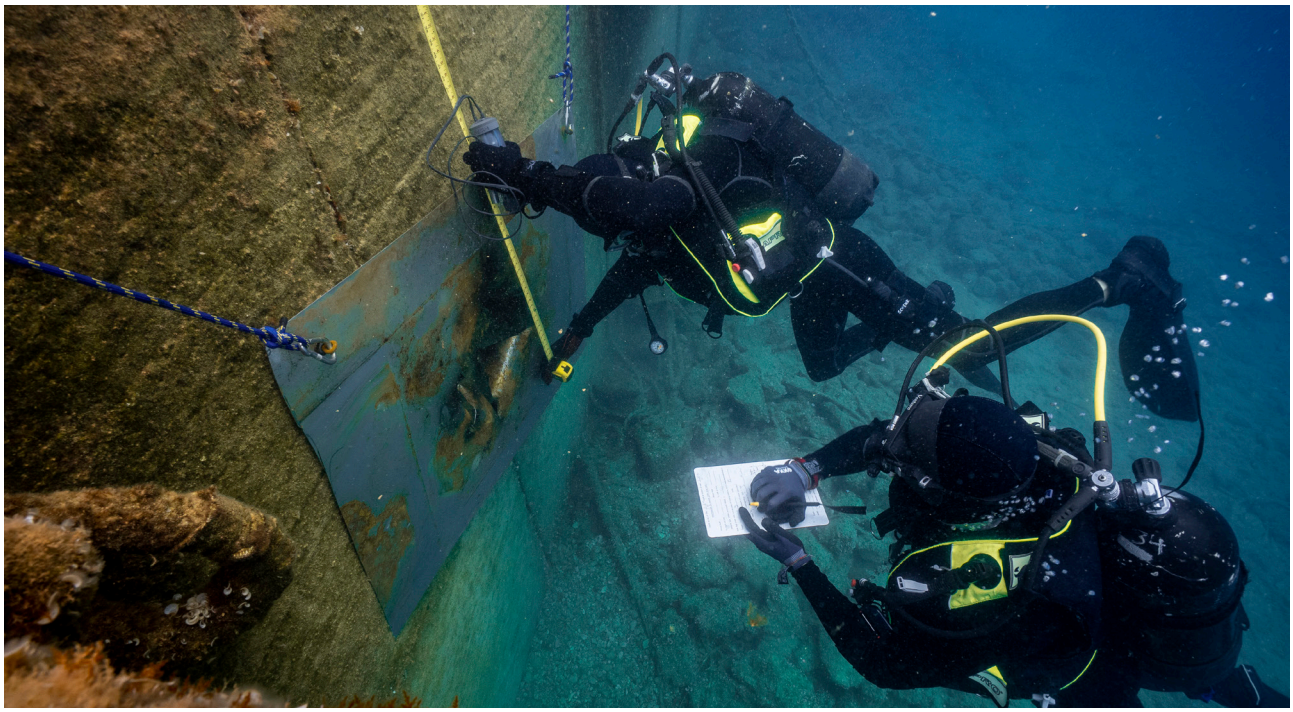
MTEP, ESPWG and EBUG-III conference hosted by NMIOTC

From 23 to 25th May 2023, NMIOTC hosted a conference of the NATO Military Training and Excercise Programme Planning Board (MTEP), the Environmental Protection Working Group (ESPWG) and the Exercise Budget Users Group Meeting (EBUG).

Underwater Post Blast Exploitation Course

An Underwater Post Blast Exploitation Training (UPX) was conducted from 8th to 12th of May, 2023 at NMIOTC training facilities.

Photo: Evan Possley



14th NMIOTC Annual Conference

From 7th to 8th June of 2023 the 14th NMIOTC Annual Conference titled: “Energy Security and the Maritime Interdiction; A road to pave in a complex Security Environment” took place at the NMIOTC premises. It was attended by more than 105 participants from 26 Nations, as representatives of National and International Organizations, academic community and from the shipping and defence industry.

17th Allied Cryptographic Task Force (ACTF) Meeting

From 12th to 15th of September 2023, the 17th Allied Cryptographic Task Force (ACTF) Meeting, led by Alliance Strategic Commands, took place at the NMIOTC premises. It was attended by 66 participants from 21 Allied Nations.

Course 25000 “Drafting, Production and Maintenance of NATO Standards”

From 12th to 16th of June 2023, and also from 2nd to 6th of October 2023, the Resident Course 25000 “Drafting Production and Maintenance of NATO Standards”, was conducted at the NMIOTC premises.

Course 5000 “Maritime Operational Terminology Course”

From 11th to 22nd of September 2023, the NMIOTC Maritime Operational Terminology Course (MOTC) was conducted at NMIOTC premises with the support of NATO Allied Command Transformation and USNR.

Courses 2000 & 3000 “Boarding Team Theoretical & Practical Issues”

From 18th to 29th of September 2023 the Resident Course 2000 “Boarding Team Theoretical Issues” and 3000 “Boarding Team Practical Issues” were conducted in tandem at NMIOTC premises.

7th NMIOTC Cyber Security Conference

From 27th to 28th September 2023, the 7th NMIOTC Conference on Cyber Security in Maritime Domain took place at the NMIOTC premises. One of the major annual events organized by NMIOTC, the conference was attended by 124 participants from 23 Allied and Partner Nations, coming from military and civilian establishments, representing International Organizations, academic community, shipping and defense industry.

Course 21000 “Medical Combat Care in Maritime Operations”

From the 30th October to 10th of November 2023, the Resident Course 21000 “Medical Combat Care in Maritime Operations” was conducted at the NMIOTC’s premises

NATO Exercise Programme Alignment Conference (NEPAC 23)

From 28th to 30th of November 2023, the autumn iteration of NATO Exercise Programme Alignment Conference (NEPAC) took place at the NMIOTC premises. It was attended by 108 participants from most of the Allied Nations.

SNMG-2 in NMIOTC

From 25th of October to 28th of November 2023, NMIOTC provided at a very short notice, a full C2 capability to the Commander and staff of Standing NATO Maritime Group – 2 (SNMG2). The utilization of NMIOTC as a Maritime Operations Center (MOC) in support of C2 for a NATO Maritime Task Group (SNMG2), demonstrated its capacity/capability to act not only as a NATO Education and Training Facility (NETF), but also as an Operational Center in a multipurpose role.

Chania Fire Brigade TCCC Training

From 20th to 24th of November 2023, a Team from Chania Fire Brigade received Tactical Combat Casualty Care (TCCC) training at NMIOTC's premises.

Training a Boarding Team from Georgia in terms of tactical movement in MIO framework.
Septemver 11-15, 2023

Members of the Philippine Navy's Special Operations Forces excercising on the containers Stack. Training in tactical movement in the framework of MIO.
29 Aug - 29 Sep 23

A team from Chania Fire Brigade receiving Tactical Combat Casualty Care (TCCC) training at NMIOTC's premises
November 20-24, 2023

NMIOTC Mobile Education & Training Team in Mauritania.
December 11-15, 2023

Visit of the EUNAVFOR MED Operation IRINI Force Commander, Rear Admiral Stefano Turchetto (ITA)
March 3, 2023

Visit of the 98th NATO Naval Forces Sensor and Weapons Accuracy Check Sites (FORACS) Steering Committee
May 17, 2023

Visit of the Commander Fleet Operational Sea Training (FOST), Commodore Andrew J. Canale Royal Navy (RN)
March 23, 2023

Visit by a delegation of the American Hellenic Institute
June 23, 2023

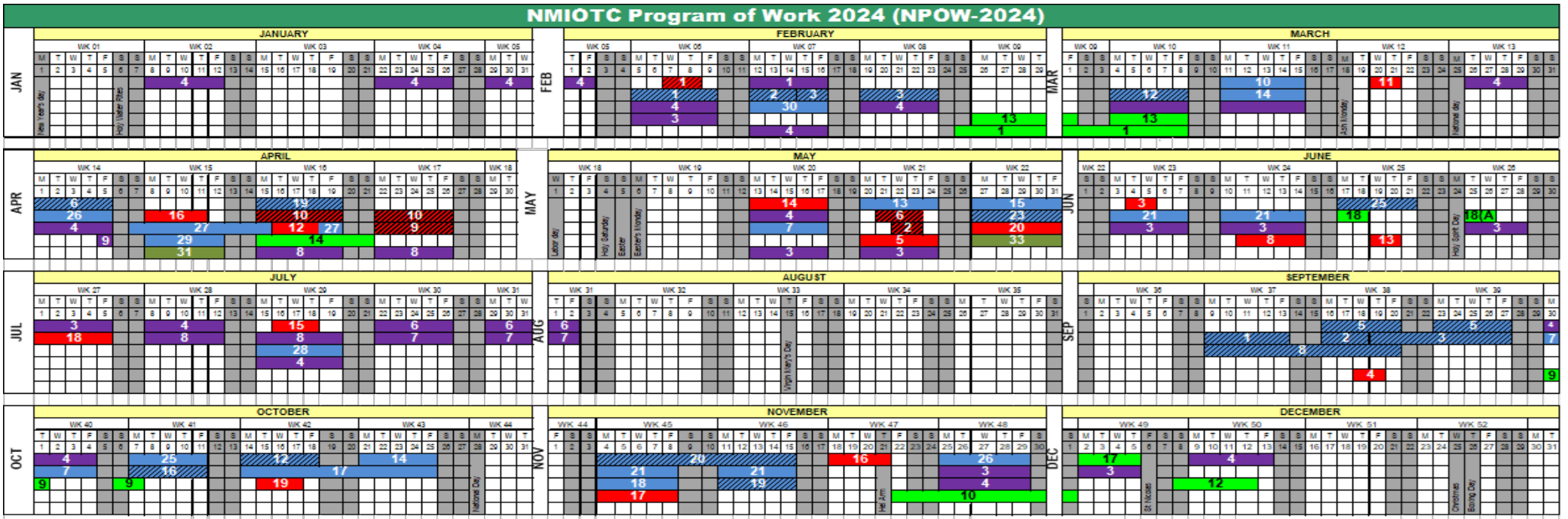
Visit of U.S. Congressional Delegation (CODEL), headed by Senator Jerry Moran (R-Kan.) and U.S. Ambassador to the Hellenic Republic, H.E. George J. Tsunis, hosted by the Deputy Chief of the Hellenic National Defence General Staff, Vice Admiral Frangiskos Leloudas. CODEL consisted also of Senators John Boozman, Katie Britt, Kristen Gillibrand, Bill Cassidy and Congressman Robert Aderholt.
July 5, 2023

Visit of the Standing NATO Maritime Group - 2 (SNMG2) Commander, Commodore Paul Stroude (RN)
November 31, 2023

Visit by 33 Engineer Regiment of the British Army's Royal Engineers
September 7, 2023

Visit of the Defence Attaché of the United Kingdom to Athens Captain Alex Bush RN
September 29, 2023

NMIOTC Program of Work 2024 (NPOW-2024)



COURSES (ETOC ID.)

1	Course 1000 - Command Team MIO Issues (MOP-MO-31201)
2	Course 2000 - Boarding Team Theoritical Issues (MOP-MO-21203)
3	Course 3000 - Boarding Team Practical Issues (MOP-MO-31205)
4	Course 4000 - MIO Final Tactical Exercise (MOP-MO-31207)
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 CCS (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)
24	Course 24000 - Building Up Interoperable Capabilities in support of MIO
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)
30	Course 30000 - NATO Identity Intelligence Analyst in a Complex Environment Course (INT-AS-36904)
31	Course 31000 - Harbor Protection and Its Relation to Maritime Interdiction Operations
32	Course 32000 - Maritime Interdiction Operations in Maritime Oil and Gas Assets
33	Course 33000 - Counter Terrorism at Sea with MIO

EVENTS

1	NAB (NMIOTC)
2	NCB (HNGS/ACT)
3	NMIOTC Annual Conference
4	NMIOTC Cyber Security Conference
5	UPX Training
6	Cyber Operations Annual Discipline Conference
7	Cyber Gordian Knot (TBD)
8	JCBRDN
9	NSHQ SOMTG HOSTED pilot COURSE
10	NSHQ SOMTU HOSTED pilot COURSE
11	Defence Policy Director Meeting (GRC-AUT)
12	Multinational Solutions Conference
13	3rd IAMD COE's Annual Conference
14	NOSP 24 - MPC
15	JALLC Lessons learned Training
16	IAMD COE CET-P
17	MIO SEMINAR FOR MAURITANIA
18	MCMSB
19	NATO M&S COE Annual Conference (TBC)
20	NATO Maritime Ops Law Course 2024

EXERCISES / METTs

1	CUTLASS EXPRESS METT (TBC)
2	SEA SHIELD METT (TBD)
3	ADRION METT (TBD)
4	SEA BREEZE METT (TBD)
5	BREEZE METT (TBD)
6	Exercise MARSEC (TBD)
7	NORTHERN SPIRIT (TBD)
8	PHOENIX EXPRESS METT (TBD)
9	OSG FOCOPS METT (TBC)
10	NIRIIS (TBC)
11	DYNAMIC MESSENGER (TBD)
12	NIRC (TBC)
13	ARIADNI (TBC)
14	SEA SHIELD (TBC)
15	NOBLE DINA (TBD)
16	NEMO TRIALS (TBD)
17	MAURITANIA METT (TBC)
18	ADRION 24 CAX (TBC)

TAILORED TRAININGS

1	DETRA TT
2	HCG Teams (TLCC)
3	DEU Teams
4	GRC Teams
5	GRC Naval Units
6	UK Cadets TT
7	USMC+SWE TT
8	MRT Teams
9	BNS F931 BT TT

► **Updated 10 Jan 2024**

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: https://nmiotc.nato.int/