Issue 24
2022
ISSN: 2241-438X

NMIOTC

Maritime Interdiction Operations Journal

NATO OTAN

NATO
OTAN

NMIOTC/ΚΕΝΑΠ

NATO
Maritime Interdiction Operational Training Centre

SAVE THE DATES

14th NMIOTC Annual Conference
7 - 8 June 2023

7th Conference on Cyber Security in the Maritime Domain
27 - 28 September 2023

CONTENTS

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Commodore Ch. Thymis GRC (N)
Commandant NMIOTC

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

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

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

Cover Photo: Lt I. Giannelis GRC (N)

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

NMIOTC
Commandant's Editorial

By its very nature, maritime environment offers abundant freedom to seafarers, being at the same time very vulnerable to activities threatening the security of Nations and the free flow of world commerce. Terrorist movements or support to them, human trafficking, smuggling, piracy and the proliferation of Weapons of Mass Destruction are just few examples of illicit activities that may be conducted from or through the sea.

Furthermore, NATO and International Maritime Organizations are facing rapidly evolving Cyber Security challenges and threats by a globally complex and diverse network of malicious actors.

NMIOTC core aim and endeavors, as the only NATO Quality Assured Educational & Training Facility, dedicated in training and research in the maritime domain, correspond to the needs of the Alliance to enhance both capabilities and awareness in maritime security, as well as to build bridges and establish common understanding among allied and partner nations, the academia and the private sector, in all matters within the broad maritime security spectrum.

Being aligned with the Alliance's concept of Deterrence and Defence of the Euro-Atlantic area, and considering the current global situation, with specific reference to the evolving crisis around the Mediterranean Sea and in the NATO's area of influence, drove us to choose the threat from Terrorism as the central theme for the 13th NMIOTC Annual Conference, during June 22.

Terrorist attacks to maritime targets are fortunately rare compared to other domains. It is almost clear that the intention to carry out attack at sea is strongly present in terrorist groups' mind and the opportunities are available at any time. At the same time, the sea is exploited for financial purposes by terrorist organizations, raising money from illicit trafficking, smugglings and through piracy/armed robbery, either by hijacking ships or robbing crews.

Human trafficking needs a special mention for its possible exploitation for financial purposes as well as for moving elements or terrorist cells from one country to another concealed as migrants.

Despite the rate, the impact that a terrorist attack in maritime domain has the devastating potential to hamper the maritime traffic, and, with it, the global market. or, in a possible worse case, to pose a threat to the life of hundreds of people, as happened on board the cruise ship Achille Lauro in 1985.

The role of the governmental agencies, along with the Navies' maritime interdiction has a key role in deterring and defending against maritime terror-

ism. To prevent terrorist threat and to increase resilience to acts of terrorism, the Alliance focuses on shared awareness of the threat, engagement with partner countries and other international actors, and developing capabilities to prepare and respond to current and future threats.

On the other hand, the impact of cyber security incidents on the conduct of future Maritime Operations may be catastrophic. Maritime operations are conducted by technology-intensive platforms, which today rely heavily on information systems. These dependences that Navies possess on information technologies will eventually affect their ability to maintain security at sea.

Therefore, during the 6th NMIOTC Conference on Cyber Security in the Maritime Domain in September 22, we stretched that Cyber has undeniably been a significant factor having changed our world. Countering Hybrid Cyber threats calls for a holistic and collaborative approach but also with the ability to join the dots between seemingly separate, but effectively interconnected events.

Cyber 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.

Bringing all this to our domain of expertise, the Maritime domain, I would like to emphasize that Maritime Operations are conducted by technology-intensive platforms, which today rely heavily on information systems and that the impact of Cyber Security incidents on the conduct of current and future Maritime Operations could be devastating. We should therefore realize that Cyberspace Operations capabilities are a critical enabler of success across all missions, and ensure that these capabilities are leveraged by commanders and decision-makers at all levels, and that in order to operate effectively, we must develop and constantly update a diverse set of Cyber capabilities and authorities.

The current ongoing conflicts have proved that Cyberspace can be used by state-sponsored and activist groups for disinformation and organized propaganda. A common practice also at the first stages of conflicts or during crisis periods is the disruption and vandalism of public services and accessible services to the citizens including bank services, satellite communications, and access to information via mostly Denial of Service Attacks (DDoS).

Furthermore, the use of ransomware and destructive malware are common tools to paralyze IT infrastructure and services in both public and private organizations like NonPetya (2017), WisperGate and Industroyer2 (2022) malwares. Targets could be energy pipelines, electric grid networks, hospital IT infrastructure, water purification facilities. A major also consideration is that these attacks can have such a cyber-physical effect that can lead to a potential escalation beyond cyberspace to a more widespread confrontation between nations.

Finally, allow me to highlight that our upcoming 14th NMIOTC Annual Conference 2023 next June, will give us the opportunity for discussions and exchange of ideas, among the International Maritime Community, on Energy Security challenges in the Maritime Domain. The ongoing conflicts shows that Energy Security and, in broader terms, the protection of Critical Infrastructures has become a major and growing challenge for NATO and Maritime Interdiction Operations (MIO) could have an important role in countering all these challenges.

Charalampos Thymis
Commodore GRC (N)
Commandant NMIOTC

NMIOTC
13th Annual Conference, 2022

by Dinos Kerigan-Kyrou

The 13th NMIOTC Annual Conference brought together a diverse, highly knowledgeable, and hugely influential group of expert speakers and panellists. Representatives from the military, academia, business, national governments, NATO, European Union, and Partner Nations from across the world discussed and analysed the critical issue of terrorism in the maritime domain.

Terrorism Threats are Broad - We Need to Adapt

From the very start of the conference, there was an emphasis that terrorist threats in the maritime environment are not new. Commodore Thymis, NMIOTC Commandant, Hellenic Navy, highlighted the example of the 1985 hijacking of the Achille Lauro cruise ship, resulting in the murder of a defenceless civilian by terrorists. As Commodore Thymis made clear what has changed in the decades since this horrendous event is the nature and scope of terrorism in the maritime environment. Moreover, as these challenges develop it becomes increasingly critical for all NATO, EU and Partner Nation stakeholders to advance a common understanding and approach to new and emerging threat actors.

This view was reinforced by Vice Admiral Drimousis, Deputy Chief HNDGS (Hellenic National Defence General Staff), stressing the broader threats we face in maritime security. He particularly emphasised piracy, human trafficking, and terrorism. VAdm Drimousis made clear that NATO must develop and adapt to the growing threat of maritime terrorism.

This theme of adaptability was continued by VAdm Keith Blount, Commander of NATO Maritime Command. The illegal and appalling invasion of Ukraine has accelerated change within NATO, invalidating much of the previous thinking. Moreover, terrorists within and beyond the maritime domain can exploit the current situation. We need to outmatch our adversaries, by 'joining the blue dots' of maritime security challenges. We must continue to maintain pressure, think carefully about what deterrence means, and be more aware of NATO's overall maritime security objectives.

Similarly, Rear Adm. Mihai Panait, Commander of Romanian Naval Forces, affirmed that we need to learn from the Ukraine conflict. He emphasised the importance of Critical Infrastructure security, and advocated the expanded use of unmanned autonomous air systems to counter NATO's maritime challenges. They key to collaboration is enabling modern capabilities to meet current operational commitments and protecting maritime critical infrastructure. RAdm Panait also highlighted the superb work that Romania is undertaking supporting Ukrainian refugees fleeing the conflict zones.

Dr Wendin Smith (Director of NATO's Arms Control, Disarmament and Weapons of Mass Destruction Non-proliferation Centre) highlighted the need to adapt and evolve

by embracing developing technologies. She stressed that there is a real threat within the maritime environment of adversaries sourcing components to create a WMD (Weapon of Mass Destruction). For instance, chemical weapons have been used many times over the past five years by terrorists and by hostile states for assassinations. Almost all of these components were shipped by sea. Fortunately, 'data fusion', which comprises smart analysis of mass or 'meta' data' that is mostly open source, is helping Allies and Partners to identify shipping anomalies at an early stage. This is well before the WMD has been transported and made into a usable device. Dr Smith stressed that we need an integrated approach, working with both private industry and academia.

Brigadier General Bart Laurent, Director of the Operations of the European Union Military Staff, described the very broad scope of EU maritime security operations in terms of both geography and strategy. The EU is currently running four Training Missions and three Operations, including coordinated maritime operation in the NW Indian Ocean. Gen Laurent emphasised the real and continuing threat of multifaceted terrorism, stressing that cooperation to combat terrorism is critical. The new Counterterrorism (CT) Agenda for the EU will take forward a holistic approach to CT. It will directly connect activities that fund terrorist activities such as radicalisation and the illicit people trafficking.

Maritime Security is Interlinked and Connected to *All* Security

This panel was moderated by Dr. Nikitas Nikitakos (University of the Aegean), with Professor James Bergeron (NATO Allied Maritime Command), Capt Efstathios Kyriakidis (EU Military Staff), and Lauren Dagan (Haifa University). The panel emphasised that maritime security is linked to all security challenges, notably the rise in proxy warfare and the increase in grey zone / hybrid activity. Hostile states are orchestrating direct attacks to our shipping, therefore we need to broaden our understanding of the scope of the maritime threat environment. We may need to start looking at new and emerging models of 'terrorism at sea'. Terrorism should be redefined to include its crossover with organised crime.

Deterrence and defence are key parts of the EU's crisis response and naval diplomacy. The EU is focussing on countering hybrid threats including human trafficking, energy security and illicit hydrocarbons smuggling, illegal archaeological research and artefact trafficking, and wildlife trafficking. These activities fund terrorism and use cyberspace and the maritime environment as enablers. This 'grey zone', the cross between Peace and War, is largely executed within the maritime environment. Although the challenges are new, some of the effective approaches we can adopt have been used for over a100 years. US President Theodore Roosevelt was quoted as saying: "A good navy is not a provocation to war. It is the surest guaranty of peace."

Maritime Threats Have Not Ended But Are Changing

This panel was moderated by Iosif Progoulakis (Fulbright Scholar), featuring Cdr Giovanni Modugno (Italian Navy Divers Group), Cdr Konstantinos Raptis (Hellenic Navy, NMIOTC), and Lt Col Nikolaos Balis (Hellenic Army, NMIOTC). The panel stressed that threats are changing, not ending. A particular example is the common misconception that maritime piracy has ceased, yet piracy in the

Gulf of Guinea continues to threaten maritime security for the global shipping community.
In the Mediterranean the situation surrounding Libya presents challenges including irregular migration, trafficking, and suspect vessels. The Gulf of Aden and the Strait of Hormuz continue to harbour huge security challenges. New threats continue to develop both at sea and in our ports and increasingly include waterborne WMD, bomb attacks on ships, and deliberate boat-to-boat collisions. LNG (Liquefied Natural Gas) ships are an increasing considered as targets by nefarious actors. Moreover, regular container vessels are being used to transport explosives. Of particular concern is the transport of CBRNE (Chemical, Biological, Radiological, Nuclear, and Explosive) material.
The Maritime security environment is vast and also incorporates the adjacent land and air domains. Threats include organized crime, terrorism, piracy, mines, IED (Improvised Explosive Devices), and smuggling. Developing our response is becoming more technically complex. For example, detecting mines and IEDs in the maritime environment is increasingly difficult as many IEDs no longer contain metal parts that can be easily identified. Indeed, IEDs targeted at ports is developing into an increasing and very significant area of concern.
While the threats from wicked actors are changing, the legal framework concerning our response as Allies and Partners to these challenges is unclear and in need of development.
From a legal perspective, the basis allowing for counter terrorism maritime interdiction operations was presented. The legal framework governing MIO falls within general International Law, Mandates and Agreements and forming an international treaty-based collective security system. These treaties aim to address current and future maritime threats, while considering international human rights law and a sovereign states' rights at sea.

Combatting Maritime Terrorism - Including Countering WMD and Illicit Trafficking - Requires Capacity Building

Lt Col Wendi O. Brown (US Army Reserve) moderated the session, featuring Siri Bjune (United Nations Office on Drugs and Crime), and Kevin Duffy (Maritime Security Consultant, US Coast Guard, Ret.). The panel strongly advocated the importance of capacity building. The panellists emphasised that terrorism threats in the maritime domain present a vast danger to global peace, and keeping oceans open for the transportation of the critical goods is needed. The maritime environment enables illicit trade at sea which financially supports terrorist groups.
To counter these threats, maritime law and cross-agency coordination needs to be further developed. Of critical importance is internationally coordinated education. NATO ADL (Advanced Distributed Learning) for Partners and Allies was mentioned as a particular response to enable this training and education to occur. The panel concluded with a quote from Ghada Waly, Director of the UN Office on Drugs and Crime: "Criminals, pirates and terrorists exploit poverty. To counter threats, we need to raise awareness and provide alternatives".

Technological Superiority is a Game Changer in Counter-Terrorism - We Need to be Smart in Adapting to the New Technological Maritime Environment

The session was moderated by Dinos Kerigan-Kyrou featuring Dr. Adam Fenton (Coventry University), Dr. Nikitakos, and Matthew Searle (Maritime Arresting Technologies). The panel examined how technology can transform the whole maritime environment. The technology could be Unmanned Water Vehicles, blockchain, autonomous shipping, or the development of Quantum computing. The panel looked at the threats these technologies pose when in the wrong hands and advantages these same technolo-

gies can give to Allies and Partners.
The panel also looked at the problems and challenges faced by Allies and Partners when developing these technologies, including the technical and logistical barriers that need to be overcome. How the strategic landscape changes markedly for NATO, the EU and Partner Nations as the technological landscape continues to transform was explored.

Protecting Maritime Critical Infrastructure Requires Information Sharing and Moving Away from Siloed Thinking

The panel was moderated by Lt Col Brown, featuring David Nordell (Haifa University), Dr. Kristen Kuhn (Institute for Peace and Security, Coventry University), Lt Cdr Stefano Canarutto (Italian Navy General Staff), and Dimitrios Souxes (Maritime Security, INTERPOL). The panel identified that one of the key challenges in the maritime environment is continual 'low intensity', 'grey zone' warfare. This constant pressure, which may not manifest itself as an actual kinetic conflict, presents a significant and continual risk for ports, vessels and critical infrastructure. These challenges present a continuous and essential need for holistic maritime security. Law enforcement and security requires countries and all stakeholders to learn from one another (including strategic and operational threats, lessons learnt, best practise), and to broadly share information. There is a clear need to move beyond the hoarding of information within silos (the traditional way of utilizing information pre 9/11) and moving toward information sharing networks. Without a new approach to information sharing, and thinking 'holistically', these new and developing challenges within the maritime environment cannot be addressed effectively.

Utilising Innovative Technology for the Benefit of NATO, the EU and Partners Requires Thinking Creatively and Differently about Maritime Security

This panel was moderated by Dr. Nikitakos, and featuring Iosif Progoulakis, US Navy CAPT (ret.) Edward Lundquist (Surface Navy Association), and Dr. Stavros Pissadakis (Foundation for Research and Technology Hellas). The panel agreed that a new framework is needed for the protection of maritime security. Innovation is required to reduce risks, especially dangers to 'soft' targets such as cruise ships. New mitigation measures are needed soon, utilising the private sector and the wealth of developing technologies that is becoming available.

Conclusions and Summary

The speakers, panellists, and all contributors to the 13th NMIOTC Annual Conference stressed throughout the event that maritime security challenges caused by terrorists and hostile states are transforming the maritime strategic landscape. The maritime environment is not only a target for nefarious actors' activities. It is, in itself, an enabler for these hostile actions, regardless of whether they predominantly occur at sea, on land, in the air, space, or indeed cyberspace.
While the threats are changing and multiplying, our responses to these challenges and our ability to work together across NATO, the European Union, and with global Partner Nations must adapt to this new maritime security environment. Failure to do so may lead to success for those who wish us harm. Adapting and working together, particularly by the breaking down of traditional barriers, gives us a chance to both minimise the frequency of terrorist and hostile actors operating within the maritime environment, and also to lessen the impact of their activities when these incidents do occur.
The 13th NMIOTC Annual Conference provided a unique, insightful, and highly creative perspective on the new and emerging maritime security challenges we face.

Dinos Kerigan-Kyrou PhD CMILT
Dinos is a Senior Lecturer at Abertay University's Division of Cybersecurity. He coordinates the cybersecurity and hybrid threats education within the Irish Defence Forces Joint Command & Staff Course. Dinos is a NATO Defence Education Enhancement Programme (NATO DEEP), instructor and a military educational advisor at the Partnership for Peace Consortium of Defense Academies (PfPC), based at US Army Garrison Bavaria. He is a co-author of the NATO/PfPC Cybersecurity Reference Curriculum and the new Hybrid War and Hybrid Threats Reference Curriculum. He is a member of the Advanced Distributed Learning (ADL) Working Group developing blended and hybrid learning for NATO and Partner Nations.

Plan, Organize, Defeat: Multilateral Maritime Counterterrorism Operations

by Kevin Duffy

The management and execution of maritime counterterrorism activities are core functions and concerns for all coastal states. Likewise, while the specific nature of threats and actors may differ across regions and eras, the unique nature of the maritime environment will always mean that the states charged with designing and planning responses to specific cases of terrorist threats or actions at sea will actually face a remarkably consistent set of challenges. Such common challenges will moreover be persistently present because maritime counterterrorism missions and operations will often be planned and executed by (in a lead or supporting role) a multinational coalition. This is because the high seas exist beyond national boundaries and sovereign territories (and the authorities and jurisdictions conferred and recognized therein), meaning that responses to threats emanating therefrom will necessarily involve similar types of international cooperation to track suspect vessels, share information and intelligence, and ultimately to interdict targeted actors.

For this reason, the application of the Maritime Imperative model for multinational approaches to coordinating regional maritime security activities can be particularly useful for the counterterrorism mission set. Specifically, and as explained in previous publications, this model outlines four standard considerations for planning and designing multinational maritime security operations and mechanisms:

- Defining the sea space, both physically and politically: are there converging territorial seas, or are only high seas involved? Are there maritime straits, choke points, or other particular risk areas?
- Defining the actors: what are the relative levels of willingness and capabilities of various partners and the potential roles of external stakeholders? What is the nature of the adversary and their level of capability? What type of terrorist act do they intend to carry out (e.g. deliver weapons, attack directly, kidnap, targeted assassination, or indiscriminate mass killing)?
- Defining the mission/purpose: is it merely to share information, to fuse intelligence, or to provide awareness? How much information or intelligence are participants willing to share with the broader coalition? If the mission is actually to conduct operations, are participating forces highly focused on and permitted to conduct only certain missions, or will there be a broader mandate?
- Defining the extent of centralized control: is there a command and control function envisioned? How much

directive authority are various participants willing to cede to the group? Will they be open to having their assets directed by a central command authority, or merely to a coordination process that provides the information needed for them to make their own decisions?

As stated, the answers to these questions should drive how any given multinational maritime security mechanism is designed and managed. For a specifically counterterrorism multilateral coordinating mechanism, planners and leaders would likely be facing the following realities:

The Sea Space being considered will depend upon the adversary's actions; in the case of an international terrorist group targeting waterborne or shoreline targets, or merely using maritime conveyance to arrive to a target area, for instance, one might well imagine a vessel transiting toward its target or delivery point; this would mean a transit across high seas and into territorial waters, with the chosen location for interdiction then driven by certain sea space factors, i.e. whether a location is particularly amenable to intercept given its geography. For instance, would interdiction within territorial waters be preferable for reasons of authorities and concentration of forces, or would farther offshore on the high seas be preferable due to the nature of the weapons and threats onboard?

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.

The Mission would be highly specific: to counter a single threat or threat type. The specificity and clarity of the mission, in fact, would necessarily drive some important legal, diplomatic, and political work before the mission even started; specifically, the relevant country or countries would need to prioritize the legal basis for their interdiction, understand their intentions for the disposition of seized individuals and property, and fully clarify, with necessary legal approvals, the rules of engagement or use of force policies to be employed by the interdicting team.

The Command and Control (C2) of the operation would also be fairly driven by the specifics of the circumstances, but one can easily envision that partner nations would engage in robust information and intelligence sharing as the scenario developed, with tightly-controlled C2 by the national authority of the interdicting force during the actual interception operation. Were there a broader coalition of actual forces on scene or in the interdiction area, clear authorities and roles established by coalition mandate would of course be required.

In conclusion, counterterrorism at sea is one of many mission sets that will have to be managed by existing command structures and entities at the national and multinational levels. Understanding how these structures can be tailored, or new structures created, to execute the missions at hand will remain an important component of mutual efforts to establish maritime security now and in the future. Coalitions like NATO are poised to lead the way in these efforts, and as such NATO bodies such as the Maritime Interdiction Operational Training Center, Maritime Security Center of Excellence, and NATO educational institutions should work together to devise and exercise various mission-based coordinating mechanisms that can be employed at sea in the future.

Robot Boats

Use of Autonomous 'Ships' in Law Enforcement, Terrorism and Counter-Terrorism[1]

by Adam James Fenton & Ioannis Chapsos

Introduction

Autonomous ships – that is ships that can observe, analyse, make decisions and navigate themselves to a destination – are now a reality. Norway's Yara Birkeland, a zero-emission autonomous cargo ship had its maiden voyage in November 2021[2] and began operations in Spring of 2022.[3] The US Navy has invested heavily in this area with a projected strategy to achieve up to "149 unmanned platforms in FY2045".[4] This investment in the future of artificially intelligent ships is largely driven by the rivalry with China in the Indo-Pacific region which some are already calling an "AI naval arms race".[5] China is also making advances in this area, recently launching the Zhu Hai Yun an 88-metre unmanned "drone carrier" capable of supporting "over 50" smaller autonomous craft. The significant benefits offered by autonomous ships – lower risk to humans, increased efficiency and expanded capabilities – will drive intense interest and use in the commercial and military sectors, but also by illegal groups such as transnational organised crime, pirate and terrorist groups. It is a rapidly developing area of interest in the maritime domain that raises a number of important technological, legal and ethical issues. As is often the case, law and ethics are lagging behind the technological advances. This article will give a general overview of current developments in autonomous ships and outline some of the legal issues raised, particularly the threshold question of whether autonomous vessels can, or should, be classified as "ships" under international law. It will argue that, in line with Moore's Law, as autonomous technology becomes cheaper and more prevalent, it will be taken up by both

[1] This research received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 101029232. This paper is based on a presentation to the NMIOTC Annual Conference on 8 June 2022.

[2] https://www.yara.com/corporate-releases/yara-to-start-operating-the-worlds-first-fully-emission-free-container-ship/

[3] https://www.yara.com/news-and-media/press-kits/yara-birkeland-press-kit/

[4] https://media.defense.gov/2022/Apr/20/2002980535/-1/-1/0/PB23%20SHIPBUILDING%20PLAN%2018%20APR%202022%20FINAL.PDF

[5] https://www.washingtonpost.com/technology/2022/04/14/navy-robot-ships/

legal and illegal groups due to the significant advantages that it offers. It will then provide some current examples of the uses of uncrewed ships by navies and terrorist groups, and conclude by looking at some possible future directions and responses.

What are autonomous ships and what are the advantages and disadvantages?

Several different typologies or systems for categorizing the levels of autonomy in ships have been offered by various authors, for example the IMO has a four-degree system (discussed below), Sheridan offers a 10-point scale,[6] and Danish Maritime Law Association has a six-point scale adapted from the Lloyd's Register.[7] What they all have in common is that they range across a spectrum from one end, which represents a fully manually-operated ship, (that is a 'traditional' ship where all the systems, navigation, engines, steering and so on, are done by human minds and hands). On the other end of the spectrum is a ship where all of those same systems and tasks are completed by autonomous computer-based systems, aided by an array of sensors, cameras, and software with radio and satellite communications. In between, where most ships today are found, is a mix of various levels of automated systems working in cooperation with humans. An autopilot for example is an automated system that is present on virtually all ships today. It can keep a ship on course automatically, however, it can be easily overridden by a human controller when necessary. Moving further across the spectrum toward uncrewed technology, a ship can be controlled from a remote location with a crew on board ready to take control if necessary – or it can be controlled remotely with no crew on board. In the ultimate case it can be fully autonomous and be remotely monitored from a Remote Control Centre (RCC). To summarise these various levels of automated operation the IMO's four degrees of Maritime Autonomous Surface Ship (MASS) are:

- Degree one: Ship with automated processes and decision support: Seafarers are on board ready to take control.
- Degree two: Remotely controlled ship with seafarers on board: Seafarers are available on board to take control.
- Degree three: Remotely controlled ship without seafarers on board: The ship is controlled and operated from another location. No seafarers on board.
- Degree four: Fully autonomous ship: The operating system of the ship is able to make decisions and determine actions by itself.[8]

What then are the benefits of autonomous ships and why is there so much interest in them? With up to 95% of accidents at sea due to human error[9], autonomous ships are potentially much safer than their crewed counterparts. Assuming the tech works well and autonomous ships, over time, prove themselves to be safer than crewed ships this would lead to lower insurance premiums. Removing crews from ships would lead to savings from salary costs, and potentially lower fuel costs. An AI-enabled ship with access to updated data for weather, traffic, tides, shipping hazards etc. may well be able to plot more efficient routes, thus saving time and fuel.[10] Some studies show that the savings could be in the millions of dollars per ship.[11] These cost benefits will drive serious interest from commercial shipping operations looking to minimise costs and maximise profits.

Autonomous ships offer a number of advantages to military operations as well including lower risk to human sailors and cost benefits. Removing human crews reduces political and diplomatic risks from the loss of human life, making autonomous ships more expendable, but also offering significant operational advantages. Uncrewed vessels can expand the operating horizon, offer support to larger vessels, increase their surveillance capabilities, and operate at sea far longer and without breaks than crewed vessels can. The US Navy for example is developing an "8000km-range, AI-enabled Medium Unmanned Surface Vessel (MUSV) which could cruise autonomously at sea for two months with a surveillance payload."[12] Uncrewed vessels may also offer a tactical advantage as stated by U.S. Vice Admiral Roy Kitchener, commander of Naval Surface Forces, "unmanned systems will increase decision speed and lethality for warfighting advantage".[13] It must be remembered that with increased reliance on networked computers, radio and satellite communications,

[6] https://www.bloomsburycollections.com/book/artificial-intelligence-and-autonomous-shipping-developing-the-international-legal-framework/ch1-international-regulation-of-shipping-and-unmanned-vessels?

[7] ibid

[8] www.imo.org

[9] https://www.agcs.allianz.com/news-and-insights/expert-risk-articles/human-error-shipping-safety.html

[10] Google researchers were surprised to see that AI-enabled balloons had learned how to tack into the wind because it was the most efficient way of reaching their target see: https://www.bbc.com/future/article/20210222-how-googles-hot-air-balloon-surprised-its-creators

[11] https://safety4sea.com/key-advantages-and-disadvantages-of-ship-autonomy/

[12] https://cimsec.org/winning-the-ai-enabled-war-at-sea/

[13] https://news.usni.org/2022/05/17/new-navy-unmanned-command-will-send-4-experimental-large-usvs-to-rimpac

sensors, cameras and other high-tech devices, all networked and interconnected, there are significant cyber vulnerabilities. These vulnerabilities must be acknowledged and the required safeguards built in and necessary training provided for staff and operators. This will be one of the most significant challenges as shipping shifts to autonomous systems, as well as safeguarding "Machine learning systems – the core of modern AI" from being hacked which, according to one commentator "are rife with vulnerabilities".[14] As AI in ships is taken up in both the commercial and military sectors, lives will depend on the technology being failsafe.

Legal issues - are they ships?

Some academic commentary exists in this area and raises a number of issues of importance to international shipping. The legal and ethical questions are many and complex. The many international shipping treaties, such as UNCLOS, COLREG, STCW, SOLAS, and MARPOL etc. were designed and written on the assumption that ships had Masters and crews. The required qualifications, practices, and procedures to be followed by ships are set out largely based on the responsibilities that they place on the Master and crew. How then are they to apply to a new generation of ships that will have no Master or crew on board? The questions are too numerous and complex to be fully considered in this article. However, one basic threshold question stands out, which is whether vessels without human crews should be granted the status of "ships" under international law at all? See for example: Soyer and Tettenborn (2021);[15] Allen (2018);[16] Mayank[17] (2020).

Throughout history our understanding of what defines a ship has been its ability to participate in international navigation and trade, its possession of a hull capable of transporting human crews and goods. Being granted the status of 'ship' grants the vessel a nationality, and a number of rights and responsibilities in international law; the right of innocent passage through the territorial seas of other states for example. It is questionable whether uncrewed vessels, particularly the smaller ones which are often used in scientific research, fulfil all, or any, of those criteria. So are they ships? This important threshold question remains unanswered in the academic literature and in international law.

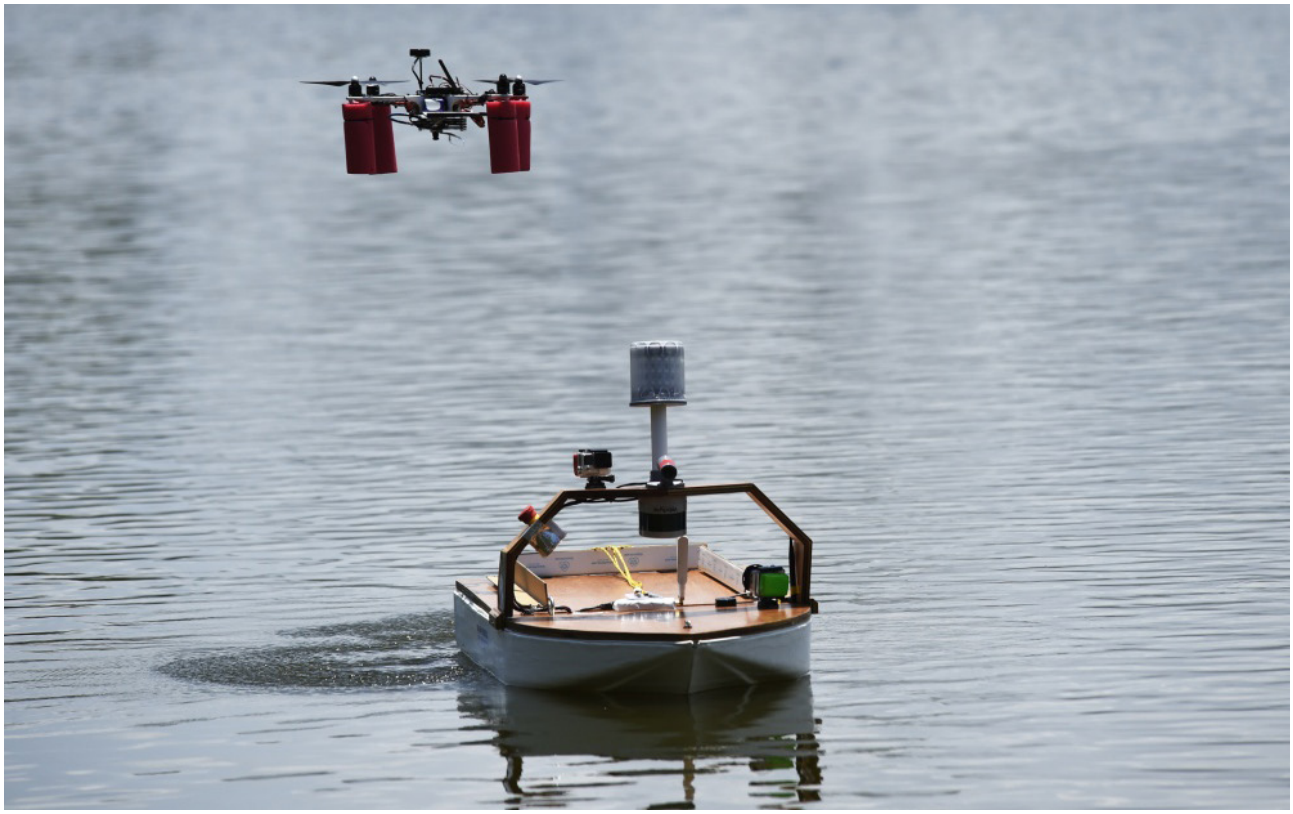
While lawyers ponder the question of defining autonomous 'ships' it is likely that in reality, at least some autonomous vessels will be categorised as 'ships' out of necessity. If we consider certain factors, firstly that UNCLOS does not contain a definition of 'ship' or 'vessel', rather by virtue of article 91 it mandates that "every State shall fix the conditions for the grant of its nationality to ships". And second, the reality of Open Registries or Flags of Convenience[18] – where some states have shown their willingness to play fast and loose with the rules in order to make a quick buck – it would seem that certain states will move ahead and classify MASS as ships if it serves their interests, and this can already be seen in some cases. The UK has registered its first autonomous ship under the Merchant Shipping Act and subject to some exceptions and legislative reform, there appear to be no significant legal barriers for uncrewed ships to operate in the UK.[19] It remains to be seen whether other coastal and port states will follow the example of the UK, or will refuse to categorise MASS as ships. The French Code des Transport (2017) for example appears to require that ships be "manned".[20]

With regard to warships, the issue is possibly even more complicated. UNCLOS does include a definition of a 'warship' at article 29:

For the purposes of this Convention, "warship" means a ship belonging to the armed forces of a State bearing the external marks distinguishing such ships of its nationality, under the command of an officer duly commissioned by the government of the State and whose name appears in the appropriate service list or its equivalent, and manned by a crew which is under regular armed forces discipline.[21]

It would seem clear as a matter of law that an uncrewed vessel cannot be legally categorised as a warship. However, the reality on the ground, or the ocean to be more specific, appears slightly different. When an uncrewed US Navy science vessel was illegally seized by the Chinese Navy in an incident in the hotly-contested South China Sea, the US responded by declaring that "the UUV (unmanned underwater vehicle) is a sovereign immune vessel of the United States. We call upon China to return our UUV immediately, and to comply with all of its obligations under international law."[22] Regardless of whether the vessel is legally defined as a warship or not,

[14] https://cset.georgetown.edu/publication/hacking-ai/
[15] https://www.bloomsbury.com/uk/artificial-intelligence-and-autonomous-shipping-9781509933358/
[16] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3244172
[17] https://www.researchgate.net/publication/347195243_Autonomous_vessels_as_ships_-_the_definition_conundrum
[18] https://www.imo.org/en/OurWork/Legal/Pages/Registration-of-ships-and-fraudulent-registration-matters.aspx
[19] https://www.bmla.org.uk/documents/2018/BMLA-Response-to-CMI-Questionnaire-on-Unmanned-Ships.pdf
[20] https://www.routledge.com/New-Technologies-Artificial-Intelligence-and-Shipping-Law-in-the-21st/Soyer-Tettenborn/p/book/9780367777920
[21] https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf. Emphasis added



it is clearly the position of the US that uncrewed vessels, even small 'gliders' such as this one, enjoy the rights and immunity of a sovereign ship.

Uses in counter-terrorism and terrorism

A number of navies are already using, or experimenting with, autonomous craft in their surveillance and enforcement operations. In March 2021, the Royal Navy's "experimentation innovator" NavyX took possession of the 'Madfox' (Maritime Demonstrator For Operational eXperimentation) Uncrewed Surface Vessel (USV) and began testing and exploring "a multitude of issues such as safety, regulatory compliance, new missions, new payloads and the role that a USV can play in complex operations and within the future fleet".[23] NavyX also announced plans for an autonomous RIB (Rigid Inflatable Boat).

The US Navy has an extensive program to incorporate USVs of different sizes into their operations including MUSVs (Medium Unmanned Surface Vessels), LUSVs (Large Unmanned Surface Vessels) and XLUSVs (Extra Large Unmanned Surface Vessels). A US Government Accountability Office report stated:

The Navy plans to introduce a number of uncrewed maritime systems into its fleet over the coming decades. While the Navy has previously operated some uncrewed systems including UUVs for missions such as oceanography and mine countermeasures, the Navy is currently developing a number of larger, more complex uncrewed systems. These include USVs—some approaching the size of a frigate or patrol ship—as well as UUVs—some approaching the size of small submarines. In addition to the vehicles, the Navy also needs to develop the software and digital infrastructure capabilities—such as data repositories and modeling and simulation—to operate these systems without a crew on board by developing artificial intelligence capabilities. While some of the software and other pieces will be unique to each vehicle, the Navy is planning for much of the digital infrastructure to be common to all of its major uncrewed maritime efforts.[24]

Israel is making significant technological advances in this area and has developed a number of autonomous vessel systems including the Elbit Seagull, a USV that can conduct surveillance and is capable of being armed with water cannons and firearms. The vessel's builder, Elbit, claims that its systems and sensors make it compliant with the COLREGs.[25] Also from Israel, Orca AI has made significant advances in the navigational capabilities of autonomous ships demonstrating a vessel that reportedly completed an "800km voyage without human assistance".[26]

The Royal Australian Navy has also made a significant

[22] https://www.un.org/depts/los/convention_agreements/texts/unclos/unclos_e.pdf. Emphasis added
[23] https://www.royalnavy.mod.uk/news-and-latest-activity/news/2021/march/26/210326-madfox-vessel
[24] https://www.gao.gov/products/gao-22-104567

commitment to incorporating autonomous vessels into its future operations out to 2040, with Vice Admiral Michael Noonan AO RAN declaring that "The race in autonomous warfare has already begun."[27] In January 2019, "Singapore, Japan, and South Korea announced their plans to use MAVs (Maritime Autonomous Vehicles) for activities such as surveillance, coastal border patrols, search and rescue, and mine detection".[28]

The advantages of autonomous vessels for navies are clear. They can operate at sea for extended periods without breaks in conditions that might be dangerous for humans. They can extend the surveillance capabilities for both land-based and sea-based operators. They can conduct surveillance, and if necessary, hot pursuit. While they cannot board a suspect vessel they could maintain an uninterrupted hot pursuit until a crewed vessel arrives to conduct a boarding. They can extend the capabilities of connected warships for example by extending the line of sight of a warship for a long range missile launch. Autonomous control also allows for maximum decentralization, expendability, freedom of design, and minimal operational costs (no crew or 24/7 operators required).[29]

The advantages that make autonomous and uncrewed vessels attractive to legal organisations such as navies and commercial ship operators will also make them attractive to illegal groups such as pirate, terrorist and transnational organised crime (TOC). TOC groups for example could use uncrewed vessels to transport illicit cargos such as drugs, weapons and trafficked people. There is a clear reduction of risk where no master or crew are on board to be arrested and interrogated by authorities. On the other hand, tech-savvy pirate and terrorist groups may develop their hacking skills to take control of autonomous vessels and use them for their own criminal ends.

The uptake of uncrewed technology for criminal attacks can already be seen with Houthi terrorist groups in Yemen having committed a number of 'suicide drone boat' attacks against international shipping.[30] These water-borne improvised explosive devices (WBIEDs) are reportedly 'surprisingly simple' to construct.[31] While these attacks have been committed using remotely controlled vessels from up to 80 miles away, it is not difficult to think that as autonomous software becomes more available it could be obtained and installed into the 'suicide drones' to extend the attack range much further. The added bonus of not having to sacrifice a trained and loyal member of their group will make this option even more attractive to terrorist organisations.

Looking ahead

Recalling the 9/11 Commission report[32] which warned that one of four failures revealed by the attacks was one of imagination, it is necessary to look ahead and ask in what new ways terrorists and criminals might use this emerging technology. New designs of drones are capable of "seamlessly transitioning between swimming and flying".[33] Such a drone would surely be of use to TOC and terrorist groups for transporting explosives or illicit packages undetected, underwater, through zones that are video monitored for example, then switching to flight mode for faster delivery. Bio-inspired suction allows drones to attach to a hull and 'hitch-hike' with a ship.[34] The advantages of this kind of tech to terror groups for limpet bombs is immediately apparent. Criminal groups could also attach payloads of illicit goods and hitch-hike below the waterline on an unsuspecting ship into a port. The drone could then detach and rendezvous with its controllers.

Aerial drones using interconnected artificial intelligence to create "swarms" with coordinated movement is emerging and provides new options for simultaneous coordinated attacks against single or multiple targets. In 2018, a swarm of 13 aerial drones attacked a Russian military base in Syria.[35] Pledger notes: "Terrorist groups have used or attempted to use aerial drones to conduct many different types of operations, including intelligence collection, explosive delivery (either by dropping explosives like a bomb, the vehicle operating as the impactor, or the drone having an equipped rocket-launching system of some type) and chemical weapon delivery…The number of non-state actors currently using aerial drones has increased each year."[36]

With the emergence of autonomous technology the range for an attack on a distant target will increase significantly. Aerial drones or surface vessels equipped with navigational AI will allow operators to set a geographical coordinate for the target and the drone will then navigate itself to the target whilst avoiding obstacles

[25] https://elbitsystems.com/pr-new/new-vision-and-analysis-capability-improves-autonomy-and-safety-of-elbit-systems-seagull-usv/
[26] https://youtu.be/M1BezS_2Jbs
[27] https://www.navy.gov.au/media-room/publications/ras-ai-strategy-2040
[28] https://www.hsdl.org/?abstract&did=829920
[29] https://georgetownsecuritystudiesreview.org/2020/10/28/the-future-for-unmanned-surface-vessels-in-the-us-navy/
[30] https://www.defensenews.com/digital-show-dailies/idex/2017/02/19/new-houthi-weapon-emerges-a-drone-boat/
[31] https://www.conflictarm.com/download-file/?report_id=2550&file_id=2564
[32] https://www.9-11commission.gov/report/911Report.pdf
[33] https://youtu.be/FC9EJhs0pc0
[34] https://www.imperial.ac.uk/news/236640/fish-inspired-drone-hitchhikes-flies-swims-using/

or traffic. The attribution for such an attack will also be difficult and opens up a variety of long-range targets such as port facilities, harbours, ammunition and fuel depots. Clearly an explosive drone attack on any of these types of facilities would cause major disruption to shipping.

In anticipating the possibility of these types of autonomous vessel attacks on shipping, it will be necessary for stakeholders such as navies and commercial shipping companies to develop robust defensive tactics. This may be difficult given that drone attacks could be sudden, unpredictable and could come from the sky, water surface or even underwater. Defences such as jamming and spoofing of the signal for remote controlled and autonomous craft may be possible but it requires specialist equipment and training and can be unreliable. Geofencing can be used to block GPS signals in particular areas but may be vulnerable to hacking. Other physical defences include nets and even trained birds or aquatic mammals.[37] More research is needed to identify and develop the most reliable defensive options for ships and ports.

Conclusion

New capabilities presented by artificial intelligence, algorithms, sensors and automated systems have led to significant advances in their incorporation into ships, thus allowing the unprecedented possibility for uncrewed ships to become a reality. The many advantages offered by such vessels will lead to their adoption by commercial shipping and navies and will enable a number of expanded capabilities and efficiencies. However, a greater reliance on such technology will also lead to vulnerabilities to being hacked, and pose a number of legal and ethical challenges which have not been fully addressed. Finally, the technology will no doubt be of use to illegal groups as well, and some indications of this are already being seen. Authorities will need to remain aware of the latest advances in tech, use them to their best advantage while ensuring that all necessary safeguards and training are in place; and remain vigilant to the ways that criminal groups will utilise emerging tech for their own nefarious goals.

Dr Adam Fenton

Assistant Professor Coventry University

Dr Adam James Fenton is a Marie Sklodowska-Curie Research Fellow at Coventry University's Centre for Trust, Peace and Social Relations. Prior to that, he worked as a Fisheries Officer in Foreign Compliance Operations based in Darwin, Australia; and as both a journalist and academic based in Jakarta, Indonesia for approximately 20 years. He has published in several international academic journals on terrorism, counter-terrorism, piracy and international law. His current research project STRAITSECURITY: Hybrid threats to Indonesia's Maritime Security, is an assessment of cyber and cyber-physical vulnerabilities in the Malacca Strait and received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Sklodowska-Curie grant agreement No 101029232.

Dr Ioannis Chapsos

Assistant Professor Research, Centre for Trust, Peace and Social Relations

Dr. Ioannis Chapsos is the Research Lead in Maritime Security at Coventry University's Centre for Trust, Peace and Social Relations (CTPSR). His research aims to better understand the land-sea nexus in the context of international security, feed into sustainable policy responses and build maritime security capacities wherever required. He is particularly interested in the increasing involvement of non-state actors in international security as victims, perpetrators and security providers, especially through a gender lens. His research interests also encompass the global trend of privatisation of maritime security and the potential implications in international security.

He has worked on a number of research projects where he explored the links between illegal (IUU) fishing and transnational organised maritime crime in the fishing industry (such as human trafficking/ modern slavery, forced labour, etc.) and the respective strategies, responses to challenges and threats, as well as their implications on coastal communities, particularly in SE Asia (Indonesia). His current research is focused on the role of gender in maritime security and the emerging cyber threats stemming from the technological advancements in the maritime domain.

Dr Chapsos is a Captain (ret) of the Hellenic Navy with more than 16 years of seagoing service and former lecturer on international security and strategy at the Hellenic Supreme Joint War College / Security and Strategy Department.

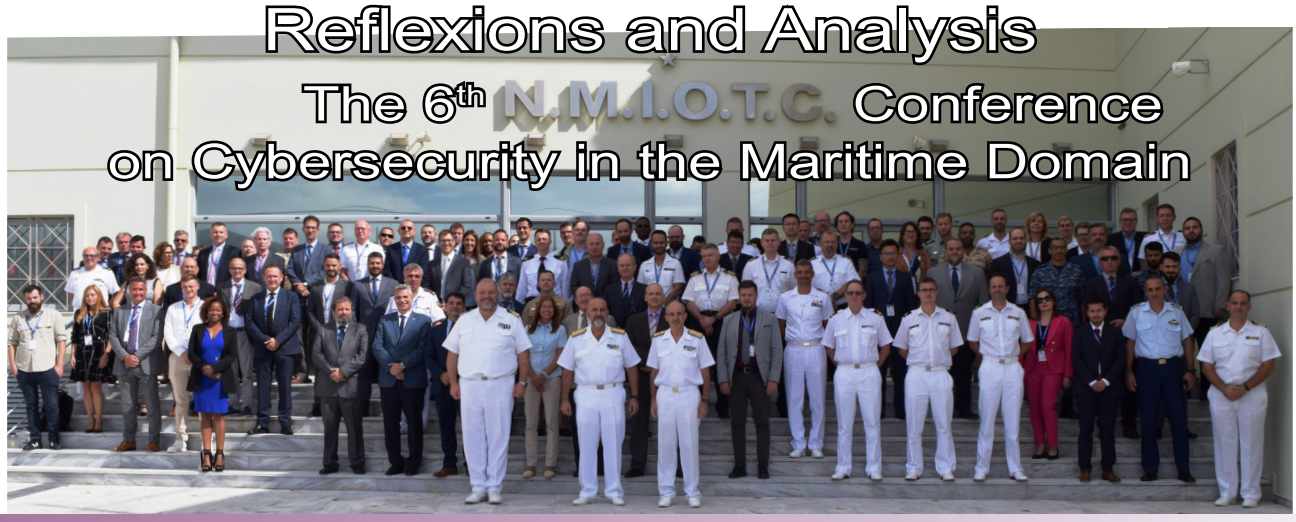
[35] https://www.ausa.org/sites/default/files/publications/LWP-137-The-Role-of-Drones-in-Future-Terrorist-Attacks_0.pdf

[36] Ibid

[37] Ibid

Reflexions and Analysis

The 6th N.M.I.O.T.C. Conference on Cybersecurity in the Maritime Domain



by Dinos Kerigan-Kyrou

The 6th NMIOTC Conference on cybersecurity built upon a key theme developing at NMIOTC over the past few years: Cybersecurity is now the central element of maritime security.

Cybersecurity is the security of Cyberspace – the online environment in which we all live and work. It is Cyberspace in which every part of the maritime industry operates, whether civilian or military. It is where we at NATO, the European Union, and Partner Nations develop our military capabilities and civilian opportunities. However, Cyberspace is also utilized by those who want to cause harm to us, our partners across the world, and those we seek to protect.

The keynote speakers at the conference encapsulated the challenges we face:

- Cyberspace is the enabler for all nefarious activity in the maritime domain.
- Cyberspace elevates the critical importance of stakeholders across economies, defence and security communities. The training of cybersecurity, needs to be greatly developed by all stakeholders.
- Information sharing needs to be greatly improved. The old ways of managing intelligence are no longer suitable for the cybersecurity challenges we face across the maritime community.

Cdre Charalampos Thymis emphasised that the maritime environment is the key enabler for the nefarious use of cyberspace. Hostile states, terrorists, criminals, and those who want to cause harm utilize cyberspace to plan and execute their actions within the maritime environment. Hostile states utilize cyberspace to plan and execute attacks on shipping, increasingly using drones in the air, on and below the water. Attacks on maritime critical infrastructure, especially hybrid 'deniable' attacks are becoming increasingly common.

Terrorists utilize cyberspace to plan and execute their atrocities. The 2000 al-Qaeda attack on the USS Cole was likely the first terrorist atrocity planned in cyberspace.

Criminals utilize cyberspace and the maritime environment to plan and operate piracy and maritime hijackings. Cyberspace is used for the planning of maritime smuggling including narcotics and wildlife. Human trafficking and forced human slavery is planned in cyberspace and carried out within the maritime environment. The profits from these horrendous illegal activities fund criminality, and, increasingly, terrorism. The distinction between terrorism, criminality, and hostile state activity in the maritime environment is becoming less and less clear.

VAdm Ioannis Drimousis of the Hellenic Defence General Staff stressed that digital transformation is now connected with every facet of modern life - economy, defence, and security. This presents new and emerging security challenges, including a requirement for better interaction and cooperation among all stakeholders. Moreover, cyber capabilities are now - and will remain indefinitely - critical for success across all maritime missions.

Dr. Athanasios Drougkas of the European Union Agency for Cybersecurity, ENISA, highlighted the importance of everyone understanding cyber risk, and the criticality of much better information sharing. This ability to share information is of particular importance across and beyond traditional organizational structures.

The panels at the conference examined a wide range of matters including technology, the cybersecurity of maritime supply chains, interaction with stakeholders, and maritime cybersecurity education.

Technology

The prospect of Quantum Computing, which may create computers millions of times faster than those we have today, was explored. Technology changes quickly and often without anyone noticing the change until it's happened. The panels and discussions agreed that it is critical to be aware that technological changes may take very unexpected directions. In order to plan for these rapid chang-

es, and to secure cyberspace in the maritime environment as effectively as possible, it is vital to capture and study the 'near miss' events. These are incidents which may not have caused a catastrophe, but could well have done. (For example, this is regularly undertaken across the aviation industry including the reporting of Air Proximity (AIRPROX) incidents where safety of 2 aircraft is compromised in the air). A clear example discussed in the panels of this type of cybersecurity compromise is GPS spoofing. Ships' navigation systems have been hacked on multiple occasions. In time there may well be a catastrophic event as a result of GPS spoofing, of deliberate radio interference. The critical importance of utilizing and understanding the security vulnerabilities of a whole new range of technologies, especially those concerning maritime logistics, was emphasised as central to progressing maritime cybersecurity. For example, developing a better understanding of the opportunities and security challenges of new satellite technology interconnected together across a vessel, creating an Internet of Things (IoT). These include power management, loading and stability systems, alarms, the bridge control console, electronic chart display and information system, navigation decision support, voyage data recorders, computerised automatic steering, global maritime distress and safety systems, and many other parts of a ship, all of which will be connected online.

Supply Chains

The panel, examining secure maritime supply chains and infrastructure, stressed how vital it is to look at security risk - especially cybersecurity risks - in a completely new way. It is important to document and address the challenges in the supply chain more effectively than we are doing at present. A supply chain has become the key route for a nefarious actor to gain access to a company or organisation and this equally applies in the maritime industry. It is critical to establish a far better audit and verification process within the maritime supply chain across NATO, EU, and global partners.

Stakeholders and Education

The security of our maritime environment and our critical infrastructure at sea depends upon developing and greatly improving stakeholder engagement and cybersecurity education for all. Moreover, the critical importance of moving beyond 'need to know' traditional notions of intelligence sharing are necessary to address the threats we face across cyberspace. As the 9/11 Commission Report correctly identified, the whole premise of traditional information sharing is based upon a flawed assumption. It is no longer possible to determine who 'needs to know' in this new asymmetric environment where hybrid threats proliferate our security challenges. The panel discussion highlighted the example of countering Russian disinformation during the illegal invasion of Ukraine. This disinformation directly leads to threats and challenges across the military environment, including at sea. The discussion underlined the critical importance of a holistic approach to cybersecurity. Superb progress has been made in cybersecurity education at NATO and the EU. Nonetheless, cybersecurity education remains an ongoing challenge. Traditional military education and university cybersecurity education sees cybersecurity as only a 'computing' issue. This approach to cybersecurity creates enormous threats for us all across the Alliance because it means we fail to understand the full range of threats across cyberspace. Indeed, US Admiral (ret'd) Michelle Howard has stated that everyone in the military is a cyber defender. Thankfully, by moving away from the outdated and dangerous notion that cybersecurity is only about computers, NATO and the European Union are doing tremendous work in addressing cybersecurity comprehensively.

Summary

Continual development, education and learning, and the realization we can always improve our cybersecurity in the maritime environment was a key emphasis of the conference.

The famous quote by the late US Defence Secretary, and naval officer, Donald Rumsfeld of being wary of 'Unknown Unknowns' was mentioned at the conference, summarising the uncertainties we face going forward in cyberspace. To address these uncertainties and 'unknown unknowns' it's clear we need to continually develop maritime cybersecurity holistically by understanding the whole security of cyberspace, engaging a broad range of stakeholders, and constantly improving and developing our cybersecurity education.

The 6th NMIOTC Conference on Cybersecurity in the Maritime Domain developed this holistic approach and has created an excellent framework going forward. It is crucial that this work continues.

Dinos Kerigan-Kyrou PhD CMILT

Dinos is a Senior Lecturer at Abertay University's Division of Cybersecurity. He coordinates the cybersecurity and hybrid threats education within the Irish Defence Forces Joint Command & Staff Course. Dinos is a NATO Defence Education Enhancement Programme (NATO DEEP), instructor and a military educational advisor at the Partnership for Peace Consortium of Defense Academies (PfPC), based at US Army Garrison Bavaria. He is a co-author of the NATO/PfPC Cybersecurity Reference Curriculum and the new Hybrid War and Hybrid Threats Reference Curriculum. He is a member of the Advanced Distributed Learning (ADL) Working Group developing blended and hybrid learning for NATO and Partner Nations.

The Technical Landscape of Ransomware: Threat Models and Defense Models

by Barton P. Miller and Elisa R. Heymann

1 Introduction

Ransomware has become a global problem, striking industry, academia and government alike. These attacks affect the smallest businesses, the largest corporations, and have even shut down IT operations at entire universities.[1,2] While there have been many papers describing the threats and risks associated with ransomware, in this paper we take a more technical approach. We start with a discussion of the basic attack goals of ransomware and distinguish ransomware from vandalism. Our goal is to present the broad landscape of how ransomware can affect a system and suggest how to prepare to recover from such an attack. We present a canonical model of a computing system, representing the key components of the system. This system model forms the basis of our discussion on specific attacks. We then use the system model to methodically discuss ways in which ransomware can (and sometimes cannot) attack each component of the system. For each attack scenario, we describe how the system might be subverted, the ransom act, the impact on operations, difficulty of accomplishing the attack, the cost to recover, and the ease of detection of the attack. We also describe strategies that could be used to recover from these attacks. In this paper we are focused on recovery not prevention. As such, we are not discussing how the ransomware might enter a computer system. The assumption is that the attacker did enter the system and rendered it inoperative. These attacks might result from a human engineering attack, an unpatched known vulnerability, or a zero-day vulnerability. Note that this document represents our best understanding of the current threats and attacks. We actively solicit corrections, feedback, and contributions to make this document more accurate, complete, and timely. Please send your comments to the authors.

2 Ransomware Attack Goals

Our focus in this document is on ransomware, that is software that causes payment to be extorted or some penalty to be imposed. These penalties can come in two varieties:

1. The contents of the computer system are modified, typically encrypted or deleted, so that the system becomes inoperative. This is done in a way that the attackers can restore the system to normal operations after a ransom payment is made.

2. Data from the computer system is exfiltrated. The attackers

[1] "El Govern destina 3,5 millones a la UAB para recuperarse del ciberataque" ("The Government allocates 3.5 million to the UAB to recover from the cyberattack"), La Vanguardia, November 23, 2021. https://www.lavanguardia.com/vida/20211123/7883348/govern-destina-3-5-millones-uabrecuperarse-ataque-informatico.html

[2] Scott Jaschik, "College Closes After 157 Years", https://www.google.com/url?q=https://www.insidehighered.com/news/2022/04/01/lincoln-collegeillinoisclose&sa=D&source=docs&ust=1657816248673164&usg=AOvVaw2Jbax20QvbjxCxMKVxUXR

demand a blackmail payment to prevent the data from being revealed to the public.

Attacks can combine the above two varieties. We identify four basic operations for malware:

(ENC) Encryption. This common operation encrypts some portion of the storage of the victim system, promising to reverse the encryption if payment is made.

(LOC) Lockout prevents the victim from accessing some system functionality. A lockout might involve an operation such as changing a password, creating a password where none previously existed , or modifying critical code such as the BIOS or firmware.

(EXF) Exfiltrating data provides the attacker with potentially private, proprietary, or sensitive data taken from the victim system. The attacker then blackmails the system owner by threatening to reveal the private information.

(DEL) Deleting data prevents some or all of the normal system operation. For this to be ransomware, and therefore reversible, it must be combined with exfiltration.

We noted that (ENC), (LOC), and (DEL) are attacks on availability and (EXF) is an attack on confidentiality. We distinguish between a ransom attack and plain vandalism. Vandalism is an attack for which there is no meaningful payment option. While there are some relevant similarities, in this paper we are not discussing vandalism.

Consider the NotPetya attack in 2018[3] on the global Maersk shipping company that wiped out the contents of the disks on the tens of thousands of computers on the Maersk corporate network. At first glance appeared to be ransomware, but it offered no functional payment option. NotPetya turned out to be malicious vandalism on a global scale.

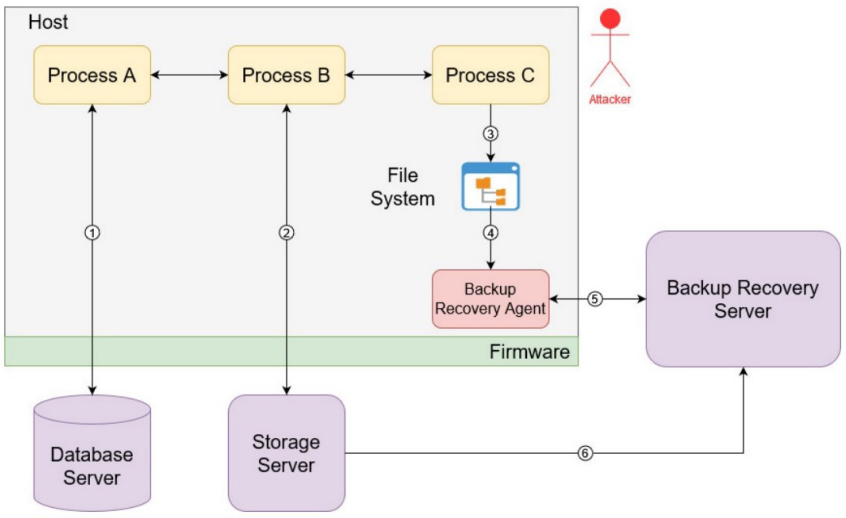


Figure 1: Canonical System

3 A Canonical System Model

We start with a model of the computer system that is being attacked, shown in Fig. 1. The goal of this model is to represent components of a system that might be attacked. The enclosing "Host" gray box represents a single computer system that is under attack. All components that are outside that box reside on different computer systems.

We start with three user processes, each of which is present to represent a different kind of attack.

Process A: User program accessing an external database service that might be in the local facility or remote.

Process B: User program accessing an external storage server (e.g., a file server or storage appliance) that might be in the local facility or remote.

Process C: User program accessing the local file system.

File System: Files that are stored on devices local to this host.

Backup Recovery Agent: Local service responsible for selecting files to back up and recover.

Backup Recovery Server: External service supporting the backup and recovery of files. It might be local or remote.

Database Server: External service running in the local facility or remotely, accepting queries from Process A.

Storage Server: External service running in the local facility or remotely, accepting file system requests from Process B.

Firmware: Semi-permanent software embedded in the devices associated with the host. These devices might include the motherboard (BIOS/UEFI and boot code), hard drives, or network card.

We illustrate both the components of the system and interaction of the components because an attack can operate on data while it is stored, data at rest, or data while it is being operated on or transferred, data in motion. We also distinguish between attacks that affect the system, which includes the operating system kernel and firmware, and those that affect user code, which includes any process running on the local host (in Fig. 1, Processes A, B, and C, and the Backup Recovery Agent).

[3] "NotPetya Technical Analysis", LogRhythm Labs, July 2017.

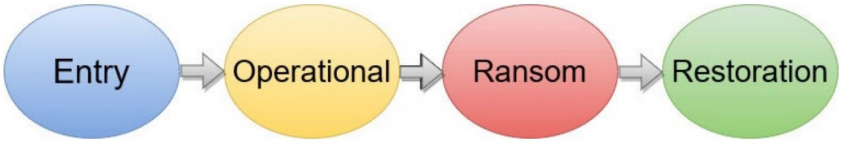


Figure 2: Workflow for a Successful Ransomware Attack

4 Attack Assumptions

This paper is focused on the recovery aspects of ransomware. As such, we are not discussing how the attacker enters the system. We assume that there has been a successful exploit and we are interested in how the attacker effects the ransom.

4.1 Attack Operations

Some of the basic operations that ransomware might use appear below:
Read, write, or create arbitrary files: These files might be on a local file system or on a remote server. The access could result in an exfiltration, encryption, or deletion of files. It could also result in modification of system configuration information. *Execute arbitrary code:* Executing any program on the system allows a wide range of control of the system. If you combine this operation with the ability to create or modify files, this means that any desired program or script can be created and executed.
Inspect the state of any process: Any information contained in the execution state of a process is available for viewing. Packages like Dyninst[4] simplify this access. *Modify the state of any process:* In the same way that a process' state can be read, it can also be modified, so, any existing running program can have its behavior changed. *Modify the state of the operating system:* A privileged attacker can modify the code or data within the operating system.

4.2 Attack Workflow

A ransomware attack goes through four basic stages, as shown in Fig. 2.
The **entry stage** is based on the initial system exploit. The exploit might be based on a human engineering attack, a known vulnerability in software that has not been updated, or a zero day attack. This part of the workflow is out of the scope of our discussion. This stage needs to be stealthy and may happen well in advance of the operational stage.
The **operational stage** is when the major damage to the system occurs. It is in this stage that data is encrypted, overwritten, deleted, or exfiltrated. An attack that encrypts or removes stored data, will transition to the ransom stage, leaving the system non-functional. To be most effective, it should operate quickly to avoid detection and interruption.
An attack that encrypts the data in motion can allow the system to keep operating even though the data is encrypted. The system would be modified so that data is encrypted when written and decrypted when read. The attacker chooses the time of transition to the ransom stage by deleting the decryption key and shutting down the system.
Lockout attacks prevent future operation of the system by changing a password, creating a new one, or overwriting critical code. After the modification, the system typically continues to operate normally until the user logs out or the system restarts.
There are, however, types of attacks that will not disable the system at all. For example, a pure exfiltrate attack, whose main goal is blackmail to prevent the public release of the data, will not prevent continued system operations.
The **ransom stage** requires payment to restore operation or prevent the release of private information. There must be some form of trust in the attacker to cooperate once payment is made. However, it is in the best interest of the attacker to fulfill their side of the bargain or else they endanger payments from future victims.
For systems that were disabled, the **restoration stage** allows continuation of normal operations. If data was encrypted at rest or in motion, the attacker will provide a decryption key. If the data was deleted, the attacker will provide a restore program to download the files. If a password was modified, the attacker will provide this new password. If a system component was modified, then the attacker will provide a key for the modified component to return to normal operations.
Of course, any payment of the ransom does not guarantee that there will be no future demands for payment. Only independent recovery will take the attacker out of the loop. Of course, the source of the initial exploit must also be determined and prevented.

5 The Ransomware Threat Space

Given our system model, we create a collection of threat scenarios, examining the model one component at a time to understand how ransomware attempts to prevent recovery. For each scenario, we discuss how the ransomware might subvert that component and how difficult it would be to recover after a successful attack. We also evaluate how difficult it is to carry out the attack and how difficult it is to detect it.

5.1 File System Attacks (FSA)

Files are the most common target of a ransomware attack, whether it is for encryption, deletion, exfiltration, or lockout. A file system attack can come in many forms, some of which are common in the wild and some of

[4] "The DyninstAPI Binary Instrumentation and Analysis Toolkit", https://github.com/dyninst/dyninst/

which have not yet appeared. The FSA scenario can come in three forms, attacks on data at rest, data in motion, and file metadata.

5.1.1 FSA on Data at Rest

The most common form of this attack is simple: read in a file, encrypt the contents, and write it back out. Encrypting a large amount of data can be slow, and that increases the opportunity for the system owner to discover the attack before it completes. To counter that issue, ransomware FSA's will often encrypt only part of each file. An alternative to the encryption FSA is to exfiltrate a copy of data with the intent on releasing the data publicly if no payment is made. This type of an attack is more blackmail than ransom. A recovery strategy from this type of FSA starts by making regular file system backups to a remote and safe server. Backing up files is a well understood and widely recommended practice to allow recovery from this type of attack. To reduce the chance that this server will also be attacked, it should follow several best practices for backups:

1. Backups should be "write once". Once they have been created, the server will not allow them to be modified. This is the "secure storage" criteria from NIST 1800-25.
2. The backup server should be physically secure.
3. Authentication and access to the server should be separate from other hosts. There should be a limited number of people that have access to the system and there should be a separate access enforcement mechanism.
4. File recovery should be tested on a regular basis.
5. Separate authoriziations and permissions for each backup client's files.
6. Using monitoring tools to detect when parts of the file system appear to have suspiciously encrypted content.
7. Limit the rate of backups that a client can make to prevent denial of service attacks.

Once the attacked host has been cleared of the attack, then the file system data can be restored using normal file restoration procedures.

5.1.2 FSA on Data in Motion

Data in motion attacks will encrypt, delete, or exfiltrate data *as it is being written* to the file system. This attack would require the file system code of the operating system to be modified, which makes this attack more difficult to implement. This attack could result in a situation *where recovery, even with best practices in backup, would be extremely difficult*.

This attack modifies the file system so that all data that is written is encrypted before it is stored. When data is read back, it is decrypted so that the attack is not visible until the moment of the attackers choosing. In the background, the existing stored data is encrypted with the same key. The attack could be scheduled to be triggered at a certain time. Triggering the attack would cause the encryption/decryption key to be deleted from the computer's local memory. At this point, all file reads would return encrypted data.

Note that since the system keeps operating while the files are encrypted, the backed up files will also be encrypted. This attack becomes more effective if the system is left to run for a longer period of time because the longer that the attack persists, the greater the change in the file system since the last unencrypted backup.

This attack might be discovered by tools that detect the presence of a large presence of anomalous or encrypted data in the file system. Such detection might also allow for the discovery of the encryption key before it was detected by the attacker.

Recovery from this type of attack is problematic. If the attack was to persist for an extended period of time then the backup best practices described in Section 5.1.1 would not be effective. Such an attack will likely result in potentially significant data loss.

5.1.3 FSA on File System Metadata

A file system attack is not limited to modifying the data stored in a file; it could also modify the information that describes how the data is stored, often called the *metadata*. Examples of metadata that could be modified as part of an effective attack include the file names and access permissions. The most effective file name attack would be encryption of the file names. While the file contents would remain intact and accessible, such an attack would make finding the files problematic.

Conceivably, a tool could be constructed that would compare the shape of the file system tree and file contents of the attacked file system to its most recent backup. Such a tool should be able to recover most of the file names.

5.2 Storage Server Attacks (SSA)

These attacks are similar to the FSAs: We are assuming that a privileged process can have arbitrary access to the files on the server in the same way as it would have access to local files. As such, most of the discussions from Section 5.1 apply to SSAs. We note that many of the FSAs are also SSAs. One way that this assumption is not true is that in an SSA, the server process is running on a different host, so it cannot modify the system software on that host. This limitation means that a comprehensive data-in-motion attack is not possible. While the attacker could intercept the reads and writes from the exploited host, it would not be able to intercept requests from other hosts. Under the data-in-motion attack, 7 after data is written to a file in encrypted form but before the ransom act, file reads need to transparently decrypt the data.

In addition, depending on how the storage server is configured, the attacked host may not be able to access all the files on the server nor have administrator access to that

server.

5.3 Database Server Attacks (DSA)

There are many similarities between a client process accessing a database server and a client process accessing a storage server. The main difference is the access protocol. In the storage server case, access follows the basic open/read/write/close semantics of a file system. In the database server case, access follows a more structured protocol such as SQL.

With a DSA, we can still have attacks that encrypt the contents of the database, exfiltrate the data, or remove it. We can also attack the database metadata by renaming relations or attributes and changing access permissions. In addition, we can intercept requests made by the client to the database server, so it can affect a data-in-motion attack. However, as with the SSA, we can only control the behavior of the clients on the attacked host and not those running on other hosts. This limits the effectiveness of such an attack.

5.4 Backup System Attacks (BSA)

Backup systems play a key role in providing system reliability both in response to normal system and device failure and in response to an attack. Given this key role, the backup system itself becomes an attractive target for attack. From Fig. 1, we can see that backups can be written to locally mounted disks or to a remote backup server. In both cases the attack has the same effect. The point of attack is the software on the local computer that identifies the files to be backed up and then writes them to storage.

A backup system attack modifies the data that is being written to the backup storage device or service by modifying the behavior of the Backup Recovery Agent. For this modification to be a ransom activity and not vandalism, it must be reversible. For it to be an effective ransom activity, it must be difficult to reverse without special knowledge.

This attack proceeds through the stages described in Section 4.2 (Fig. 2). During the entry stage, the attack modifies the backup software to encrypt all data that is backed up. During the operational stage, any backups that are produced will be encrypted in such a way that the user cannot use them. The longer the system runs, the more data will be stored in an encrypted, and therefore useless backup. The backup software would also be modified so that any recovery requests made during the operational stage properly decrypt the data. This recovery behavior ensures that the attack continues to be stealthy until the ransom phase is triggered.

The ransom phase is triggered by deleting the primary copy of the files from the file system and deleting the decryption key from the host. At this point, the files are gone and the backups are encrypted.

Preventing a BSA is based on limiting the damage that can occur. Such limiting requires that we can detect when backup data is unexpectedly encrypted. Such detection might be accomplished by using a file system monitoring tool as described in Section 5.1. Recovery for such an attack is problematic as the primary data is gone and the secondary data is encrypted. The longer that this attack is stealthily present in the computer, the larger the percentage of data that is likely to be encrypted.

5.5 Firmware Attacks (FWA)

Firmware is the software that is provided by a device manufacturer and runs inside a device to control that device. It is separate from the operating systems and applications that run on the computer and is stored in separate memory local to the device it controls.

5.5.1 FWA Modifying the Firmware

There have been significant firmware attacks in recent years.[5, 6] In a ransomware context, taking control of a device's firmware has serious security consequences, such as:

- Taking control of the disk firmware, preventing booting the system.
- Taking control of the keyboard firmware, allowing an attacker to set a boot password that would also prevent booting.
- Taking control of the NIC firmware, isolating a computer, or allowing remote access and control.
- Taking control of the battery firmware[7], causing shutdown of the computer at will.

The good news is that modern systems provide significant defenses against such attacks, starting with processor-based security mechanisms that provide cryptographically strong storage of keys. Unless you can open the chip and defeat its anti-tampering mechanisms, the data stored can be considered reliable and secure. The encrypted keys and certificates, combined with signing of each software update delivered to the computer from the vendor, make it difficult to replace any system component.

While a successful firmware attack can be difficult to do, recovery from such an attack can be extremely labor intensive. Such a recovery can require reprogramming the EEPROM or FLASH memory on the motherboard or in the devices themselves. While the labor to recover a few computers is manageable, the cost to recover a large number of computers, such as found in a data center or corporate network, can be prohibitive.

Best practices for prevention and recovery include:

1. Ensure that your operating system is updated to the most recent release. The newest versions of the major operating systems require signed software and (mostly) signed firmware and up to date hardware.
2. Ensure that Secure Boot has not been disabled.
3. Ensure that the Trusted Platform Module (TPM)[8] has not been disabled.

5.5.2 FWA Setting a Boot Password

A standard security feature of modern computer systems is the ability to set a boot-time password. These passwords require that the password be typed on the keyboard. The BIOS/UEFI will enforce "proof of presence" at the keyboard to accept a password. Subverting protections on setting a boot password could be done by subverting the keyboard firmware. If the keyboard says that a person is present and entering a password, then the operating system is likely to accept this entry. The boot password is stored in separate volatile CMOS RAM on the motherboard. The battery on the motherboard that powers the RAM needs to be physically disconnected to reset any security data stored in this RAM. Such disconnection may involve unsoldering the battery connection. A best practice for prevention is to have a boot password already set on your computer.

5.6 Operating System Attacks (OSA)

5.6.1 OSA on the Boot Loader and Boot Image

The boot loader is the software responsible for initial loading of the operating system kernel. As described in Section 5.5, there is a cryptographically secured chain of steps that ensures that only software that originated from the vendor will be booted. A successful attack on the boot loader or operating system boot image will prevent the operating system from starting. Until this situation is repaired, the computer will be unusable until it can be booted from an alternative device.

The Secure Boot feature, along with Boot Guard or Hardware Validated Boot, will prevent an attacker from replacing the boot loader or operating system boot image. However, it will not prevent a vandalism attack that overwrites these items with non-functional code, such as was done for NotPetya attack on Maersk's shipping network.

Most operating systems offer the ability to boot from removable media or the network. Once this is done, then the boot loader or operating system image can be restored. Such operation requires physical presence at the computer, so it is reasonable for recovering individual computers but expensive for large facilities or data centers. Best practices for this situation are the same as those described for firmware attacks in Section 5.5.

5.6.2 OSA on Account Passwords

A simple attack is to change the passwords for users and administrators. Such an attack will prevent normal access to the computer though it may not stop services from starting on booting the system.

As mentioned before, most operating systems offer the ability to boot from removable media or the network. Once this is done, then the password file(s) can be restored. Such operation requires physical presence at the computer, so it is expensive for large facilities.

Best practices here include:

1. Make sure that files storing login authentication data are included in the backups.
2. Ensure that you have escrowed the disk encryption keys for all the storage devices on all your systems.

6 Conclusion

We have described a framework for how a ransomware attack can affect a computer system, described the risks associated with such attacks, and presented some best practices for prevention and recovery. This document should be considered only a starting point for a longer technical discussion on ensuring that recovery from a successful ransomware attack can be prompt and effective.

[5] "Sean Metcalf, "Thunderstrike: EFI bootkits for Apple MacBooks via Thunderbolt & Option ROMs", https://adsecurity.org/?p=854

[6] Pavel Shoshin, "Malware delivery through UEFI bootkit with MosaicRegressor", https://usa.kaspersky.com/blog/mosaicregressor-uefi-malware/23419/

[7] C. Miller, "Battery Firmware Hacking", DEF CON 19, Las Vegas, August 2011.

[8] Trusted Computing Group, "Trusted Platform Module (TPM) Summary", https://trustedcomputinggroup.org/resource/trusted-platform-module-tpm-summary/

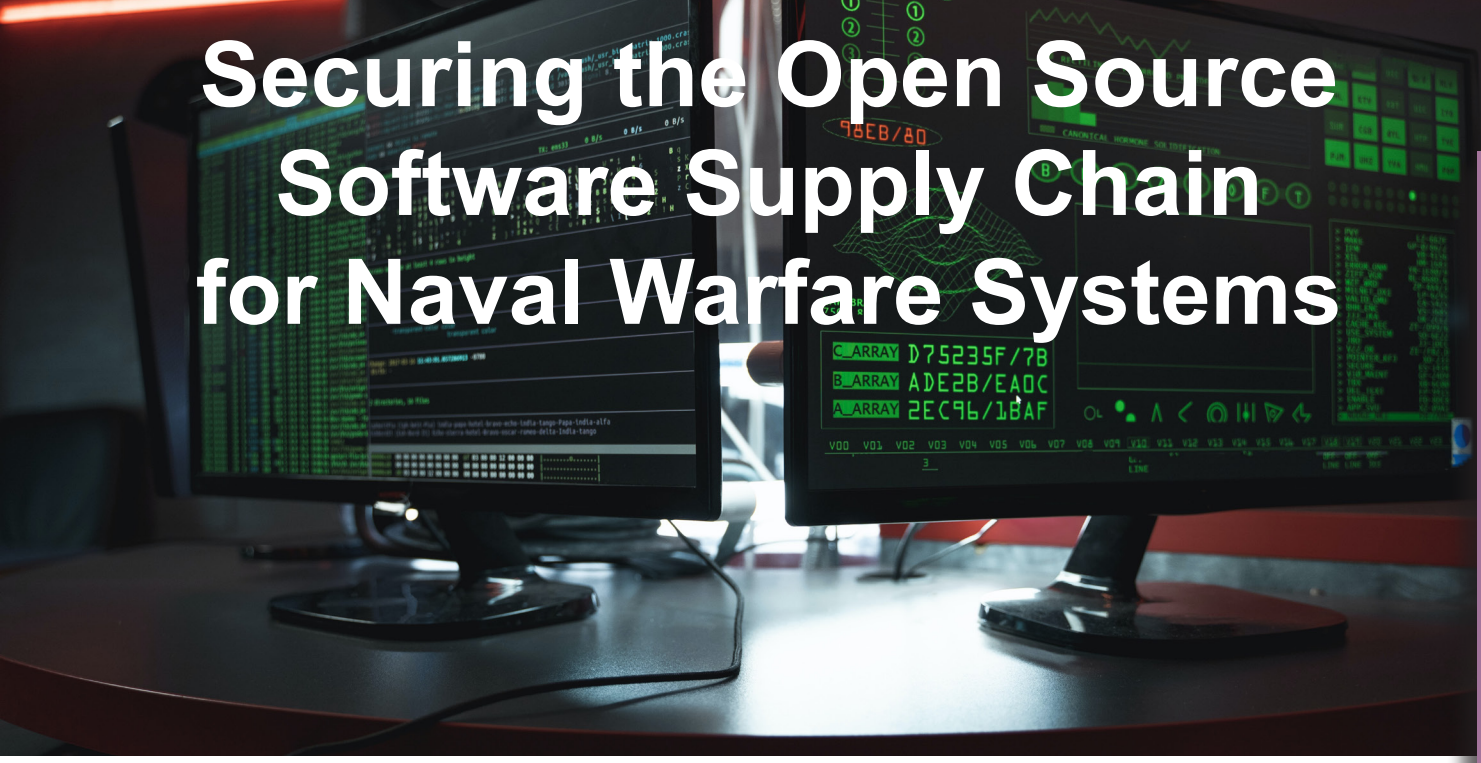
Barton Miller is the Vilas Distinguished Achievement Professor and the Amar & Belinder Sohi Professor in Computer Sciences at the University of Wisconsin-Madison. He is a co-PI on the Trusted CI NSF Cybersecurity Center of Excellence, where he leads the software assurance effort and leads the Paradyn Tools project, which is investigating performance and instrumentation technologies for parallel and distributed applications and systems. His research interests include software security, in-depth vulnerability assessment, binary and malicious code analysis and instrumentation, extreme scale systems, and parallel and distributed program measurement and debugging. In 1988, Miller founded the field of Fuzz random software testing, which is the foundation of many security and software engineering disciplines. In 1992, Miller (working with his thenstudent Prof. Jeffrey Hollingsworth) founded the field of dynamic binary code instrumentation and coined the term “dynamic instrumentation”. Miller is a Fellow of the ACM and recent recipient of the Jean Claude Laprie Award for dependable computing.
Miller was the chair of the Institute for Defense Analysis Center for Computing Sciences Program Review Committee, member of the U.S. National Nuclear Safety Administration Los Alamos and Lawrence Livermore National Labs Cyber Security Review Committee (POFMR), member of the Los Alamos National Laboratory Computing, Communications and Networking Division Review Committee, and has been on the U.S. Secret Service Electronic Crimes Task Force (Chicago Area).

Barton P. Miller, Vilas Distinguished Achievement Professor, Sohi Professor in Computer Sciences,
NSF Cybersecurity Center of Excellence, University of Wisconsin-Madison
bart@cs.wisc.edu

Elisa Heymann is a Senior Scientist on TrustedCI, the NSF Cybersecurity Center of Excellence at the University of Wisconsin-Madison, and an Associate Professor at the Autonomous University of Barcelona. She co-directs the MIST software vulnerability assessment at the Autonomous University of Barcelona, Spain. She coordinates in-depth vulnerability assessments for NFS Trusted CI, and was also in charge of the Grid/Cloud security group at the UAB, and participated in two major Grid European Projects: EGI-InSPIRE and European Middleware Initiative (EMI). Heymann’s research interests include software security and resource management for Grid and Cloud environments. Her research is supported by the NSF, Spanish government, the European Commission, and NATO.

Elisa Heymann, Senior Scientist, Associate Professor
NSF Cybersecurity Center of Excellence, University of Wisconsin-Madison, Autonomous University of Barcelona
elisa@cs.wisc.edu

Securing the Open Source Software Supply Chain for Naval Warfare Systems



by Eric Hill, Sonatype

Introduction

We live in a "Software Defined World" where even the semiconductors at the core of processors are defined in software pre-fab. It was thus that the author had intended to spend more professional time in 2022 addressing the concept of a "Secure Semi-Conductor Factory" [pre-fab]. The author sent an informal letter to a US Congressional office, as an engaged US citizen concerned with national security, and was even asked to address the topic at a professional conference later in 2022.

But alas, Log4Shell dislodged holiday calendars across the Free World as 2021 was coming to a close. Americans across the USA engaged in the Defense Industrial Base (DIB) and critical infrastructure whether enlisted in the military, employed by the government or within the private sector went "above and beyond the call" into 2022 to address this national security concern. The current employment of the author reflects a decision to have a more direct & precise impact on securing the open source software supply chain for naval warfare systems.

This paper is not intended to be a corporate advertisement. However, it is unavoidable in some way to not associate with an existing integrated capability platform so as to not mislead the reader to believe this is simply theory; as opposed to implementable, deployed and working technology. The suite noted in this paper has allowed for solutioning to unique challenges currently being faced in the maritime space. Thus, while care will be taken to address capabilities, the reader will also understand specific software notations.

It is worth noting that war was brought to Europe during February 2022, with the invasion of Ukraine by Putin's Russia. Prior to the kinetics and land incursion, there were also cyber-attacks on maritime ports in Europe. Per articles at the time, the energy terminals were specifically targeted. Timed with the invasion, Russian cyber units ensured that base capabilities of telecommunications infrastructure in Ukraine were taken out of play. These capabilities were later restored per Elon Musk's software defined Star Link satellites.

This white paper should be considered a Part 2 to "Securing the Software Supply Chain for Naval Warfare Systems" presented 2021 at the 5th NMIOTC Cybersecurity Conference in the Maritime Domain" and subsequently published in the journal.

Log4Shell

On July 11, 2022, the Department of Homeland Security released a report entitled "Review of the December 2021 Log4J event". The timeline was well laid out. One can see in the timeline in Figure 1 that on Nov 24, 2021, a team from Alibaba, a mainland China company, reported the Log4J vulnerability to the ASF (Apache Software Foundation). By Dec 1, 2021, the Log4J vulnerability was exploited in the wild. Eight days later on Dec 9, it was shared on a Chinese language blogging platform. Within 1 day, Dec 10, CISA (Cybersecurity and Information Security Agency – USA) released its first advisory while CVE-202144228 was entered into the NVD (National Vulnerability Database – USA). Dec 13 the vulnerability was officially reported to the PRC's Ministry of Industry and Information Technology.

Over December, through the 28th, what proceeded was a series of iden-

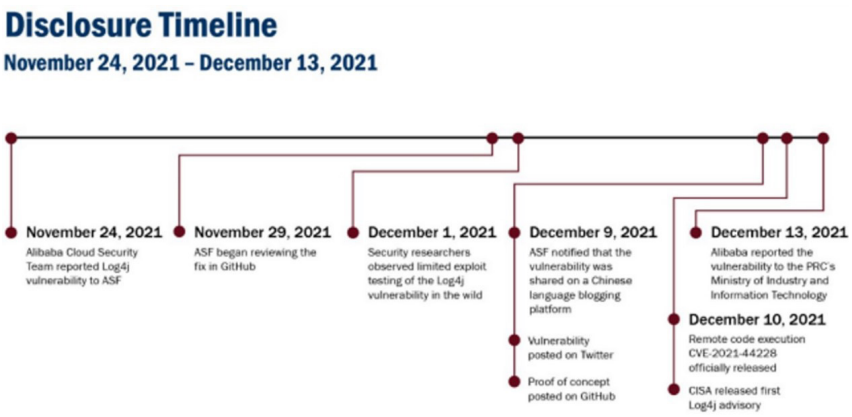


Figure 1: Log4Shell Disclosure Timeline
"Review of the December 2021 Log4J event", DHS July 11,2022

tified vulnerabilities, each a national security concern due to the nature and near global use of the open source Log4J libraries. (CVE-2021-45046, CVE02021-4104, CVE-2021-45105 & CVE-2021-44832). Following public disclosure on December 9th, the report noted a number of attempts by known malicious actors along with statistical break outs.

Per the author's experience, the Defense Industrial Base (DIB), military domains, and federal agencies scrambled to identify where the Log4J open source libraries were in use on enterprises followed by methods for expedient mitigation. This single series of events proved that securing the open source supply chain proactively is of the utmost national security concern.

Sonatype, the long-term steward of Maven (public java repository), released a series of concerning statistics in the months that followed Dec 2021. As of March 7, 2022, 37% of Log4J downloads were still vulnerable versions. There is no wonder that for the first time ever the Federal Trade Commission had to step in during 2022 and declare that all businesses in the USA needed to purge these vulnerabilities from their systems. This was after declarations by CISA, Homeland Security, the FBI, the NSA & other agencies.

Later during 2022 the author presented during on-site Naval conferences, online meetings and on-base briefings how with the Sonatype integrated suite in a software factory configuration the OSS cyber posture could be maintained for assets; ashore and afloat (sea, air, space).

NPM & PyPI Attack Surface

Having mentioned the Maven (java) public open source repository, it is worth mentioning npm (javascript) and PyPI (python) public repositories. Amongst many other uses, these 2 repositories are in heavy utilization,

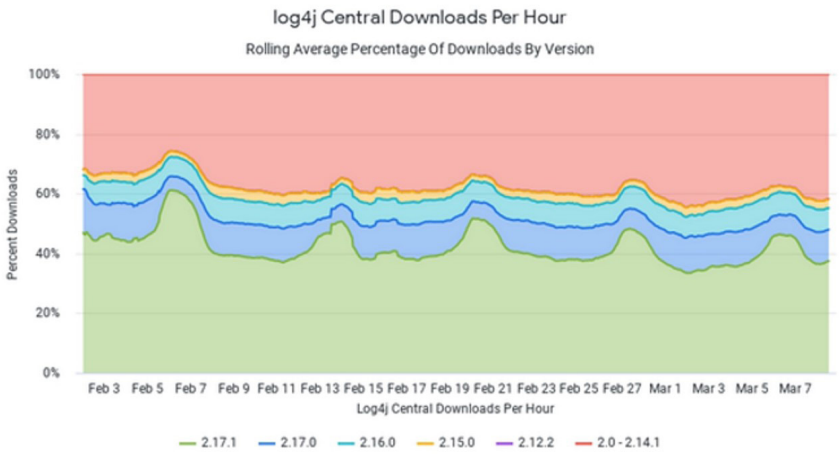


Figure 2: The Shifting Landscape of Open Source Attacks *- Sonatype*

including the defense industrial base, for AI applications. New component submissions that have been constituted of malicious code is staggering. The Sonatype Nexus suite has an AI/ML-powered quarantine capability that has identified 88, 217 malicious packages in npm and PyPI as of August 18, 2022. Communication to the stewards of these repositories by Sonatype resulted in 15,185 of these packages being taken down.

Worth noting, enterprises using this AI/ML-powered quarantine capability to protect their SDLC have not been exposed to this cyber risk.

Artificial Intelligence

In "Understanding AI Technology" (DoD Joint AI Center , April 2020) two types of AI are defined:

Handcrafted knowledge AI is defined as "software developed in cooperation between computer programmers and human domain subject matter experts. Handcrafted Knowledge Systems attempt to represent human knowledge into programmed sets of rules that computers can use to process information."

In this white paper this is referred to simply as "AI".

Machine Learning AI is defined as "systems generate their own rules. For Machine Learning systems, humans provide the system training data. By running a human-generated algorithm on the training data, the Machine Learning system generates the rules such that it can receive input x and provide correct output y."

In this document this is referred to simply as "AI-ML".

These two definitions will be important when we differentiate capabilities.

Note that in 2022, the JAIC was folded into the CDAO (DoD Chief Artificial Intelligence Office).

A Word on Provenance

NIST 800-53 defines provenance as:

"the chronology or the origin, development, ownership, location and chang-

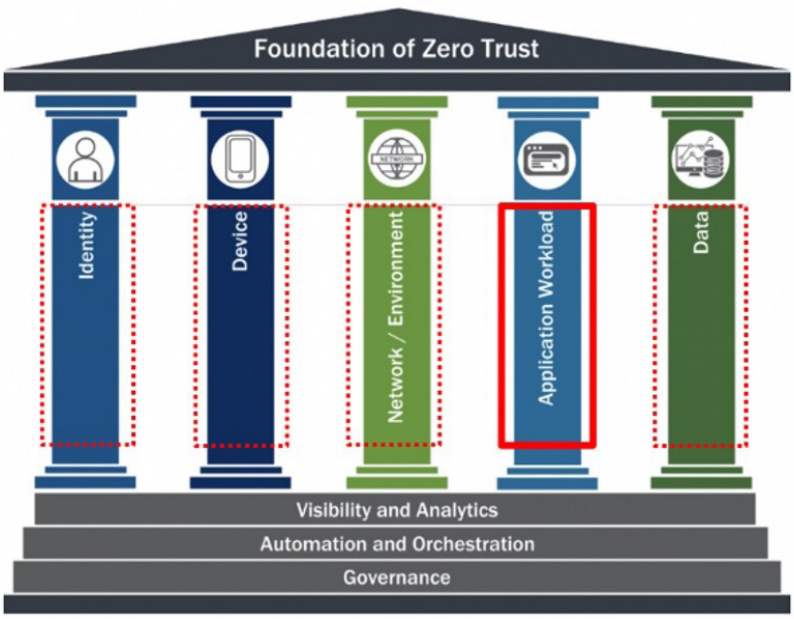


Figure 3: *"CISA Zero Trust Maturity Model 1.0" June 2021 (red markup by author)*

es to a system or system component and associated data. It may also include personnel, and process used to interact with or make modifications to the system, component, or associated data".

Utilizing public open source repositories such as Maven, npm and PyPI give some degree of provenance. Given the open source supply chain attacks, including by state funded actors, much has been discussed regarding personnel, modifications to oss projects, etc. To that end, the sigstore effort (www.sigstore.dev) has evolved into an industry effort for providing added measures for chain of custody of open source components. On August 9, 2022, Microsoft announced the intention to utilize sigstore with the npm public open source repository for which the company is the steward.

A Word on Zero Trust

CISA (Cybersecurity and Information Security Agency) was tasked with extending and managing much of the effort to operationalize Executive Order 14028. In June 2021, CISA released a draft version of its "Zero Trust Maturity Model". It is intended to give a framework for enterprises to evaluate and progress in zero trust efforts. Of note, the topic of this white paper is central to the 4th pillar, "Application Workload", as indicated by the solid red rectangle in **Figure-3** , while multifactor authentication seems to be the focus of many Zero Trust efforts.

We live in a Software Defined World where the activities encompassed in the 4th pillar to maintain cyber posture of software that are inherently utilized in the other pillars; Identity, Device, Network and Data. The author contends that a parallelized approach should be adopted in good measure when moving forward in Zero Trust Maturity. This has been a topic of discussion in DC-area conferences during 2022 and such a strategy has been confirmed to be utilized by several federal agencies.

In environments where Kubernetes is in use, the Istio Project (http://www.istio.io/) offers an operational model to apply zero trust concepts to the software system architecture.

EO 14028 & DoD/Intelligence Community Guidance

On January 19, 2022, US President Joe Biden issued NSM-8 titled "Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems" that gave a timeline to recommendations by the DoD and Intelligence community to the organizations under their respective jurisdictions. As of this writing, the author is aware that all branches of the US Military, including the US Navy, intend to implement principles of EO14028, including SBOM generation and consumption as well managing cyber risk. As EO14028 originally applied to federal agencies, the Department of Transportation, with domain over maritime ports and under jurisdiction of the CISA, has had compliance in its purview.

It should be noted that CISA, the NSA & the Office of the Director of National Intelligence on Sept 2, 2022, released "Securing the Software Supply Chain: Recommended Practices Guide for Developers" continuing EO14028 rec-

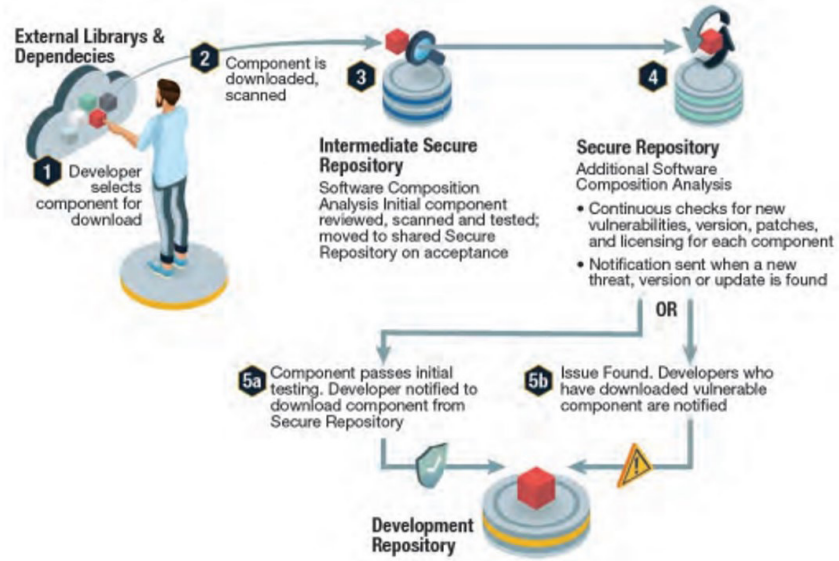


Figure 4: *"Securing the Software Supply Chain: Recommended Practices Guide for Developers" - CISA/NSA/ODNI, p. 15, August 2022*

ommendations. **Figure 4** represents a high level diagram on p. 15 of the document that is supported by the capabilities platform that is highlighted later in this white paper in a US Department of Defense context.

Capabilities for Risk Mitigation in the SDLC

Before we revisit the context of the Software Factory in this part 2 white paper, we will define some capabilities. Given the current outlook on cyber-attacks to the open source software supply chain, as previously stated, it is of utmost importance that the reader understand that these capabilities currently exist in an integrated platform and are not relegated to theory. Icons representing capabilities encompassed in the platform are superimposed over the DoD Software Factory diagram for clarity in the next section.

F -capability (Sonatype Nexus Firewall) – AI/ML-powered quarantine, AI-powered Risk Policy Engine, AI-powered component Situational Awareness, etc inhibits risk uptake into SDLC

L -capability (Sonatype Nexus Lifecycle) – SCA, AI-powered Risk Policy Engine, AI-powered Situational Awareness, SBOM scan, SBOM ingestion, SBOM export, Vulnerability management, Component management, Continuous Monitoring, etc across the SDLC

R -capability (Sonatype Nexus Repository Manager) – proxy repository, hosted repository, etc with failover

It is important to remember that when we speak to a vulnerability, per Part 1 of this Part 2 paper, we are concerned with CVE's on 3rd party OSS components, whether registered w/ the NVD (National Vulnerability Database) or proprietary; as opposed to CWE's which are identified in 1st party code via SAST & IAST scans.

The Software Factory Core

Figure 5 is a DoD diagram that has been decorated in red. Likewise highlighted capability icons have been placed so that readers understand the functionality discussed in positions 2-9 are not theory, but available in an integrated platform.

The **L-capability** at 5-8 represent SBOM capabilities provided by integrations with source code control (5) and CI/CD (6, 7 & 8); the latter representing build, staging and release phase security gates of the SDLC. Likewise, risk policy failures identified as a result of scans can, and should, be configured to message stake holders via available communication channels (email, ticketing, etc) where appropriate.

At 9 the **R-capability** represents the release package in a "hosted repository". On the higher end of enterprise and mission maturity it will include containers and other artifacts per stamped release. At the same time, represented by the **L-capability**, is continuous monitoring of the release SBOM for component vulnerabilities & related risk policy assessment without rescanning the software for the SBOM itself. Continuous Monitoring is a function important later in this paper.

In addition, CycloneDX SBOM's can be ingested at 9 via REST interfaces by the **L-capability** and apply continuous monitoring. In this case it is recommended CI/CD tooling also place the SBOM, with consistent naming methodology applied, into the release repository via REST interfaces of the **R-capability**.

Moving to the left of the diagram, position 1 represents the public open source repositories such as: Maven, npm, PyPi, R, Conan, etc.

A simple scenario:

1. A developer at 4, via code IDE plug-in delivered situational awareness, evaluates risk in a component visible in the SBOM per the **L-capability**. Via the package manager command-line the user requests to download a newer version of the OSS component from a public repository.
2. As the package manager is configured to utilize the "proxy repo" as an intermediary to the public repo, the request is forwarded to the proxy repo at 3 per the **R-capability**.
3. The request is forward to the matching public repo at 1.
4. The component itself is evaluated at 2 by the **F-capability**.
5. Assuming the OSS component passes policy evaluation, it is available in the proxy repo at 3 per the **F-capability** & **R-capability**.
6. The component is then downloaded to the filesystem of the developer at 4 per the *package manager* technology utilized in 1, (of this list).

AI -powered Situational Awareness for Component & Vulnerability Management

A key to component and vulnerability management is delivering situational awareness to all stakeholders. The AI-powered widget in this capability platform is accessible in 2 – 9 in the decorated software factory diagram in **Figure-5** via the **F–capability**, **R-capability** and the **L-capability**. Each stakeholder role is able to navigate from the SBOM, in the case of 4-9,

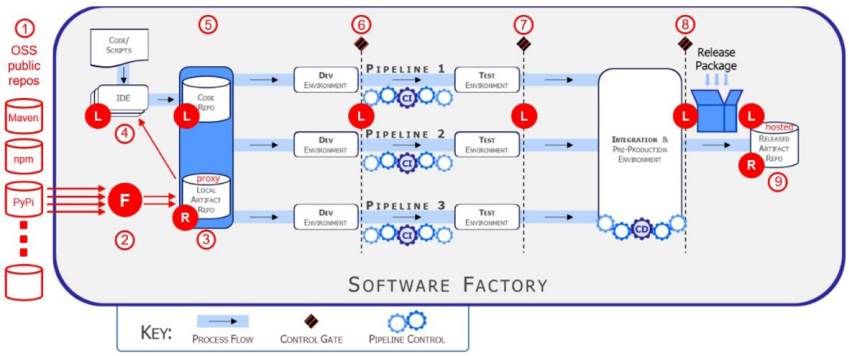


Figure 5: DoD DevSecOps Strategy Guide, *US Department of Defense, 2021 - red markup by Author*

Figure 6: AI- Powered OSS Component Situational Awareness
- via Sonatype Nexus IntelliJ plugin

or a view of individual components at positions 2 & 3. Important to note that in 4-9 whether the SBOM visual is delivered via IDE (4) or cut-over from advice to developers & CM personnel using source code control (5) or from the CI/CD tools (6-8) or even from ticketing, email, etc in 5-9 if the policy engine is configured to message on policy violations triggered.

In positions 4 – 9 of **Figure 5**, where applicable, there may be a Recommended versions list displayed above the widget. This may include:

a. *Next version with no policy violation*

b. *Next version with no policy violation & no breaking changes*

c. *Next version with no policy violations for this component and its dependencies*

d. *Next version with no policy violations for this component and its dependencies & no breaking changes*

Clicking on the displayed version number in each case will move the slider to the version in the widget.

At position 4 in the software factory, the developer using an IDE, where applicable there may be a button labeled "*Migrate to selected*". Clicking on the button will update the relevant package manager files on the developer's filesystem, the SBOM depiction and, of course, the widget itself.

Wherever the slider in **Figure 6** is placed, properties and their values displayed to the right of the widget give finer grained detail on the component.

Reviewing quickly in the widget, one can see the 3 types of risk outlined in the author's previous paper "Securing the Software Supply Chain for Naval Warfare Systems": Security, License and Quality. For each risk category, the highest severity policy violation is propagated to the display and reflected in the heat map.

Breaking changes represents the ease of upgrading to a version represented in the widget from the current version; given standard software development conventions.

In the heat map, colors represent higher level severities in increasing order: **blue**, **yellow**, **orange** & **red**.

AI/ML -powered Quarantine to Inhibit Risk Uptake into the SDLC

Inhibiting uptake of cyber risk into the SDLC is a must given the current active threats. In the **F-capability** we are presented with a solution. In the section on npm and PyPi some statistics were presented earlier regarding success against blocking "malicious" OSS components downloaded from public OSS repos. In addition, the policy engine enforces quarantine of uptake of new components that violate policy.

Figure 7, an activity diagram with swim-lanes, gives us the opportunity to gain high-level clarity of this process. By now the reader should be able to match this flow to the decorated Software Factory Diagram and previous description in **Figure 5**. The line numbers in the description below map to the **Figure 7** activity diagram in this section.

1. A new OSS component is submitted to an OSS public repository. (at 1 in **Figure 3**)
2. At time **T** a developer has decided to utilize this new component in a project, possibly a new version of an existing OSS component, and requests to download it to the proxy repository. (at 4 in **Figure 3**)
3. The **F–capability** utilizes AI-ML to evaluate 40+ properties of this new OSS component. (at 2 in **Figure 3**)
   a. If OSS component is *suspicious* to 4 below
   b. If OSS component is NOT *suspicious* to 7 below
4. The OSS component is moved to *quarantine* in the proxy repository (at 3 in **Figure 3**)
5. The OSS component is researched by security analysts to evaluate if it contains malicious code; at worst executing in the Software Factory environment.
   a. If *malicious* to 6 below
   b.If NOT *malicious* 7 below
6. The new OSS is marked *malicious* and stays in *quarantine*. For other users of the **F–capability**, the policy engine will be set to *quarantine* this OSS component in other Software

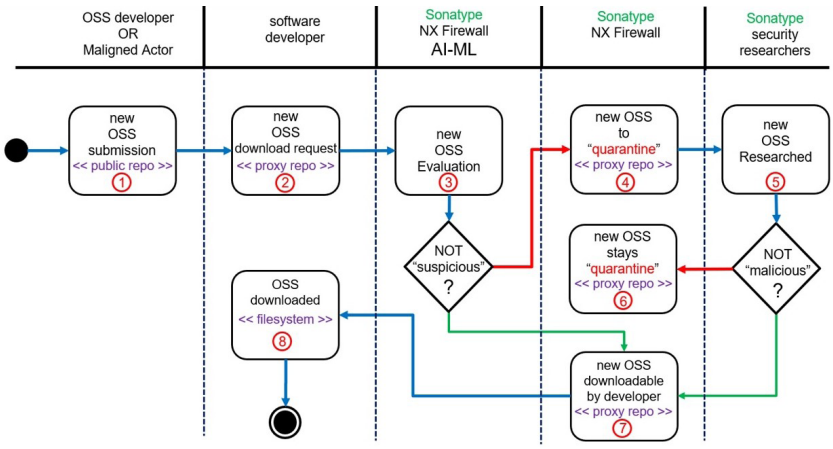


Figure 7: Quarantine Capability Swimlane Activity Diagram *by Author*

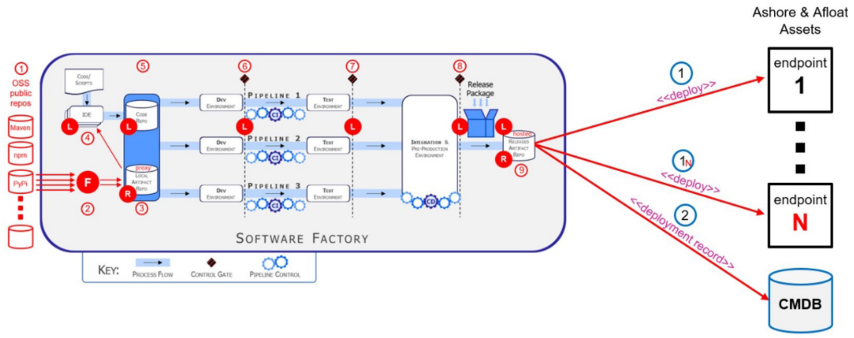


Figure 8: Optimize Zero Day Situational Awareness & Mitigation to the Tactical Edge *LEFT "DoD DevSecOps Strategy Guide" with red markup by Author RIGHT deployment diagram by Author*

Factory environments when download requested.

7. The OSS component is present in the proxy repo for subsequent use by other developers. (at 3 in **Figure 3**)

8. Per the initial request the OSS is downloaded to the developer's filesystem. (at 4 in **Figure 3**)

Shift Continuous Monitoring LEFT

It has been observed by the author that the culture of US Navy considers "continuous monitoring" to be a be a concern of real-time protections at endpoints; be the asset ashore or afloat. While the author contends this must be done, it is not enough. To align with being Cyber Ready per the DON CIO "Strategic Intent for Cyber Ready" there must be a Shift Continuous Monitoring LEFT function. Outlined in the previous sections we covered how a Software Factory developing software releases with SBOMs (per a scan), OR having ingested SBOM's from other sources, can status the vulnerability posture for a SBOM.

Shifting continuous monitoring LEFT, we can now advantage deployment principles depicted in **Figure 8**; which has been presented in a number of onsite and remote Naval capabilities briefings.

With each release of mission-centric software in the Software Factory, the software will eventually be deployed to 1 – N assets. Each software deployment will be recorded in a CMDB (configuration management database) or equivalent (asset database, etc). If we use consistent naming from the SBOM in the **L-capability**, the release in the **R –capability** and the entries in the CMDB, we can now do the following on the occurrence of a national security level CVE threat (such as Log4Shell) to a naval warfare system:

1. Automation queries the REST API of the **L-capability** for releases where the CVE is present.
2. For each named release, query the CMDB(s) for the assets to which the software release was deployed
3. Merge the data sets
4. Display the assets in a console or display in a command center, etc
5. With this situational awareness, stakeholders can then make informed decisions based on other parameters (theater of deployment, ashore or afloat, etc).

This scenario is obviously simplified. However, in simplicity we can begin to acquire common understandings and operationalize capabilities. Even in the era of the digital twin, the basic concept will still hold.

The form factor of the data display could be in a simple grid format, a multi-dimensional graph display on a 2d surface, or even a multi-dimensional graph displayed in a holographic format.

Cyber Ready to the Tactical Edge

In February 2022, the "Department of Defense Software Modernization Strategy" was published. **Figure 9** in many ways presents delivering cyber ready systems to the men and women serving at the tactical edge. In times of war, of course, we are concerned about lethality and the well being of the warfighter. Per the capabilities and methodology presented in previous sections of this whitepaper, and indicted in the highlighted diagram, we have an opportunity to truly provide cyber ready assetts and systems to the warfighter at the tactical edge.

Joint All Domain Command and Control – Project Overmatch

"Joint All Domain Command and Control: Background and Issues for Congress" (updated January 21, 2022) defines Joint All Domain Command and Control as:

"JADC2 intends to help commanders make better decisions by collecting data from numerous sensors, processing the data using artificial intelligence algorithms to identify targets, and then recommending the

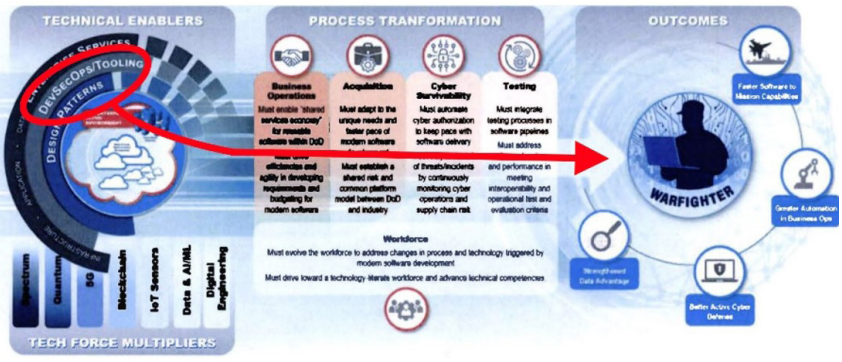


Figure 9: DoD Software Modernization Strategy, Feb 2022*, red markup by Author*

optimal weapon—both kinetic and nonkinetic (e.g., cyber or electronic weapons)—to engage the target."

Project Overmatch constitutes the US Navy's efforts at JADC2. As articulated in this paper regarding securing the open source software supply chain, the discussed capabilities are needed to keep these naval warfare systems cyber ready for JADC2. The author, and public documentation, confirms the capabilities are, in fact, in use by the US Navy.

At this same time, the US Department of Defense has announced intention to link with JADC2 equivalent capabilities of US allies. Specifically, the United States and United Kingdom have begun exploratory efforts on integrating the US's JADC2 and the UK's MDI CP (*Multi-Domain Integration Change Program*) utilizing a federated concept. This has been titled FNC3 or "*Fully Networked Command, Control and Communications*".

Other allies that have approached the USA for integration are members of the Federated Mission Networking Framework. Regardless, it goes without saying that allies integrating with JADC2 will also need to ensure that their open source software supply chain is secure on an ongoing basis to the Tactical Edge.

Summary

The US Navy is paying high regard to Software Factory Configurations & moving towards a more refined approach using the presented capabilities, or rather applying Software Composition Management. Meanwhile, kinetic war has arrived in Europe during 2022 supported by maligned cyber activities. The Free World must ensure software that is deployed is continuously cyber ready, particularly in combat theaters. It is the authors hope that via the technology sharing in the Joint All Domain Command and Control effort amongst allies, advanced Software Composition Management platform capabilities & practices, as presented in this white paper, will be adopted amongst the navies, maritime fleets and ports of the Free World … Sea, Air, Space and Land.

Eric Hill has a BS in Computer Engineering from the University of New Hampshire and his career spanning nearly 3 decades. He has been involved with product development life cycle of telecommunications equipment and the advanced software that manages it. For nearly a decade he consulted in automation efforts on critical infrastructure.

Eric worked as a Technical Account Manager for the defense sector customer base of a large technology firm specializing in silicon & software assurance where he provided industry thought leadership. Securing the software supply chain with Synopsys' SCA, SAST, IAST & DAST tool chain elements of Software Factory solutions was key to this role. As well he provided guidance on placing of corporate silicon and software assurance assets into the defense industrial base. Mr. Hill also promoted the concept and organization of a Secure Silicon Factory concept. He was also referenced for validating corporate investment into university research efforts.

As the Log4Shell vulnerability became a national security concern at the end of 2021, Eric was engaged with a number of DIB companies, military domains and federal agencies. It was at this point he made a professional decision to join Sonatype. Today as a SME he is dedicated to accelerating adoption of Sonatype technology and best practices to secure the software supply chain and fulfill national security needs.

Email: ehill@sonatype.com

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

References

NIST 800-53 rev 5 – "Security and Privacy Controls for Information Systems and Organizations"
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
"Securing the Software Supply Chain: Recommended Practices Guide for Developers"- CISA/NSA/ODNI
Securing the Software Supply Chain: Recommended Practices Guide for Developers (defense.gov)
"Understanding AI Technology" – JAIC (DoD Joint AI Center – now DoD CDAO) April 2022
https://apps.dtic.mil/sti/pdfs/AD1099286.pdf
DoD CIO Library
https://dodcio.defense.gov/Library/
"Software Modernization Strategy" – Department of Defense, November 2021
https://dodcio.defense.gov/Portals/0/Documents/Library/SoftwareModStrat.pdf
CISA Zero Trust Maturity Model
https://www.cisa.gov/zero-trust-maturity-model
Cybersecurity Manual – US Department of the Navy, April 2022
https://www.secnav.navy.mil/doni/SECNAV%20Manuals1/5239.3.pdf
Strategic Intent for Cyber Read – DON CIO , Aug 04, 2022
https://www.doncio.navy.mil/ContentView.aspx?ID=15781
"Memorandum on Improving the Cybersecurity of National Security, Department of Defense and Intelligence Community Systems" – NSM-8 Jan 19, 2022
https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
Sonatype DevZone:
https://dev.sonatype.com/
ISTIO
https://istio.io/
CycloneDX & SBOM
https://cyclonedx.org/
Sigstore
https://www.sigstore.dev/

Other References

"Navy on track to deploy Project Overmatch capabilities with carrier strike group in early 2023" – FEDSCOOP Aug 25, 2022
https://www.fedscoop.com/navy-on-track-to-deploy-project-overmatch-capabilities-with-carrier-strike-group-in-2023/
"Joint All Domain Command and Control (JADCs)" – Congressional Research Service, January 21, 2022
https://crsreports.congress.gov/product/pdf/IF/IF11493
"Project Overmatch" Connects Ships, Drones, Missiles & Sensors in Seconds" - Warrior Maven Feb 14, 2022
https://warriormaven.com/sea/navy-project-overmatch
"Why are details of Navy's Project Overmatch so scarce? Adversary eyes, for one" - Breaking Defense Feb 18, 2022
https://breakingdefense.com/2022/02/why-are-details-of-navys-project-overmatch-so-scarce-adversary-eyes-for-one
"Navy to Release Cyber Readiness, DevSecOps Guidelines Ahead of Zero Trust" – GovCIO July 22, 2022
https://governmentciomedia.com/navy-release-cyber-readiness-devsecops-guidelines-ahead-zero-trust
"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
"Oil terminals disrupted European ports hit by cyber attach" – Feb 3, 2022
https://www.euronews.com/2022/02/03/oil-terminals-disrupted-after-european-ports-hit-by-cyberattack

The Security Value of Small and Medium Sized Ports in a Supply Chain Service

by Pinelopi Kyranoudi[1,2] & Nineta Polemi[1,3]

Abstract
This study focuses on explaining key concepts about ports, their characteristics (e.g., size, operational field, infrastruc-ture), potential threats (e.g., interception of sensitive infor-mation, illegal access, terrorism) and attacks (cyber, physi-cal and/or combined), providing an overview of port risk analysis. It also focuses on recording the characteristics of port facilities to document the requirements in small and medium sized ports (SMPs), which act as Supply Chain Service (SCS) providers and/or business partners (BPs). Finally, three attack scenarios are described based on different types of threats, which could cause particularly problematic effects, even paralyzing an entire port and by extension the entire region that benefits from or depends on it.

Keywords
Supply Chain Service, Small and Medium Sized Ports, Cyber Security, Risk Analysis, Threats and Attacks Scenar-ios

1. Introduction

According to ISO 28000:2007 [1], a Supply Chain Service (SCS) "is considered the service that entails a linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport."

By extension, a maritime SCS is a dynamic system consist-ing of a set of interconnected organizations (e.g., port au-thorities, coast guards, customs services, shipyards, marine insurance companies), other critical infrastructures (e.g., energy, transportation, telecommunications), people, ser-vices and other elements aimed at providing a service or product to end users.

In recent years this complex chain has significantly increased its reliance on Information and Communications Technology (ICT) with the aim of providing innovative SCSs in the context of the highly competitive maritime trade [2],[3]. As a result, more and more cybersecurity inci-dents have been recorded in ports, due to the digitization related to the interconnection of Information Technology (IT), Operational Technology (OT) assets, as well as the introduction of new technologies, such as cloud computing, big data, Internet of Things (IoT), etc. Some of the most well-known events, due to their impact, are the cyber attack on port of Antwerp, the NotPetya ransomware on Maersk and the wave of ransomware attacks on the port of Barce-lona and San Diego [3].

There are many ways to categorize ports; for the purposes of this study, the categorization of ports will be limited to two main axes: their size (i.e., small, medium, large)

[1] Department of Informatics, University of Piraeus, Karaoli & Dimitriou Str. 80, 18534 Piraeus, Greece
[2] MAGGIOLI SPA, Via Del Caprino 8, Santarcangelo Di Romagna 47822, Italy
[3] Trustilio B.V. , Vijzelstraat 68, 1017HL Amsterdam, The Netherlands

and the type of SCS they operate (i.e., cargo, passenger, fishing).

Small and medium sized port (SMP) facilities are often the mainstay of a variety of activities in remote areas, such as islands, riverside or peripheral areas. The SMPs pay the most important economic role and have significant impact in the goods' distribution, people mobility and their well-being. SMPs in the small Greek islands, for example, are the main trading areas and economic local providers. Any neg-ative impact on the operation of the SMPs have catastrophic impact to the small regions (e.g., loss of jobs, short-age of basic goods, loss of national safety, loss of lives).

So far, the area of cyber security in these types of ports has lacked attention in existing risk analysis methodologies. This study challenges the belief that SMPs are less important than the larger ones in SCS management and security.

2. Categories and Characteristics of SMPs

There are many ways to distinguish ports, especially the smaller ones, which may be the only communication of some remote areas with the rest of the world and because of this, probably provide more than one SCS. The most com-mon approach to categorizing them is to use metrics based on annual cargo volume or the total volume of ships handled by them. Therefore, for the needs of this study, the categorization of ports will be focused on two main axes; their size and the type of SCS they manage.

More specifically, for size the ESPO categorization will be followed, while regarding the type of SCS that can be managed by the ports their distinction will mainly be made according to that of ENISA. The two categorizations are analyzed below.

According to a European Sea Ports Organization (ESPO) report published in 2010 on the governance of European ports [4], port authorities are classified based on the annual volume of goods handled into small, medium and large.:

- small: 10 million tonnes maximum;
- medium: more than 10 million tonnes and 50 million tonnes maximum;
- large: more than 50 million tonnes.

In 2019, the European Union Agency for Cybersecurity (ENISA) published a study on good practices for cyber security in shipping and in particular in ports [3]. According to this, ports can be distinguished into three main groups, depending on the categories of their maritime SCS infrastruc-ture and services:

- cargo: those that have special infrastructures for the management of operations, such as loading, unloading and storage of goods, sanitary and customs control, etc., and related to any type of cargo, for example liquid, dry, container, etc.;
- passenger: those whose infrastructures are specially designed for the transport of vehicles and passengers and provide reception services for them on ships with parking areas, passenger corridors, bars/restaurants, etc., e.g., serve ferries or Roll-on/Roll-off (Ro-Ro) ships, where the goods are transported in trucks and lorries;
- fishing: those which provide services related to fish-ing, through their special infrastructures, such as the reception of fishing vessels, loading and unloading, inspection, storage and cooling of catches, etc.

However, a small port facility may have additional roles due to its uniqueness in the area, such as serving Navy or Coast Guard vessels. By the same logic, the SCS that can be served by an SMP are from passengers on liners, private boats and yachts, boats and fishing trawlers, to goods and materials, such as for earthworks and construction works. The SCS that can be managed by an SMP is not limited in terms of its distance or the value of the goods transported, but only in terms of the volume of the goods, the infrastructures and the systems used. For example, a cargo of electronic devices could be transported from China or America, chocolates from Switzerland or diamonds from Africa, but it would be impossible for a ship carrying liquefied gas or containers to dock and unload its cargo, because of the shortcomings of its infrastructure, such as large terminals, special cranes or water depths.

Regarding the legal and regulatory framework that applies to SMPs, "all the necessary regulations apply to both small and large ports and the cost of compliance can be dispro-portionately high," as Howard Holt, director of Seaports, reports [5]. The same applies to standards, as they are de-signed to cover the full range of infrastructure and processes that may need to be secured.

3. Potential Threats and Attacks

Port facilities are places through which countless crowds of people pass every day and a large volume of goods are traded worldwide and, by extension, provide equally great economic, political or even military benefits to the respective region. For this reason, they can become the target of a multitude of criminal actions. However, the losses a port can suffer from maritime crime are not only financial, which are often immediate. Costs may include potential loss of life, reemployment, retraining, redesigning functions, spending time with law enforcement such as the Coast Guard, lawyers, etc. or even the mass media. This means that the costs include port exposure and by extension exposure to liability, loss of goodwill and reputation, loss of business and/or increased insurance costs. So overall there is a big impact on productivity [6].

The most important physical threats that a port can face are fraud, for example, through false customs declarations for financial gain, sabotage for military, political or ideological reasons, vandalism, theft of property, unauthorized access to its premises, vehicles and equipment or even unauthorized port entry via vehicles. In addition, common

physical threats are terrorism for political, ideological or religious reasons, hacktivism, coercion, extortion or corruption, as well as piracy, any sort of illegal action or other crime. Finally, environmental or natural disasters are always potential physical threats [3].

As technology evolves, ports are becoming increasingly complex environments that include both onshore and offshore activities and systems, while combining the physical and digital worlds [7]. This results in them facing additional cyber threats. Such can be mediation and monitoring of communications and systems or espionage, interception or causing functional problems in systems through various cyber attacks, such as denial of service (DoS), entry of malicious software (malware), social engineering, etc. In addition, they pose intentional threats, such as the leakage or deletion of information by employees, system errors, etc., as well as failures or malfunctions. Finally, power or network outages, as well as staff shortages could paralyze the opera-tions of the entire port [3].

Ports play an important role in SCSs and their infrastructures have interdependencies at multiple levels, such as local, national or international. In this context, they closely interact with all the factors of a SCS, i.e., SCS provider, SCS business partners (BPs), SCS physical and IT/OT/IoT assets, various authorities. This results in cyber-physical threats such as eavesdropping, piracy, interception, malicious activity and abuse, accidental damage, physical attacks as well as system failures and malfunctions, internally, externally and/or pervasively [8].

In a port, as in a SCS, there are different services that have been developed for the smooth running of business activity. All services are affected by threats that have various con-sequences if a malicious user exploits them. According to [3] there are specific categories of effects that may occur due to threats and attacks in such a space and environment. Such may be the shutdown/paralysis of the port operations, human injury or death, theft of cargo/goods, theft of sensitive/critical data, financial loss, illegal trafficking, theft of money/fraud, system failures/disaster, loss of competitiveness/tarnished reputation and/or environmental disaster. A further category of impact is added to this work; that of social/commercial/political disruption.

The impact of cyber-attacks can extend to a SCS, even on a physical level, which, depending on the type of good being transported, can be more or less devastating. Examples of dangerous goods are classified by International Maritime Organization (IMO), according to the main risks they pose during transport (e.g., explosive substances and articles, gases, radioactive material, etc.) [9].

4. Attack Scenarios

According to the formula, risk is equal to the product of the probability of an event occurring times the impact it will have (Risk = Probability x Impact). This means that proba-bility and impact are inversely proportional to each other, while both are proportional to the risk itself. In other words, the greater the probability of something happening or the impact it will have, the greater the risk. Essentially, any threat, cyber or physical, that can happen to a large port can be adapted to the goods of a smaller one. The main difference is that in SMPs there is often a resource con-straint, which increases the degree of impact, or a reduced budget, therefore insufficient security measures, which increases the probability and consequently leads to increased risk.

For a risk to manifest, a threat must be found to match a vulnerability in order to have an impact. In other words, a malicious user must successfully exploit a vulnerability. Next, three attack scenarios are described based on different types of threats, which could cause particularly problematic effects, even paralyzing the entire port and by extension the entire region that benefits from or depends on it.

4.1. SQL injection attack on a database of a ferry ticket purchase website (cyber threat)

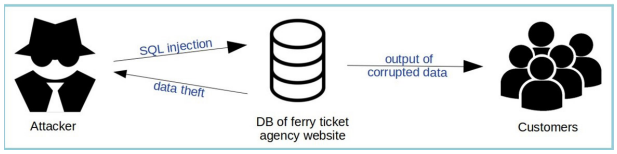
Assume that someone malicious (e.g., competitor, spy) via SQL injection gains access to the database (DB) of the ferry ticketing website of a small company that owns a limited number of passenger cruise ships that operate from the port of a small island to that of a larger one and vice versa, three times a week. The attacker compromises the confidentiality, integrity and/or availability (CIA) of passen-

Table I: Elements of scenario 4.1

1.	Maritime SCS	Transportation of passengers and/or patients
2.	SCS Provider	Small ferry company/ticket agent
3	SCS BPs	i. Small island medical center ii. Large island hospital/clinic iii. Port authority
4.	SCS Assets	a. Digital: ticket agent website (DB, server, etc), passenger data b. Physical: vessel, medical centers, people (passengers, employees, crew, port staff), SMP
5.	Threats	a. Cyber: SQL injection, illegal access b. Physical: -
6.	Impacts	• Patient health burden / loss of life • Interception of personal data and payment details • Damage to company reputation • Financial loss of the company • Social, commercial and political disruption

ger data by gaining access to their personal information and their debit/credit card or other means of payment. The attacker can additionally create dummy passenger bookings in the DB with the aim of disrupting their transport and disorienting the Coast Guards. This tourist ship is also used by the junior doctor or the general practitioner of the small island's medi-cal center for transfers of patients to the hospital of the larger island, patient referrals to the Emergency Department or to specialist doctors in general. Thus, it could either delay a transfer, as it would eventually have to be done in a different way (e.g., a special Coast Guard vessel or helicopter) or delay a referral, which could not be done in a different way, resulting in the health burden of the person needing medical care or even death. Such an incident would cause loss of human life, heavy damage to the company's reputa-tion, financial damage, political unrest.

The elements characterizing the above scenario are summarized in Table I and it is depicted in Graph I.



Graph I: Depiction of scenario 4.14

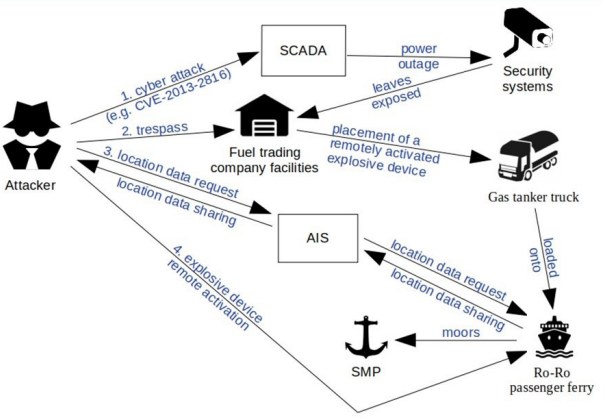
2. Terrorist act on a gas tanker truck inside a liner (cyber-physical threat)

An SMP located within a natural bay, when free from scheduled coastal shipping routes, is often used by naval vessels when they are required to anchor temporarily to hide from the radar of enemy ships while patrolling the surrounding area. The enemy, unable to approach the port with its own warship, attacks the Supervisory Control And Data Acquisition (SCADA) system related to the supply of power to the gas warehouse and tanker trucks refueling facilities of a fuel trading company. This causes a power outage paralyzing all security systems in the area. Members of the terrorist group enter the site and place a remotely activated explosive device on a gas tanker truck. The tanker truck then follows its established route, for which it must be loaded onto a Ro-Ro passenger ferry. The ship, in turn, tempo-rarily moors at the specific SMP for boarding and disembarking passengers, as it is an intermediate destination of its itinerary. Then, knowing the precise location of the ship through the Automatic Identification System (AIS), which shares the data publicly, the terrorist group remotely activates the explosive device, with the risk that the initial explosion could cause a larger explosion if extended and in the ship's fuel tanks. This results in injuries and loss of human life, as well as the destruction of the port or even part of the residential area around it with all this implies for the functionality, economy and tourism of the area, while at the same time alerting the national security and the navy loses an important cover position for its ships, thus making its work on patrols more difficult.

The elements characterizing the above scenario are summarized in Table II and it is depicted in Graph II.

Table II: Elements of scenario 4.2

1.	Maritime SCS	Transportation of fuel
2.	SCS Provider	Fuel trading company
3.	SCS BPs	i. Shipping company that owns the large ship of the line ii. Shipping company to which the oil tanker vehicle belongs iii. Port authority
4.	SCS Assets	a. Digital: fuel provider systems (SCADA, PLC, etc.), AIS b. Physical: fuel tanker vehicle, ship, people (passengers, employees, crew, port staff), SMP
5.	Threats	a. Cyber: attacks on fuel provider systems (SCADA, etc.) b. Physical: trespass, explosion
6.	Impacts	• Injuries/loss of life • Destruction of the port and potentially part of the surrounding residential area/damage to the functionality, tourism and economy of the area • Jeopardizing national security, reputation of the country • Patient health burden/loss of life



Graph II: Depiction of scenario 4.2

4.3. Attack on oil tanker's HSMS System (cyber-physical threat)

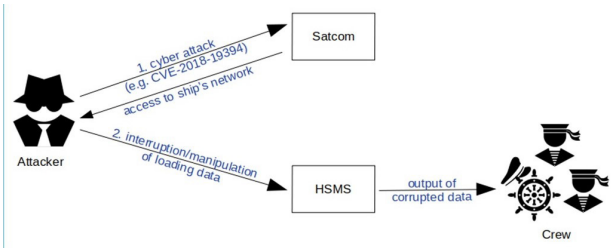
There are ports of small island regions that serve tankers carrying oil, which is vital for residents as it is used to generate energy. The transport of this good, of course, is also common in larger ports, in order to supply factories, gas stations, etc. If the process of loading and unloading these ships is not done carefully enough and the neces-

sary safety measures are not taken, then oscillations are created capable of splitting the ship in half and consequently sinking. For this reason, the Hull Stress Monitoring System (HSMS) is used to help the crew ensure that design specifications are not exceeded, hogging and sagging are avoided and the ship balances more correctly by sending audible signals to the bridge if excessive stress is detected on the ship's reefs. Suppose a malicious crew member gains access to the ship's network and then to the HSMS in order to intercept or manipulate the cargo data fed to and from the monitoring system. As the crew fully trusts the system during the unloading process, they believe that everything is going well, until the ship from the significant deformations in its hull caused by the excessive pressures breaks in two and finally sinks in the harbor. Alternatively, a malicious person could gain access to the ship's network remotely, by hacking the Satellite Communication (Satcom) system. The sinking of the ship can cause injuries or even loss of human life, loss of energy and all that this entails due to the loss of oil, environmental disaster, port malfunction until cleared, as well as damage to the reputation and, by extension, financial loss of the shipping company, but also of the area itself, due to the reduction/loss of tourism.

The elements characterizing the above scenario are summarized in Table III and it is depicted in Graph III.

Table III: Elements of scenario 4.3

1.	Maritime SCS	Transportation of oil
2.	SCS Provider	Oil provider
3.	SCS BPs	i. Shipping company ii. Transport company iii. Port authority
4.	SCS Assets	a. Digital: HSMS, Satcom system b. Physical: oil, ship, port and area environment, people (passengers, employees, crew, port staff), SMP
5.	Threats	a. Cyber: attack on the ship's HSMS/remote attack on the ship's Satcom system b. Physical: malicious crew, illegal access of natural port resources
6.	Impacts	• Injuries/loss of human life • Environmental disaster • Loss of energy due to the loss of oil • Port malfunction until cleared • Damage to the reputation of the shipping company • Financial damage to the company and also to the island due to reduction/loss of tourism



Graph III: Depiction of scenario 4.3

5. Conclusions and Future Work

In this study, basic concepts related to ports are analyzed, such as the categories used to be distinguished and their characteristics, such as their size, operational scope, infra-structure, focusing on small and medium-sized ports (SMPs). An overview of a brief port risk analysis is provided citing potential threats such as interception of sensitive in-formation, illegal access, terrorism, as well as cyber, physi-cal and/or combined (cyber-physical) attacks and the im-pacts they can cause. Based on different types of threats, three attack scenarios are presented, which show how par-ticularly problematic effects can be caused to SMPs by ex-ploiting vulnerabilities in maritime supply chain services (SCSs) capable of crippling an entire port and by extension the entire region benefiting from it.

All ports are economically and strategically valuable to sur-rounding areas, especially SMPs, as there are areas that are completely dependent on them. All of the above leads to SMPs acting as hubs of an SCS like major ports, since the delivery of goods has no borders. The fact that SMPs have the same types of needs, work under the same laws and regulations as major ports and can be exposed to similar threats and attacks challenges their day-to-day safe and secure operation, due to the limitation of financial resources and the expenses of security management. Risk analysis is a process that usually requires deep knowledge of the infra-structure and factors that can affect the operation of an organization, so cybersecurity experts are needed to model and calculate risk.

There is a need for a methodology and a corresponding tool that can provide a holistic solution of highly automated cyber risk assessment and enable the correlation of cyber and physical threats. Our future research work leans to-wards this direction and aims to create a methodology and a tool that can be easily used by SMPs as well.

Acknowledgment

This work is supported by Partnership Agreement for the Development Framework 2014-2020, Operational program "Competitiveness, Entrepreneurship & Innovation" (EPA-nEK), in the context of the project CYSMET: Integrated, Dynamic & Collaborative Risk Management System for Maritime Transport & Supply Chains, with project number: T2EΔK – 03488. The authors also thank all partners of this project as well as the University of Piraeus, Research Centre (UPRC) for its continuous support.

References

[1] ISO 28000:2007 international standard, “Specifica-tion for security management systems for the supply chain”, 1st Edition 2007-09. Online available: https://www.iso.org/standard/44641.html, accessed on September 14 2022.
[2] ENISA, “Cyber security aspects in the maritime sec-tor”, December 19, 2011. Online available: https://www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1, accessed on September 14 2022.
[3] ENISA, “Port Cybersecurity - Good practices for cybersecurity in the maritime sector”, November 26, 2019. Online available: https://www.enisa.europa.eu/publications/port-cybersecurity-good-practices-for-cybersecurity-in-the-maritime-sector, accessed on September 14 2022.
[4] ESPO, “The ESPO Fact-Finding Report”, 2010. Online available: https://www.espo.be/media/espopublications/espofactfindingreport2010.pdf, accessed on September 14 2022.
[5] “A cluster initiative: Small and Medium Sized Ports as Hubs for Smart Growth and Sustainable Connectivity”, 2 Seas Magazine, November 2014. Online avail-able: http://archive.interreg4a-2mers.eu/2seas-files/page_ext_attachments/1602/PAC2_2SEAS_MAGAZINE_EN.pdf, accessed on September 14 2022.
[6] U.S. Department of Transportation, “Port Security: A National Planning Guide”, May 21, 1997. Online available: https://rosap.ntl.bts.gov/view/dot/13693, accessed on September 14 2022.
[7] The Institution of Engineering and Technology, “Good Practice Guide – Cyber Security for Ports and Port Systems”, January 27, 2020. Online available: https://www.gov.uk/government/publications/ports-and-port-systems-cyber-security-code-of-practice, accessed on September 14 2022.
[8] ENISA, “Guidelines - Cyber Risk Management for Ports”, December 17, 2020. Online available: https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports, accessed on Sep-tember 14 2022
[9] IMO, “International Maritime Dangerous Goods (IMDG) Code”, 2020, Corrigenda May 2022. Online available: https://wwwcdn.imo.org/localresources/en/publications/Documents/Supplements/English/QM200E_180522.

Pinelopi Kyranoudi has obtained her master’s degree in Security of Information and Communication Systems from the School of Engineering of the University of the Aegean (Dept. of Information and Communication Systems Engineering). She served as Network and Information Security Officer at the European Union Agency for Cybersecurity (ENISA) contributing: to five publications in the areas of Cybersecurity in Maritime, e-Health, and National Cybersecurity Strategies; to the creation of web tools, and to the organization of EU Cybersecurity events. She worked as a Web and Application Developer at Express Publishing S.A. and as IT Security Engineer at Cosmote S.A., among others. She is currently conducting her Ph.D studies in the Cybersecurity field at the University of Piraeus (Dept. of Informatics). She holds a position as Cybersecurity researcher at Maggioli SpA. Her research interests are in the field of Cyber Security, especially in Maritime, IoT, and Threat Intelligence

Professor Nineta Polemi has obtained her Ph.D. in Applied Mathematics (Coding Theory) from The City University of New York (Graduate Center). She is an Associate Professor in the University of Piraeus (Dept. of Informatics) teaching cryptography, security of ICT systems, port security and e-business & innovation. She is a member in the European Network of Information Security Agency (ENISA) high level expert groups on Artificial Intelligence and working group on Risk Assessment. She has served as Programme Manager and Policy Officer in the
European Commission, DG CONNECT, Unit H1: Cybersecurity Technologies & Capabilities. She held teaching and research positions in Queens College, Baruch College of City University of New York, the State University of New York and Université Libre de Bruxelles (ULB)- Solvay Brussels School. She has acted as President of the BoD in the security consultancy company, Expertnet. Her research interests are in the fields of security and cyber defense. She has over one hundred publications in the above areas and has organised numerous security scientific international events. She has received many research grants from various organizations such as the Danish Research Foundation, MSI Army Research Office/Cornell University, IEEE, State University of New York (SUNY), and The Graduate School of City University of New York (CUNY). She has been project manager (PM) / technical manger (TM) in security projects of various programmes such as National Security Agency (NSA), NATO, Dr. Nuala McGann Drescher Foundation, Greek Ministry of Defence the last three (5th, 6th, 7th) Framework Programmes of the European Commission (E.C.)

A Holistic Approach for the Dependability Enforcement of Cyber & Power Systems on future MVDC Ships

by Massimiliano Chiandone, CDR Marco Merola, Andrea Vicenzutti, Giorgio Sulligoi, CDR Gianluca Maria Marcilli

Abstract — Modern shipboard power systems are complex systems that rely on automation for their correct operation. The power and the control layers are strictly interrelated, and the data infrastructure is as critical as the power one. Future power systems exploiting resilient architectures (like the zonal medium voltage dc one) will rely more and more on controlled components (e.g., power electronics converters) to achieve their operational advantages, thus increasing the integration among data and power infrastructure. In such a context, the cyber security of the data infrastructure constitutes a critical point for the correct operation of the ship. Existing approaches mostly focus on enforcing the dependability on the cyber infrastructure, taking the power infrastructure as a given. However, ensuring the dependable operation of the power system means ensuring the supply of the onboard critical loads, which directly depends on the power system architecture, its design, and how it is operated. Therefore, it is critical to evaluate the effect on the power system of the malicious actions performed on the data infrastructure, and consider the possibility of acting on the power system itself to avoid or react to the threats (i.e., designing a dependable power system). In this paper such a holistic approach for the dependability enforcement of integrated cyber & power systems on ships is presented, discussing some of the solutions for the actual power systems and presenting an overview in regards to future medium voltage dc power systems.

Keywords—component, formatting, style, styling, insert

I. INTRODUCTION

In modern ships, the Integrated Power System (IPS) is a core component because it supplies both onboard loads and propulsion (either in full electric or hybrid configuration). Fig. 1 depicts a notional IPS of a cruise ship, which is at present, one of the most complex examples of shipboard power systems. In such an IPS, two separable main switchboards operating at medium voltage (MV) are powered by a total of four generators. The MV distribution directly supplies the higher power loads, such as propulsion variable frequency drives, while low voltage busbars fed through transformers are used for the low power users. Being the IPS an islanded system with high installed power (tens of MW), ensuring Power

Quality (PQ) and Quality of Service (QoS) is a demanding task [1]. Therefore, proper system design and control are capital. Regarding the latter, a multilayered hierarchical control system is used, which relies on several devices and automation channels to correctly operate. Nowadays, IPSs are evolving due to the introduction of more demanding requirements (e.g., mission and payload related ones for naval vessels, or pollutant emissions related ones for merchant ones), pushing towards the use of new architectures and innovative subsystems. The most performing architecture actually conceived it based on the Zonal Electrical Distribution System (ZEDS) approach, using MV direct current (MVDC) [2].

The modern implementation of control architecture in power systems (IPS included) is made using digital systems. Indeed, from analog controls technology has moved on, rewriting/redesigning them in discrete time and implementing them digitally on controllers specifically dedicated to automation. The increase of the computational capacity in these devices allows to implement more and more control functions, and to integrate more and more sophistication in a single device. The resulting increase in complexity in developed control software implies that low-level programming languages are practically no longer usable, and there is a standardization in high level development languages and platforms. Specifically, the tendency is to use Central Processor Units (CPU) with standard 32- and 64-bit architectures, to allow for great flexibility, offering virtual memory management and multitasking. These platforms require a real-time operating system (RTOS) for proper management of hardware and timing requirements, which enables using standard software platforms (e.g., cryptographic suites, communication protocols, software for hardware management)

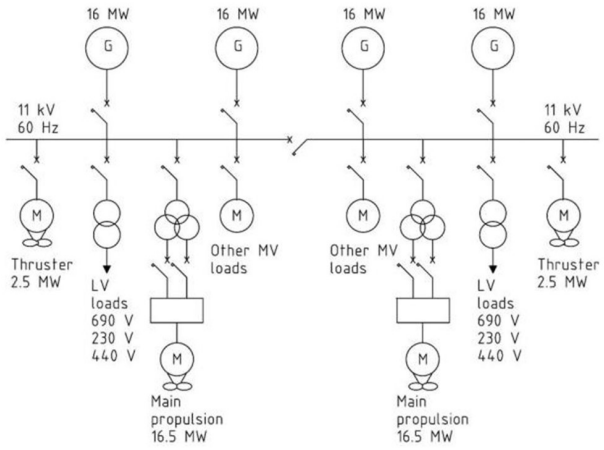


Fig. 1. All-Electric Ship: Integrated Power System layout [1]

[3]. On the other hand, the complexity of the IPS control software architecture poses security and reliability issues. In this paper, a unified approach to dependability of complex system that contemplates the hardware and software structures in a single model is presented.

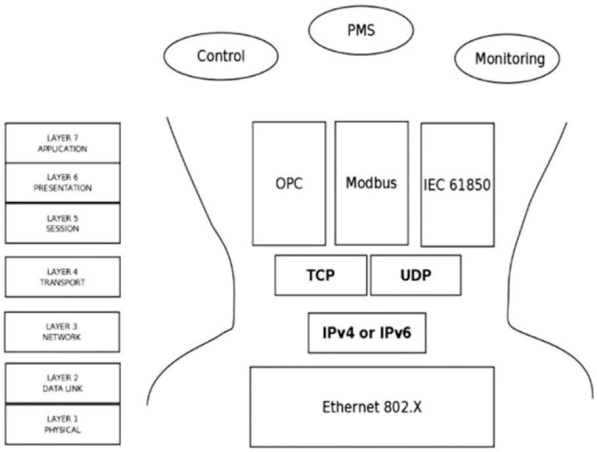


Fig. 2. Protocols used for control and energy transactions. The central role of IP stack.

The paper is organized as follow: in Section II common aspects between hardware and software errors are detailed, Section III deals with some security issues related to protocols communication in naval systems. In section IV the holistic approach is presented, and in Section VI is shown the help of simulations in the application of the holistic approach is presented.

II. HARDWARE AND SOFTWARE FAILURES

Due to the increasing pervasiveness of power converters in modern IPSs, their operation depends less and less on the physical laws of electricity and more and more on the control system algorithms. The latter are performed by dedicated CPUs and exchanged data through a communication infrastructure. Thus, two main components of a shipboard power system can be recognized: the power (physical) infrastructure and the cyber infrastructure. The latter consists of all the software that implements the algorithms and protocols to transmit data among devices. All this can be summarized generically as continuous growth in the digitalization of IPSs. In such highly digitalized systems, the software component assumes a role comparable (due to the effects it has on the plant) to those of the hardware component. In both these elements, events may occur that lead to system degradation. Suppose only the malicious events due to an intentional fraudulent action are considered. In that case, the cyber part can be subjected to errors due to malware, errors in the code, cyber-attacks, intentional actions on controls or on communication channels, and fraudulent actions on sensors and actuators. Intentional malicious events on hardware components are essentially physical damage to equipment or control actions that bring the devices to an operating point outside the physical limits of the device. Both kinds of events generally lead to a failure that causes abnormal behavior of the IPS and, therefore, to a degradation of its performance and Quality of Service (QoS). In such a context, it is clear that cyber infra-

structure security constitutes a critical point for the correct operation of a ship. Existing approaches mostly focus on enforcing the dependability of the cyber infrastructure, taking the power infrastructure as a given. However, ensuring the dependable operation of the power system means ensuring the supply of the onboard critical loads, which directly depends on the power system architecture, its design, and how it is operated. Therefore, it is critical to evaluate the effect on the power system of the malicious actions performed on the data infrastructure and consider the possibility of acting on the power system itself to avoid or react to the threats (i.e., designing a dependable power system). In this paper, such a holistic approach for the dependability enforcement of integrated cyber & power systems on ships is presented, discussing some of the solutions for the existing power systems and presenting an overview in regards to future medium voltage dc power systems.

III. CYBER SECURITY INFRASTRUCTURE IN IPSs

A. Communication protocols in actual and future IPSs

Communication protocols have been standardized on a few models, one of the most used is TCP/IP, which has also entered the field of automation systems [4]. The convergence of General Purpose Processors (GPP) and IP-based communication protocols has also given way to the use of different software platforms (an example is the use of IoT platforms also in the field of automation [5]). As regards the communications between the different subsystems, in the last 20 years, there has been a convergence towards the Internet Protocol (IP), which has become the most used transport layer. In physical levels 1 and 2 of the ISO-OSI model [6], there has been a proliferation of different physical media for the various domains currently standardized in one of the many Ethernet protocols of the IEEE802 family. Different specific protocols have been adopted for each domain in the higher application levels. Modbus, IEC61850 and OPC are perhaps the most common protocols used for ship automation and are used mainly over IP. IP version 4 does not have any security mechanisms, thus, data encryption is adopted at the application level, where deemed necessary, possibly through public key infrastructures and with the Transport Layer Security (TLS) protocol. Power Management System (PMS), hierarchical control and monitoring of the IPS are implemented on top of those protocols.

In the new power distribution architectures, including MVDC ZEDS, the power flows are even more dependent on the controls of the converters. Therefore, there is a direct relation with the behavior of the CPUs transmitting data and commands through the data protocols. More sophisticated hierarchical controls can be implemented in this type of IPS, such as zonal control. Nevertheless, the communication architecture still relies on the Fig. 2 structure.

B. Cyber security of the data infrastructure

The growing use of distributed controls and communication protocols (in cyber interactions within the electrical system) leads to greater control over its operation. However, it can also lead to a general weakening of the system against software errors, communications errors, or fraudulent actions taken against the system through its cyber infrastructure. The security by design paradigm must become preeminent with respect to generic prevention of every possible type of cyber-attack. Two types of problems can be considered in an IPS: software problems (due to software malfunction and errors in data transmission) and hardware problems (therefore, the fault of a physical device). For each of these two types, non-voluntary (due to errors and misconfigurations, aging of components or breakage) and voluntary events can be considered. Concerning the cyber infrastructure, the software problems can be caused by the insertion of malicious code or the fraudulent insertion of incorrect data capable of affecting the correctness of the operation of the entire system or part of it. All types of errors can lead to

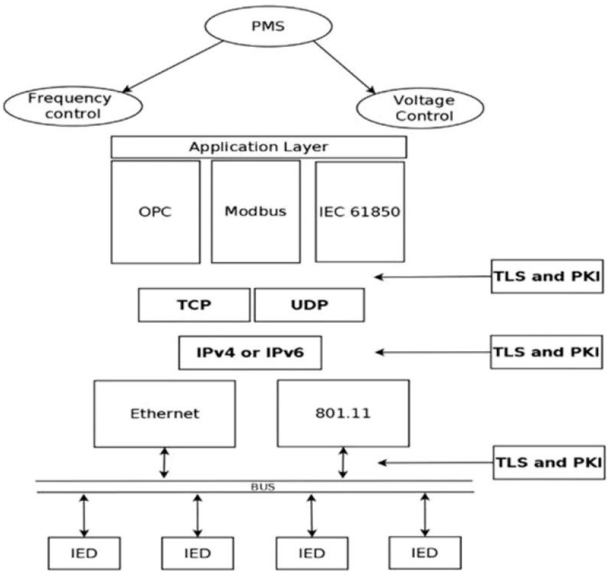


Fig. 3. Data management architecture for the grid control with three different levels where cryptography can be applied.

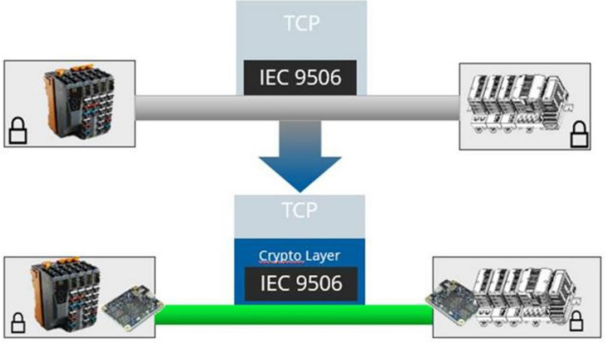


Fig. 4. Crypto layer for real-time comms.

a failure that causes an incorrect operation which in turn can lead to a lowering of the quality of the service offered by the system.

C. Approaches to increasing the security of cyber infrastructure and related critical points

An increase of security level in communication channels can be achieved using the encryption of transmissions. The encryption can be implemented at different levels (Fig. 3), but the most common are: at the physical layer, at the network level or, more generally, at the application level.

At the application level, message encryption can be implemented directly on the CPUs that control the static converters that interface with the PMS or secondary controls. Provided the processors support this possibility, encryption should be done using standard encryption software suites.

Some aspects of this infrastructure have effects on the vulnerability of the system:

• the use of standard libraries and protocols brings the system at the state of the art but only if it is reg–ularly updated (by constantly applying all the necessary patches). In the absence of an update, you are exposed to known and well-documented attacks;

• the use of modern cryptographic suites has a computational cost that effectively excludes some proces–sors (i.e., microcontrollers) from being usable;

• the addition of a software component increase es the complexity of the system (and therefore affects its safety) in the same way as adding a new hardware component.

The increased complexity and the computational cost due to the cryptography layer can be considered non-sustainable by the existing OT devices (e.g. PLC, RTU), especially in near real-time and mission-critical applications. Dedicated crypto devices (Fig. 4) could represent an affordable solution: principal design requirements are low latency encryption-decryption processes for real-time coms, filtering IP and ARP messages, and easy setup over existing systems. The crypto-layer must protect from external, extraneous or compromised OT/IT devices connected to the control network, preventing spoofing, tampering and other malicious activity. Combined with a behavioural Intrusion Detection System that analyses network traffic and software and firmware configuration, the complexity of an effective cyber attack increase dramatically.

In general, a perfectly secure system cannot be built; hence it is always necessary to consider a possible failure in the cyber section of the system. However, such failure can or cannot affect the IPS operation depending on its design, making it necessary to study both the cyber and the physical sections of the system as a whole.

IV. A HOLISTIC APPROACH TO THE DEPENDABILITY ENFORCEMENT OF CYBER-PHYSICAL SYSTEMS

A. Effect of the cyber infrastructure on the physical one

Existing approaches mostly focus on enforcing the dependability of the cyber infrastructure, taking the power infrastructure as a given. However, it should be considered that not all possible attacks can be faced only by increasing the security of the HW and SW architecture of the former. Given the complexity of present control systems used in electrical power systems, it must be assumed that some security flaws are always present. If they are not found during system construction, they could be discovered during their useful life. In critical systems, a continuous security assessment and a system update activity must therefore be envisaged for the cyber infrastructure (e.g., updating the software whenever new exploits are discovered), as happens with their physical part with predictive maintenance. Despite the preventive corrective actions, the possibility of fraudulent actions must be always taken into account. Thus, the evaluation of their effect on the physical part of the system is needed, considering not only the single affected subsystem, but all the system as a whole. This is a complex task, due to the several interrelations between cyber and physical parts, which are already complex by themselves.

Following a cyber-attack (for example, an attack that modifies the power system control layer by injecting false data into it), actions on the hardware must be taken to mitigate its effects. In a power system a cyber-attack can tamper with the references in the automatic voltage regulator of one or more generators, bringing them to a point outside the safety values and causing their disconnection. The result is equal to a physical fault, leading to the failure of the power system if this has not been correctly designed to manage such an event. Malicious actions of this type can thus be represented by using their final effect on the power system modeled as a fault of one component or subsystem, and then assessing the capability of the system to resist such fault. Through this approach it is possible to enforce the dependability of these systems, by applying an integrated methodology that acts both on the cyber and the physical sections.

B. Applying dependability theory to IPS analysis

The dependability theory consists of a set of definitions and concepts for analyzing and managing the origin of faults, errors, and failures, determine their effects on a system, and set appropriate countermeasures, using a systematic approach. The general theory corpus originated from the computing and communication systems area, and is consistently and exhaustively depicted in literature (e.g., [7][8]). Thanks to its generality,

it is possible to extend its application to systems aimed at performing different tasks, like ships' IPSs [9],[10]. This can be done because the latter are complex systems, i.e., a set of components that, once assembled, function as a single entity with a given functionality. In fact, an IPS is a set of electrical, mechanical, and control components that are designed and built to provide power to the onboard loads with a specified QoS (defined by the design requirements). Given the size of a ship's IPS, the complexity of designing it dependable and secure is evident. From a practical point of view, several tools have been developed to aid in this task, like Failure Mode and Effects Analysis (FMEA) or Fault Tree Analysis (FTA), to mention two of the most famous only [10]. Although all the tools aimed at evaluating dependability or its specific attributes (reliability, maintainability, availability, etc.) are useful, the ones capable of providing a quantitative evaluation (i.e., calculate numerical indexes) are the most powerful ones. As an example, FTA method allows building failure-trees of specific failure events, and apply simple mathematical equations to evaluate numerical indexes starting from failure data (e.g., failure rate, MTTF, MTTR, etc.) [11].

By considering cyber originated events by means of their effect on the power system hardware, it is possible to include cyber-attacks in the dependability analysis of a power system. Thus, the evaluation of the overall IPS performance is enabled, not only in respect to physical faults, but also in respect to cyber originated events. It is relevant to notice that different types of cyber-attack and related countermeasures can lead to the same physical effect. As an example, a cyber-attack may be aimed at a generator, and its success leads to protection intervention, uncontrolled behavior, or the machine stopping producing power. In either case, at some point at least one electrical protection (possibly the ones in the main switchboard, if the generator's ones are compromised by the cyber-attack) intervene, disconnecting the generator from the power system. On the contrary, the cyber-attack may not be directed immediately to the generator, but a loss of security in the data communication infrastructure is identified by a suitable method. In such a case a possible solution is to stop relying on the compromised equipment, thus stopping the generator as a preventive measure. In either case, from the electrical point of view the effect is a stopped generator, which is considered as a fault in the power station. From this point onwards, it becomes possible to consider the effect of the cyber-attack on IPS operation with different tools, using either an estimate of the cyber-attack probability of occurrence (calculated through a vulnerability assessment) or setting a 100% probability to evaluate the worst case.

It is relevant to notice that the evolution of a power system towards a failure is a dynamic process, and not a Boolean one. Thus, it is possible to act on the failure process (to stop it) not only before its occurrence, but also during it and at different time instants. This can be properly highlighted by means of mathematical modeling and simulation of the physical system. Focusing on IPSs, suitable power system dynamic simulators can be built, at different levels of detail depending on the specific power system and the analysis goal. Then, the simulation results, in conjunction with the considered critical events, can be used to define enforcing techniques to the system, as fault prevention, tolerance, or removal. The result of this process is the modification of the IPS design, so that the problems discovered are solved and a more dependable system is obtained. The latter can be done changing the system design, if possible, or introducing modification to an existing system [11]. For a given identified critical event, the modifications can be done on the physical part of the IPS, on the cyber part, or on both of them.

V. MATHEMATICAL MODELING AND DIGITAL TWINS FOR CYBER SECURITY TESTING AND DEPENDABILITY ENFORCEMENT

The use of software simulators has become an established practice in design. Through the implementation of mathematical models of physical systems, it is possible to calculate with great precision the system's dynamic response to various inputs to define a design capable of complying with the relevant requirements before its construction [12]. This possibility is useful in the design phase, since it can reduce the risk and the need of relying on expensive experimental phases. As an example, it is possible to check the correct coordination between control system and protections of an IPS, and plan actions to face emergency situations or to increasing flexibility, defining the correct control system's parameters and support crew training [13]. The physical system modeling can include a section of the cyber infrastructure, to provide an integrated assessment tool to test the security of a power system. Moreover, the mathematical model can be compiled in a real-time environment and executed in parallel with the real system continuously exchanging data with it, constituting the so-called digital twin. If properly built and managed, the latter can be a critical asset for enforcing system's dependability. Indeed, it can be used to identify cyber-attacks and other malicious actions by comparing the real component behavior and the expected one given by the digital twin.

In the following, two examples of how the proposed approach works are given, considering actual and future IPSs architectures.

A. Actual IPS example

To provide an example in regards to an actual IPS, it is possible to refer to [11]. While in such paper

only the physical components' faults where applied, it is still possible to use such a case by considering a cyber-attack that leads to a component or subsystem fault. Then, the same process for the analysis and dependability enforcement can be applied. E.g., it is possible to assume a cyber-attack affecting the data communication infrastructure of the ship, causing a loss of security in the data channel between the PMS and one generator. The result (either by the attack itself or as a security measure after the attack is identified) is the shut off of the compromised generator. From this point onwards the cyber section of the system is not concerned anymore with the resulting physical system behavior, until specific actions by the PMS are to be adopted to maintain the system operation. Depending on the power system design and operation, the effect of the generator shut off may or may not be critical.

In the [11] case study, the power system fails after a short amount of time due to overloading of the remaining generators. Specifically, Fig. 5 and 6 show frequency and active power output of the remaining DG

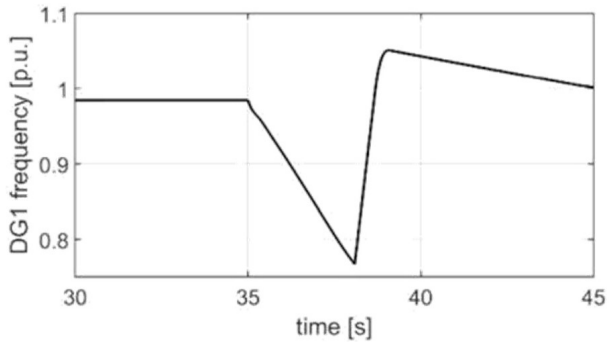


Fig. 5. Frequency of a running generator [11]

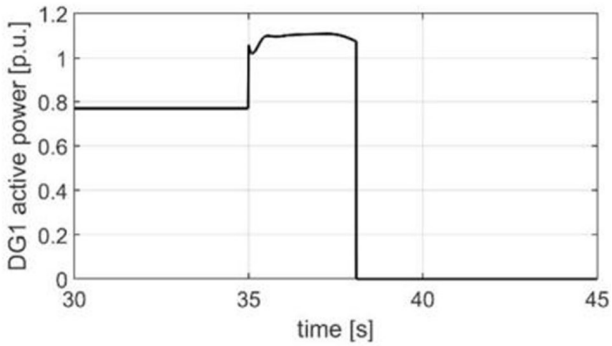


Fig. 6. Power of a running generator [11]

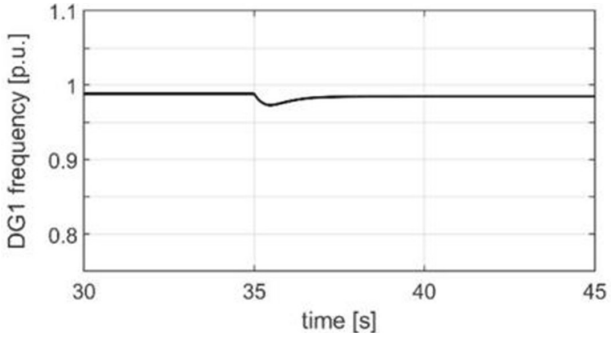


Fig. 7. Frequency of a running generator, with one more active DG [11]

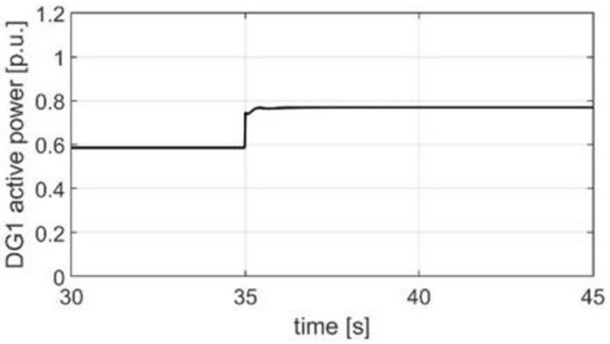


Fig. 8. Power of a running generator, with one more active DG [11]

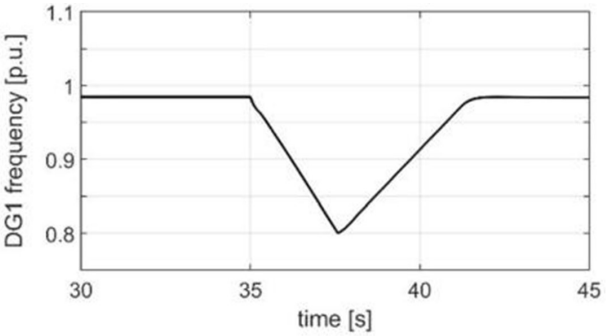


Fig. 9. Frequency of a running generator, with load-shedding [11]

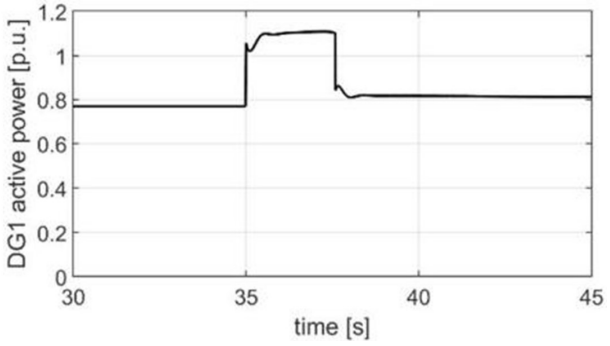


Fig. 10. Power of a running generator, with load-shedding [11]

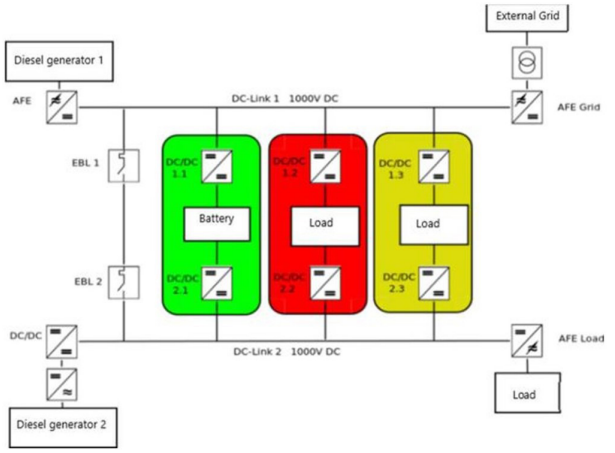


Fig. 11. Zonal DC electrical distribution under study.

after the shut-off of one running DG at t = 35s, and it is evident the failure of the latter due to the intervention of the under-frequency protection (caused by the overload). However, if an additional DG was operating prior to the event (operational-based solution, Fig. 7 and 8), or if a

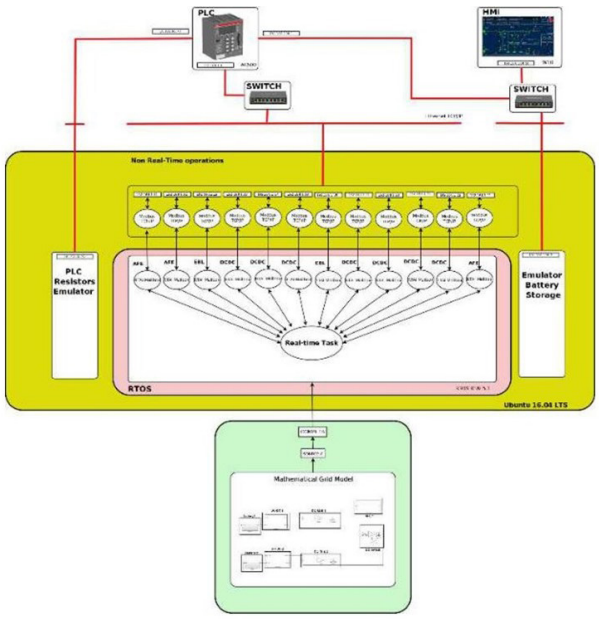


Fig. 12. HIL communication layout: each converter in the mathematical model has its own modbus interface task.

load-shedding function was implemented (control-based solution, Fig. 9 and 10), the system would have survived. It is worth noticing that the former solution does not require any additional action by the PMS, thus being possible also in presence of a fully compromised data communication system. However, it has a significant impact on the physical section, because it leads to increased fuel consumption and running hours for the generators. This example demonstrates how the same cyber-attack can lead to different outcomes depending on the physical system design and operational condition. Moreover, it demonstrates how the use of mathematical modeling can be useful to address the intertwined nature of modern

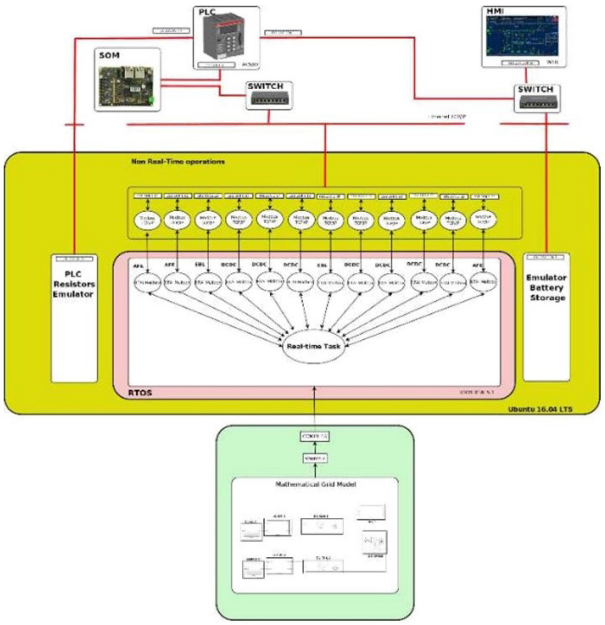


Fig. 13. HIL communication layout with a System on Module attacking in Man in The Middle configuration.

IPSs.

B. Future IPS example

The same approach applied to the actual IPS can be used to study, design, and manage future shipboard power systems. To provide an example, in Fig. 11 a MVDC ZEDS is shown. It consists of two dc buses connected by Electronic Bus Link (EBL), and interfaced with batteries, an electronic load, generators, and an external AC network by means of twelve static converters. A complete mathematical model of the grid has been developed in Matlab Simulink environment, has been translated into a C++ source, and then has been compiled for real-time execution. Each component is simulated by coupling its mathematical model (running in real-time) with a software interface for connecting it to the control system. In the case shown here the latter is a real PMS (implemented by a CPU with suitable onboard software), which communicates using a standardized protocol (e.g., Modbus/TCP or IEC 61850) over an IP network. Each converter therefore has its own IP address and exchange data with the PMS. The simulator scheme is shown in Fig. 12. The built simulator allows applying a classic Man-In-The-Middle attack, as described in [14]. The insertion of a fraudulent device into the network is assumed, and the possibility of manipulating the data is considered, leading to incorrect system operation. The attacking device is implemented with a System on Module (SOM) having two appropriately configured Ethernet cards. The scheme of the attacking action is in Fig. 13. The model allows to evaluate the effect of the attack on the entire physical system, by modifying the data sent from/to the PMS and analyzing the consequent power system behavior for evaluating the various options for enforcing its dependability.

The work towards using the Fig. 13 simulator is in progress, and case studies results will be provided in future publications.

VI. CONCLUSIONS

In this paper an integrated approach for enforcing the dependability of shipboard integrated power system is proposed. By considering both the cyber and physical infrastructures as interrelated, it is possible to determine the performance of the system as a whole. In particular, the cyber originated events are modeled as faults of the physical components, thus enabling their evaluation through power system analysis and simulation tools. Such an approach enables additional degrees of freedom in counteracting malicious actions, being the failure process of the power system a dynamic one. Indeed, the IPS evolution towards a failure takes a variable amount of time (depending on the operating point of the system and on

the specific failure), which can be used to apply corrective measures. Thus, by means of the dynamic simulation results it is possible to determine enforcing actions for the system. These actions can then be focused on the cyber infrastructure, on the physical infrastructure, or on both at the same time.

Additionally, dynamic models of the cyber and physical infrastructures can be used to build a digital twin of the system, which enables continuous system surveillance by providing a tool to identify malicious actions (comparing real system and digital twin behavior in real time).

Massimiliano Chiandone graduated from University of Udine (M.Sc.) in Computer Science and from University of Trieste (B.Sc.) in Electrical Engineering and received a Ph.D. in Electrical Engineering from University of Padua (Italy) in 2012. He has been working for several years at MSC Software Corporation and at the Synchrotron Light Laboratory in Trieste as system administrator and software developer.
His main research interests are in real time control systems.
Department of Engineering and Architecture, University of Trieste, 34127 Trieste, Italy (mchiandone@units.it)

Giorgio Sulligoi (Senior Member, IEEE) received the M.Sc. degree (Hons.) in electrical engineering from the University of Trieste, Trieste, Italy, in 2001, and the Ph.D. degree in electrical engineering from the University of Padua, Padua, Italy, in 2005. He is the Founder and the Director of the Digital Energy Transformation & Electrification Facility, Department of Engineering and Architecture, University of Trieste. He is a Full Professor of Electric Power Generation and Control and an appointed Full Professor of Shipboard Electrical Power Systems. He is the author of more than 100 scientific papers in the fields of shipboard power systems, all-electric ships, generators modeling, and voltage control.
Department of Engineering and Architecture, University of Trieste, 34127 Trieste, Italy (gsulligoi@units.it)

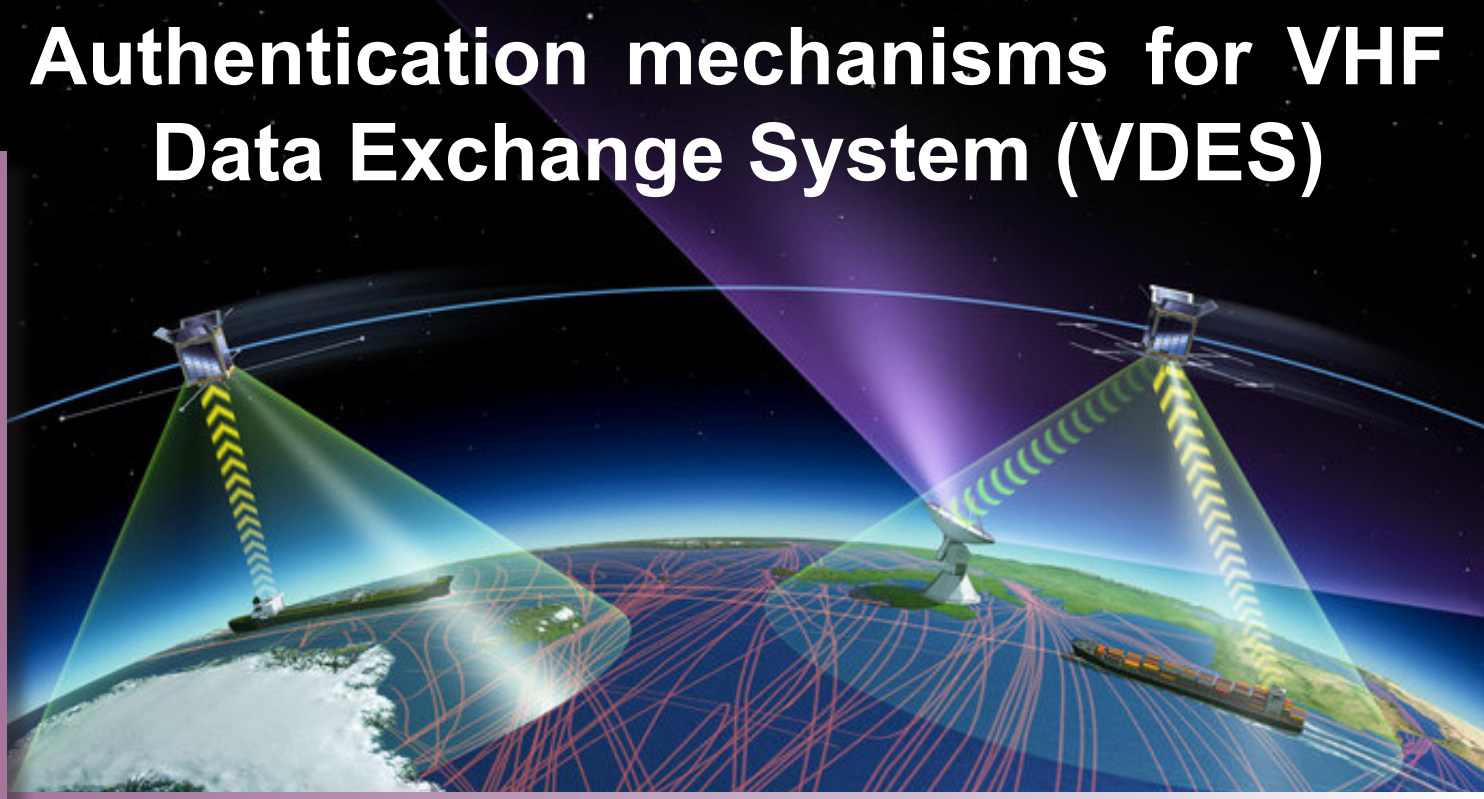
Andrea Vicenzutti received the M.Sc. degree (Hons.) in electrical engineering at the University of Trieste, Trieste, Italy, in 2012, and the Ph.D. degree in industrial engineering from the University of Padua, Padua, Italy, in 2016.
He is currently an Assistant Professor on Power Systems Design with the Department of Engineering and Architecture (DIA), University of Trieste. His research interests include power systems design and dependability, for both marine and land power systems.
Department of Engineering and Architecture, University of Trieste, 34127 Trieste, Italy (avicenzutti@.units.it)

Commander Gianluca Maria Marcilli is graduated in Naval Engineering (M.Sc. Genova University) in 2003 and in Computer Science Engineering (BA - ECAMPUS University, Milan) in 2012. Commanded MARCILLI served aboard Italian Navy ships as Technical Officer and Chief Engineer until 2015. He serves as Specialist Technical Officer in the Italian Naval Directorate since 2015. His main research interests are in Naval Platform Automation, Human Centred Design, Digital Prototyping, Artificial Intelligence and Cyber Security.
CDR MARCILLI's education includes: Master in "Strategic-Military International Studies" (La Sapienza University, Rome - 2016); Master in "Strategic Studies and International Security"(Ca' Foscari University, Venice - 2019); Master in "Digital forensics and Cyber Technologies" (UNIMORE, Modena e Reggio Emilia - 2018). Post graduate courses in "Cyber Analyst" and "Penetration Tester" (UNIMORE 2021).
Directorate of Naval Armaments, Italian Navy, 00175 Roma, Italy (gianlucam.marcilli@marina.difesa.it)

References

[1] A. Vicenzutti, D. Bosich, G. Giadrossi, e G. Sulligoi, «The Role of Voltage Controls in Modern All-Electric Ships: Toward the all electric ship.», IEEE Electrification Mag., vol. 3, n. 2, pagg. 49–65, giu. 2015.
[2] Z. Jin, G. Sulligoi, R. Cuzner, L. Meng, J. C. Vasquez, e J. M. Guerrero, «Next-Generation Shipboard DC Power System: Introduction Smart Grid and dc Microgrid Technologies into Maritime Electrical Netowrks», IEEE Electrification Mag., vol. 4, n. 2, pagg. 45–57, giu. 2016.
[3] V. Arcidiacono; M. Chiandone; G. Sulligoi, "Voltage control in distribution networks using smart control devices of the Distributed Generators" 2011 International Conference on Clean Electrical Power (ICCEP)
[4] McClanahan, «SCADA and IP: is network convergence really here?», IEEE Ind. Appl. Mag., vol. 9, n. 2, pagg. 29–36, mar. 2003.
[5] M. Chiandone e G. Sulligoi, «Energy control in all-electric ship: State of the art and IoT perspectives», in 2017 AEIT International Annual Conference, 2017, pagg. 1–4.
[6] H. Zimmermann, «OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection», IEEE Trans. Commun., vol. 28, n. 4, pagg. 425–432, apr. 1980.
[7] A. Avizienis, J. C. Laprie, B. Randell, e C. Landwehr, «Basic concepts and taxonomy of dependable and secure computing», IEEE Trans. Dependable Secure Comput., vol. 1, n. 1, pagg. 11–33, gen. 2004.
[8] M. Al-Kuwaiti, N. Kyriakopoulos, e S. Hussein, «A comparative analysis of network dependability, fault-tolerance, reliability, security, and survivability», IEEE Commun. Surv. Tutor., vol. 11, n. 2, pagg. 106–124, Second 2009.
[9] G. Buja, A. da Rin, R. Menis, e G. Sulligoi, «Dependable design assessment of Integrated Power Systems for All Electric Ships», in Railway and Ship Propulsion Electrical Systems for Aircraft, 2010, pagg. 1–8.
[10] R. Menis, A. da Rin, A. Vicenzutti, e G. Sulligoi, «Dependable design of All Electric Ships Integrated Power System: Guidelines for system decomposition and analysis», in Railway and Ship Propulsion 2012 Electrical Systems for Aircraft, 2012, pagg. 1–6.
[11] A. Vicenzutti; R. Menis; G. Sulligoi "All-Electric Ship-Integrated Power Systems: Dependable Design Based on Fault Tree Analysis and Dynamic Modeling", IEEE Transactions on Trasportation Electrification Vol. 5, Issue 3, September 2019
[12] A. Boveri, F. D'Agostino, A. Fidigatti, E. Ragaini and F. Silvestro, "Dynamic Modeling of a Supply Vessel Power System for DP3 Protection System," in IEEE Transactions on Transportation Electrification, vol. 2, no. 4, pp. 570-579, Dec. 2016
[13] G. Sulligoi, D. Bosich, A. Vicenzutti, L. Piva, G. Lipardi and T. Mazzuca, "Studies of electromechanical transients in FREMM frigates integrated power system using a time domain simulator," in IEEE Electric Ship Technologies Symp., Arlington, USA, 22-24 April 2013
[14] H. Palahalli, M. Hemmati and G. Gruosso Analysis of Cyber Security Threat of using IEC61850 in Digital Substations involving DERMS

Authentication mechanisms for VHF Data Exchange System (VDES)



by Mirko Frasconi, Gianluca Mandò

Abstract - VHF Data Exchange System (VDES) is a radio communication standard under development that operates in the Marine VHF band. A possible solution to increase the security of VDES can be to rely on an authentication and encryption method. This paper describes an approach, validated through a Proof-of-Concept in the frame of an EU-funded Project, to provide authentication and encryption by establishing a Public Key Infrastructure (PKI), in order to assure unequivocal evidence that the information exchanged by VDES originate from genuine and trusted sources.

1. INTRODUCTION

VHF Data Exchange System (VDES) is a radio communication system, defined by IALA Guidelines [4], [5] and ITU -R Recommendation [1], that operates between ships, shore stations and satellites. VDES features an efficient use of radio spectrum, building on the capabilities of AIS (Automatic Identification System), used for vessel tracking and other navigational and safety-related purposes, and addressing the increasing requirements for data through the system. New techniques providing higher data rates than those used for AIS is a core element of VDES. Furthermore, VDES network protocol is optimized for data communication so that each VDES message is transmitted with a high confidence of reception [2].

Thales Italia (a Thales Group company) has developed a VDES prototype in the frame of the EU-funded Project « Palaemon » [3]. Palaemon is a holistic passenger ship evacuation and rescue ecosystem, which scope is providing a Proof-of-Concept (PoC) of an innovative Situational Awareness and Decision Support System to improve ship mass evacuation procedures in response to maritime incidents, by designing an innovative Mass Evacuation Vessel (MEV) and developing a Smart Evacuation Management System.

In this project, Thales Italia has also defined an Authentication and Encryption mechanism established between the software modules of the Palaemon platform.

The following Chapters describe how VDES can rely on such Authentication and Encryption architecture to securely access and exchange the relevant information.

2. OVERVIEW OF PALAEMON PLATFORM

In more detail, the Palaemon system implements and integrates a number of ICT methods and tools (coupled with the required hardware infrastructure) that can be summarized as follows:

• A number of Data Sources, that collect information about ship stability and health status, weather forecast information, passengers real time positioning, etc.

• A Core Platform, composed by specific software modules that elaborate the data inputs and store the relevant information in a central Data Base.

• Several System Outputs, that receive and present the outcomes of the Core platform modules, e.g.: information is presented on the integrated bridge to support the Ship Master in deciding about evacuation; in case of evacuation, information is sent to the crew to easily locate and evacuate passengers; evacuation notifications are sent directly to passengers; other information is sent, via VDES, to shore stations or other ships to help search and rescue operations, etc.

3. OVERVIEW OF VDES STANDARD

AIS is a widely used tool for safety of navigation. However, with increasing demand for maritime VHF data communications, AIS has become heavily used for maritime safety, maritime situational awareness and port security. As a result, AIS channels have become overloaded, causing the need for additional bandwidth. This has led to the definition of VDES, which main features are the following:

• VDES operates between ships, shore stations and satellites on AIS, Application Specific Messages (ASM) and VHF Data Exchange (VDE) frequencies in the Marine Mobile VHF band.

• It provides capability to transmit to a specific vessel (addressed); to a group of vessels (addressed); to all units in the vicinity (broadcast).

• The data transmission can be achieved through terrestrial or satellite link.

• It features an efficient use of the radio spectrum, providing higher data rates than AIS.

• Its protocol is optimized for data communication and is characterized by a high level of availability.

• Data integrity monitoring is performed at VDES link layer (e.g. check sum).

• It is based on Software Defined Radio (SDR) technology

In conclusion, it can be stated that VDES provides faster data rates with greater integrity, thus improving maritime efficiency, safety and security.

In detail, the main differences with respect to AIS are the following:

• The Modulation and Coding Scheme (MCS): AIS uses GMSK while VDES features a Dynamic MCS using π/4-QPSK, 8PSK and 16QAM.

• The channel bandwidth is raised from 25 kHz per channel (simplex) of AIS, up to 25/50/100 kHz per channel (duplex) of VDES.

• The Data rate is increased from 9.6 kbps of AIS up to 307.2 kbps of VDES.

4. VDES IMPLEMENTED ARCHITECTURE

For the implementation of the VDES prototype in the context of the Palaemon project, the Software Defined Radio (SDR) technology has been adopted.

The following figures show the VDE transmitter architecture, implemented in the simulator, used for performance assessment, and the receiver section architecture:

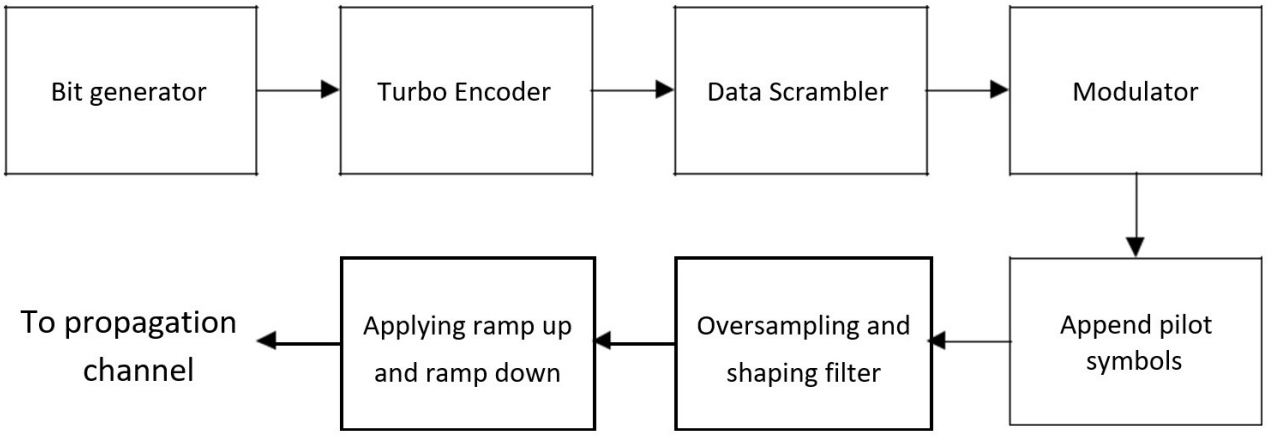


Figure 1 – VDES Transmitter architecture

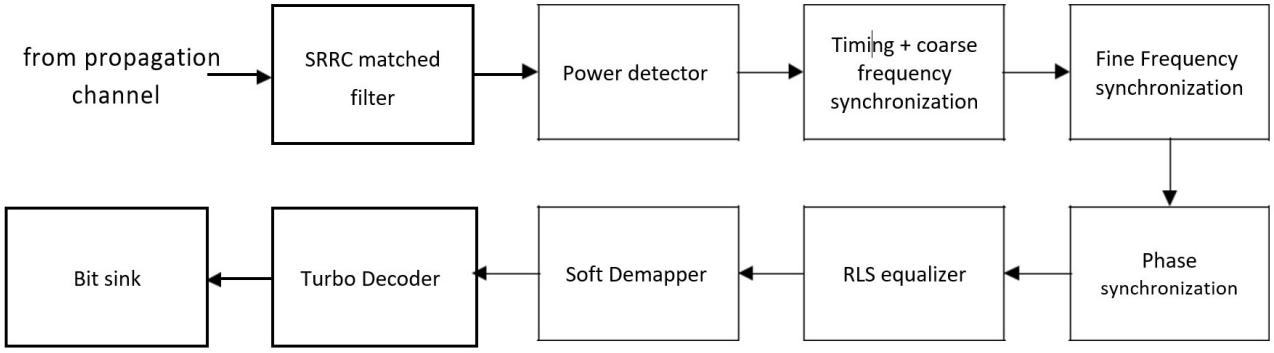


Figure 2 – VDES Receiver architecture

For the software implementation of the Waveform, developed in C++ language, the basic idea has been to map a single algorithm over a thread. The resulting software architecture is that of multi-threads working in pipeline. The concept above relies on the mechanism of data exchange among two consecutive threads.
The shared buffer has been implemented with read and write methods, used by "consumer" and "producer" threads, regulated by a mechanism, which checks the validity of the data read / written.
The resulting software architecture of the multi -thread framework consists of the following elements: shared buffers; chain of transmission threads; chain of receiving threads; global variables; variables shared across multiple threads.

5. VDES SDR HARDWARE SOLUTION

As SDR hardware platform, a combination of radio and carrier boards has been selected, able to carry out the development of an optimised high performance SDR solution, whilst retaining the flexibility to support specific OEM/ODM needs and future evolution of the standard.
This architecture consists of a Base-Band (BB) System-on-Chip (SoC), paired with Radio Frequency (RF)
SoC, in particular we have selected:

- Analog Device EVAL-ADRV9002 evaluation board, as radio front-end
- Xilinx Zynq®-7000 SoC ZC706 Evaluation Kit, as carrier board

The BB SoC contains Field Programmable Gate Array (FPGA) fabric and ARM dual-core Cortex A9 processor. Its high-level block diagram is shown in the following figure:

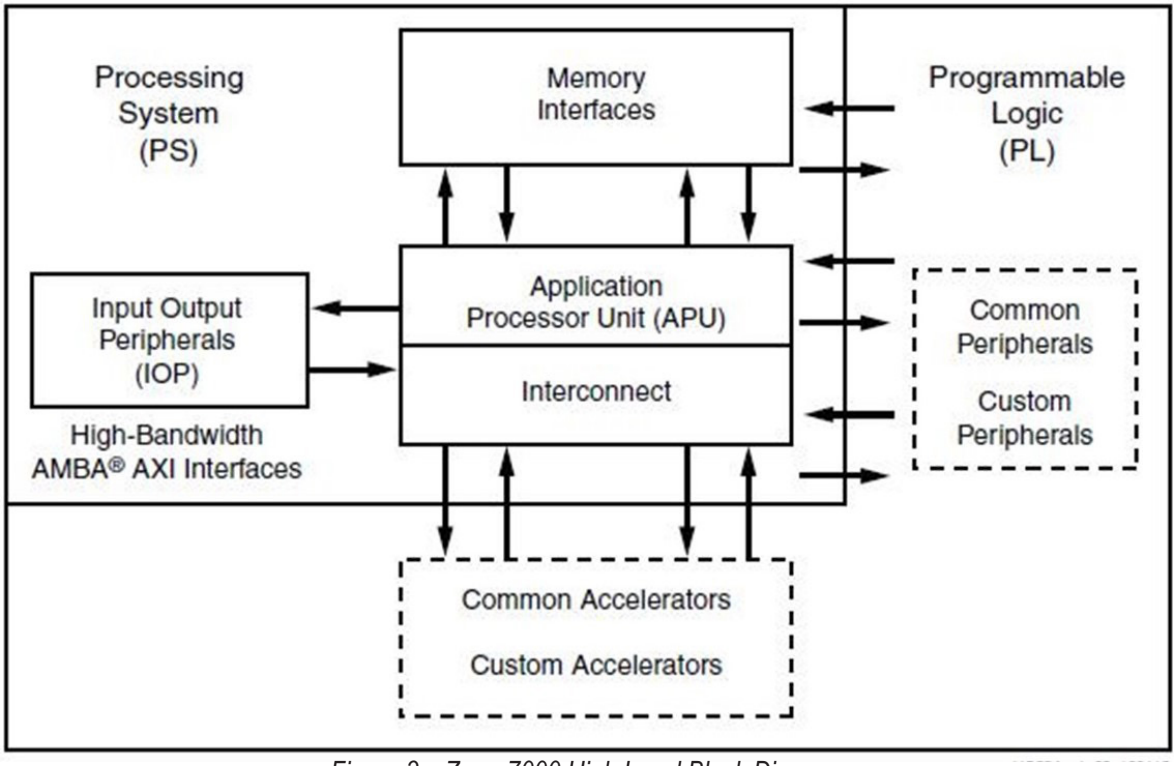


Figure 3 – Zynq-7000 High Level Block Diagram

The selected RF card operates from 30 MHz to 6000 MHz and covers the UHF, VHF, licensed and unlicensed cellular bands, and industrial, scientific, and medical (ISM) bands. This board can support both narrowband and wideband standards up to 40 MHz bandwidth on both receive and transmit.
The ported VDES transceiver code has been adapted, with respect to the VDES simulator code, in order to interface the RF front end section of the selected hardware platform. This interface relies on the C APIs, to initialize, configure, program, and control the RF front end both in transmission and reception.

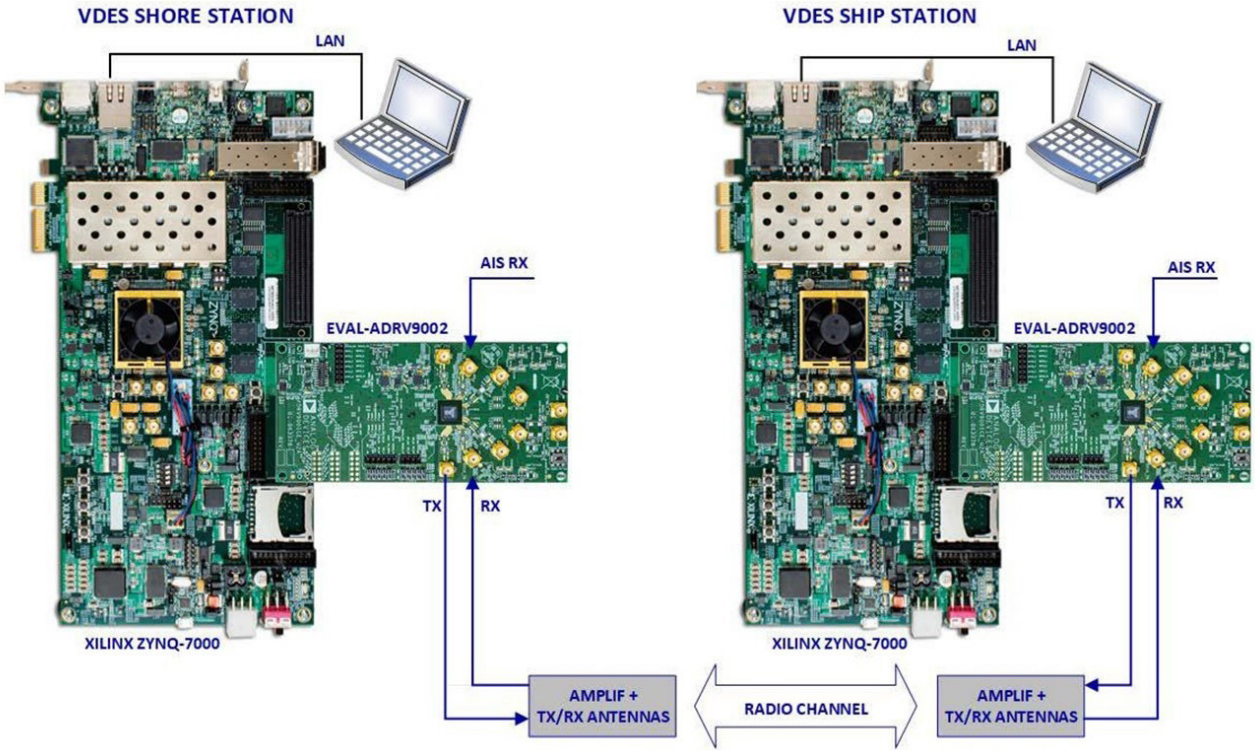


Figure 4 – Overall VDES Prototypes Setup

The two boards have been assembled and connected to amplifiers and antennas in order to create a VDES prototype. In order to perform validation tests, between two VDES prototypes a Radio Frequency link has been established. The overall test setup is shown in Figure 4.

6. IMPLEMENTED AUTHENTICATION AND ENCRYPTION STRUCTURE

In order to provide an adequate level of protection for the Palaemon platform, including the VDES system, several issues had to be faced from a security point of view: first of all, the access to the Palaemon system from outside; secondly, the access to the Core Data Base from the various platform modules; finally, the Passengers Identity Management, which raises issues for what regards the GDPR, in particular due to some processes that need to exchange sensitive information, like the Embarkation registration, the Real Time Location, or, some information that need to be exchanged only in emergency situation, like passengers list and health status.

A multi-layered security approach has been adopted, based on open-source solutions, implementing a hybrid

Kubernetes cluster and Docker Compose deployment, which can rely on several levels of security:

1) Docker [9], a solution to implement and execute Virtual Containers, which protects the inner part of the Platform.
2) Kubernetes [8] is a portable, extensible, open-source platform for managing containerized workloads and services, that facilitates both declarative configuration and automation. Kubernetes, with its native security, controls how the components interact with each other's.
3) Apache Kafka [6] is an open-source project for a distributed publish/subscribe messaging system, widely used for real-time applications to exchange information. Kafka has been adopted in this project to store messages in topics that are partitioned and replicated across multiple brokers in a cluster. "Producers" send messages to topics from which

"consumers" read. Kafka can monitor operational data, aggregating statistics from distributed applications to produce centralized data feeds. Kafka can use SSL Certificates, which provide security through TLS encryption protocol. One dedicated SSL Certificate is issued by a Certification Authority per each component that requests to access a resource. In the Palaemon Proof-of-Concept, the certificates are issued by one of the partners of the Project, acting like a Certification Authority.

4) Other level complementary to Kafka, adopted in Palaemon, is Keycloak [10]: an open-source Identity and Access Management solution, that implements an additional level of security based on the OAuth 2.0 Authorization Framework. This framework can be used to enable third-party services to gain limited time access on protected resources. In the Palaemon system, Keycloak has been used to allow software components involved in the People Management data flows to access the Core Data Base.

5) Finally, top level protection is provided by NGINX [11], an open-source HTTP and reverse proxy server that maps between internal IP addresses and Domain Names, acting like an internal DNS, configured inside the Palaemon Cluster. Through NGINX we can force the system to accept only internal requests coming from a pre-defined IP range. NGINX, that is implemented as a Kubernetes deployment, has been configured with basic authentication.

7. VDES OPERATION IN THE PALAEMON ECOSYSTEM

In normal operation, VDES will feed Palaemon platform with data from coastal stations or other vessels, e.g., weather or environmental conditions, position monitoring, etc. At the same time, the VDES software is subscribed to the notifications from a Palaemon software module called Evacuation Coordinator, allowing it to be aware of evacuation phase changes. In case of evacuation, ship's VDES transceiver can broadcast a Mayday signal and send messages to coastal stations and vessels, e.g. the evacuation plan, passenger list, ship waypoints and route plan report, useful for Search & Rescue operations.

In order to interface the VDES radio with the Palaemon platform, we have developed an application, called VDES Gateway (VDES_GW), using RUST programming language [12]. Two versions of VDES_GW have been deployed: one for Ship side and one for Shore side.

We have demonstrated the VDES end-to-end functionality in three use cases:

1) AIS position extraction
2) Weather information acquisition
3) Evacuation information transmission

Use Case 1: AIS position extraction

This use case is used as a demonstration of the capability of the VDES shore radio to interface and extract information from the AIS system. The data is provided to VDES_GW which forwards it to Palaemon's ICT system, called DFB (Data Fusion Bus), at shore:

- Step 1: The VDES Shore radio interface the AIS system and extracts the ship position data.
- Step 2: The VDES Shore radio publishes the received data in the LAN and the VDES_GW application acquires it. The received data are stored by the application for usage in other scenarios.
- Step 3: the VDES_GW application publishes the data to the DFB system.

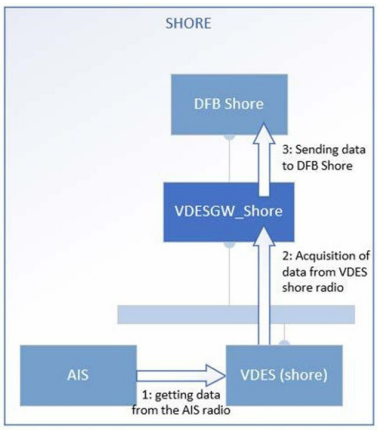


Figure 5 – AIS data extraction use

case Use Case 2: Weather information acquisition

In this use case the VDES_GW_Shore application polls the Weather data service to get the current forecast of weather condition (next three hours) in the current position of the ship (acquired as from the previous Use Case 1), and sends this weather data directly to DFB shore and, indirectly, to the DFB Ship through the VDES radio channel:

- Step 1: If the VDES_GW_Shore application has a valid and fresh position of the ship, obtained from the Use Case 1, it polls periodically the Weather data service to get the current weather condition for that position.
- Step 2: The VDES_GW_Shore application sends the weather data to the DFB Shore.
- Step 3: The VDES_GW_Shore application sends to the VDES Shore radio the request to send the Weather data to the Ship.
- Step 4: The VDES Shore radio sends the data to the VDES Ship radio.
- Step 5: The VDES Ship radio publishes the received data towards the VDES_GW_Ship application.
- Step 6: the VDES_GW_Ship application sends the weather data to the DFB Ship.

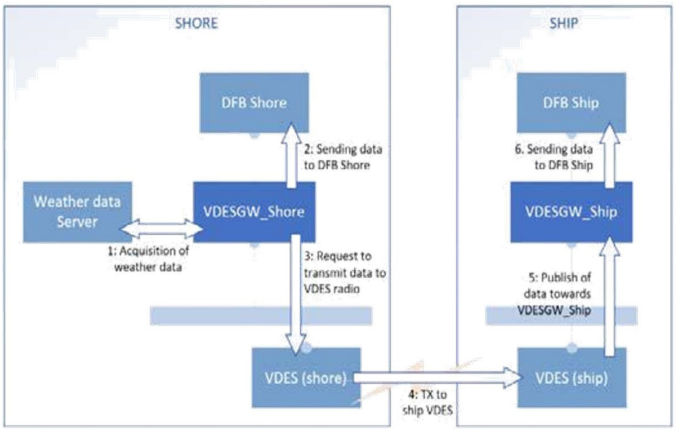


Figure 6 – Weather information acquisition use

case Use Case 3: Evacuation information transmission

This use case demonstrates the transfer of data between Ship and Shore using the VDES radio channel. The "Ship Evacuation command" is used as a sample of data to be transferred:

- Step 1: the DFB Ship component publishes an "evacuation command" message; the message is received from the VDES_GW_Ship application.
- Step 2: The VDES_GW_Ship application sends to the VDES Ship radio the request to send the evacuation command to the Shore.
- Step 3: The VDES Ship radio sends the data to the VDES Shore radio
- Step 4: The VDES Shore radio publishes the received data towards the VDES_GW_Shore application.
- Step 5: the VDES_GW_Shore application passes the evacuation command to the DFB Shore application.

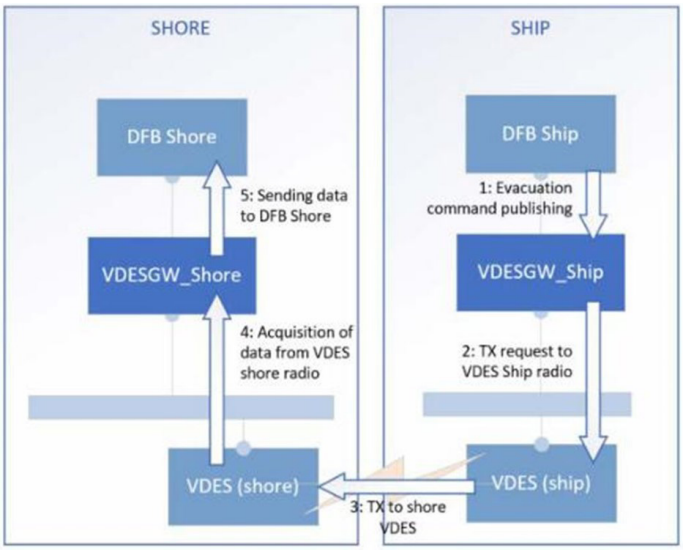


Figure 7 – Evacuation information transmission use case

8. VDES INTERFACES DESIGN

Three main interfaces shall be managed by the VDES_GW applications (Shore and Ship):

1) Interfaces with the DFB systems.
2) Interfaces with the VDES radios.
3) Interface with the Weather Data service

Regarding the first interface, the Palaemon ecosystem streams and receives the data using Apache Kafka [6] messaging system, introduced in Chapter 6.

The VDES_GW_Shore application produces a Kafka client that connects to the shore Kafka cluster to exchange data with the DFB Shore system.

The VDES_GW_Ship application, similarly, produces a Kafka client that connects to the ship Kafka cluster to exchange data with the DFB Ship system.

Regarding the second interface, the VDES radio sends and receives data using a publish/subscribe mechanism based on MQTT [7]. MQTT is a lightweight, network protocol that transports messages between devices. The protocol usually runs over TCP/IP, however, any network protocol that provides ordered, lossless, bi-directional connections can support MQTT. It is designed for connections with remote locations where resource constraints exist, or the network bandwidth is limited. The protocol is an open OASIS standard and an ISO recommendation (ISO/IEC 20922). In both shore and ship side an MQTT Broker has been deployed. Both VDES radio and Gateway applications will instance an MQTT client and exchange topics and data with the mediation of the MQTT Broker.

Regarding the third interface, the Weather Data Service is a data proxy that can be polled to obtain current or historic maritime weather condition over the globe accessing National Oceanic and Atmospheric (NOAA) data. The weather information is published using a REST interface and can be accessed at a specified URL. A get request is done in order to obtain the weather condition of a specific point of the globe at a given time.

Summarizing, the following figure details the interfaces managed by the VDES_GW applications, on Shore and Ship side, showing also the middleware used for the communication (Kafka, MQTT):

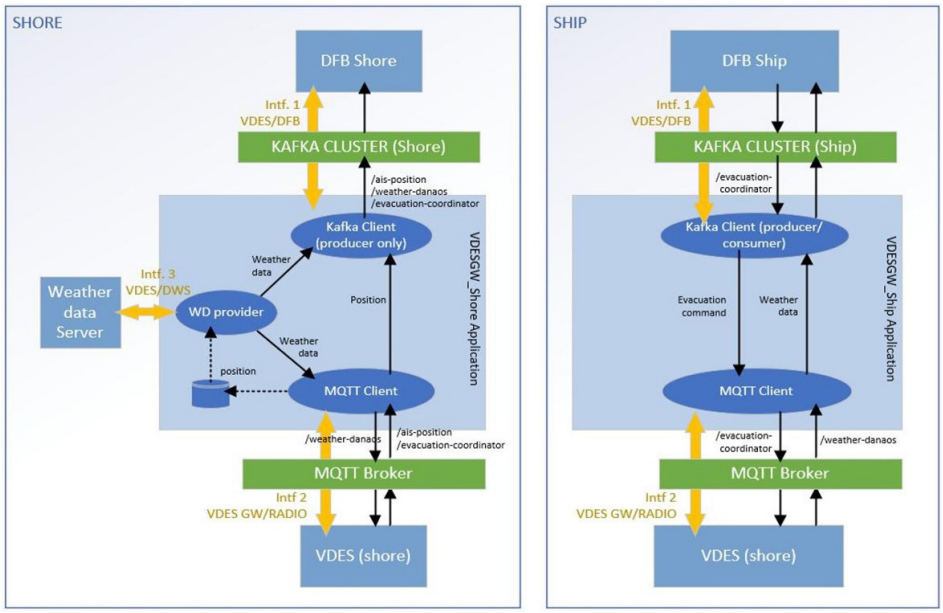


Figure 8 – VDES Gateway interfaces

9. CONCLUSIONS AND FURTHER IMPROVEMENTS

In this paper, a protection mechanism has been presented, able to authenticate VDES and to assure that the data that VDES needs to access and exchange come from a trusted source. In order to do this, a Public Key Infrastructure has been established, based on open-source solutions like Kafka, that can rely on TLS encryption and on authentication through certificates provided by an entity acting as Certification Authority. The overall solution has been validated through a Proof-of-Concept in the frame of an EU-funded project [3].

Further improvements to increase VDES system security can be:

1) To use an Identity and Access Management solution like Keycloak in order to access and transmit sensitive

information like passengers list, only if triggered by an emergency status change. This feature would be easy to implement, as Keycloak is already part of the overall PoC platform.

2) To exploit the VDES Gateway application to provide “cross-authentication” between ship and shore station.

3) To improve the VDES security providing end-to-end encryption of the radio signal transmitted between ship and shore. This can be also done, leveraging the Software Defined Radio flexibility by implementing a public key encryption (e.g. RSA encryption) software module at VDES software level.

Moreover, some initiatives are ongoing in order to further develop this prototype towards a commercial product.

ACKNOWLEDGEMENTS

The project “Palaemon” has received funding from the European Union’s Horizon 2020 Research and Innovation Programme under Grant Agreement No 814962.

REFERENCES

[1] Recommendation ITU-R M.2092-1 (02/2022)
[2] https://www.iala-aism.org
[3] https://palaemonproject.eu/
[4] IALA Guideline G1117 VHF Data Exchange System (VDES) Overview, Ed. 2.0, Dec. 2017
[5] IALA Guideline G1139 The Technical Specification of VDES, Ed. 3, Jun. 2019
[6] https://kafka.apache.org/
[7] https://mqtt.org/
[8] https://kubernetes.io
[9] https://www.docker.com/
[10] https://www.keycloak.org/
[11] https://www.nginx.com/
[12] https://www.rust-lang.org

Mirko Frasconi (mirko.frasconi@thalesgroup.com), Systems Engineer from Engineering dept. of Thales Italia, carries out design and system integration of Communication and Security solutions for Critical Infrastructures, and system/product engineering of military systems. He is involved in bids and projects in both civil and defence sectors, as well as in EU research programs. In Thales Italia since 2016, in the past he has gained experience in the Radio signal transmission technology, working and consulting in the Space sector (Thales Alenia Space) and in the Telecommunications industry (Telecom Italia Group).

Gianluca Mandò (gianluca.mando@thalesgroup.com), Research, Technology & Innovation (RTI) Manager of Thales Italia, is responsible for research programs and technology insertion in business product lines. After working for 15 years in multinational industries (Italtel, Siemens, Leonardo) holding various management positions in R&D departments, he joined Thales Italia in 2009 as responsible for the development of Security & Transportation product solutions. He took part to several regional, national and EU research programs as scientific and program coordinator, by supervising all technical activities.

NMIOTC Annual Information Meeting & Advisory Board 2022

NMIOTC's Annual Information Meeting (AIM) and Advisory Board (NAB), chaired by NMIOTC Commandant, were held at the Center's premises on Thursday 3rd February 2021.

Course 1000 "Command Team MIO Issues"

NMIOTC conducted the resident Course 1000 "Command Team MIO Issues" from 14 to 18 February 2021. The aim of the course is to assist Staff Officers and Naval Units' Command Teams in the efficient application of NATO common standards in the planning and execution of Maritime Interdiction Operations (MIO). It was attended by 7 participants from 5 Nations.

Courses 2000 & 3000 "Boarding Team Theoretical & Practical Issues"

Resident Course 2000 "Boarding Team Theoretical Issues" and Course 3000 "Boarding Team Practical Issues" were conducted in tandem from 21st February to 4th of March 2022 at NMIOTC premises. It was attended by 19 participants from 7 Nations.

Course 6000 "Weapons of Mass Destruction in MIO"

Resident Course 6000 "Weapons of Mass Destruction in Maritime Interdiction Operations" was conducted from 21st to 25th of February 2022 at NMIOTC premises. It was attended by 6 participants from 3 Nations.

Course 26000 "Tactical Combat Casualty Care/ Combat Lifesaver in Maritime Operations"

Resident Course 26000 "Tactical Combat Casualty Care/ Combat Lifesaver in Maritime Operations" was conducted from 28th of February to 4th of March 2022 at NMIOTC premises. It was attended by 10 participants from 5 Nations.

Course 10000 "Maritime Interdiction Operations in Support of Countering Illicit Trafficking at Sea"

Resident Course 10000 "Maritime Interdiction Operations In Support Of Countering Illicit Trafficking At Sea" was conducted from 14th to 18th of March 2022 at the NMIOTC premises. It was attended by 8 participants from 3 Nations.

Above Water Warfare Capability Group (AWWCG) 2022-1 Meeting

From 22nd to 24th March 2022, the Above Water Warfare Capability Group (AWWCG) 2022-1 meeting was hosted at the NMIOTC's premises. In total twenty four (24) delegates from NATO relevant Organizations and entities participated in the meeting.

NMIOTC Presence at "Military Strategic Partnership Conference 2022 (MSPC 22)"

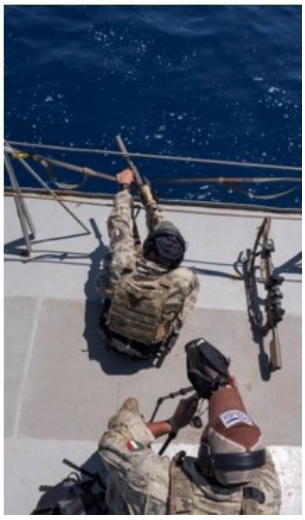
From Monday 27th March to Friday 1st April 2022, NMIOTC participated with a three staff officer delegation in the "Military Strategic Partnership Conference 2022 (MSPC 22)", organized and conducted by SHAPE Partnership Directorate (PD), in Dublin, Ireland.

Course 14000 “Maritime Improvised Explosive Device Disposal (M-IEDD)”

Resident Course 14000 “Maritime Improvised Explosive Device Disposal (M-IEDD)” was conducted from 4th to 8th April 2022 at NMIOTC premises. It was attended by 20 participants from 8 Nations.

Course 27000 “Maritime Sniper Course”

From 9th to 20th May 2022 the NMIOTC Maritime Sniper Course was conducted at NMIOTC premises and in the broader area of Chania, Crete. It was attended by 22 participants from 5 Nations.



Medical Support Annual Discipline Conference (ADC)
and Military Medical Training Working Group Meeting (MMT WG)

From 17th to 19th May 2022, the Medical Support Annual Discipline Conference and Military Medical Training Working Group Meeting were hosted at the NMIOTC's premises. In total 27 delegates from NATO Organizations and National relevant entities participated in the meeting.

Course 13000 "Command Team Issues in Maritime Interdiction Operation in Support of International Efforts to Manage the Migrant and Refugee Crisis at Sea"

Resident Course 13000 "Command Team Issues in Maritime Interdiction Operation in Support of International Efforts to Manage the Migrant and Refugee Crisis at Sea" was conducted from 23rd to 27th of May 2022 at NMIOTC premises. It was attended by 9 participants from 3 Nations.

NATO Maritime Operational Law Course

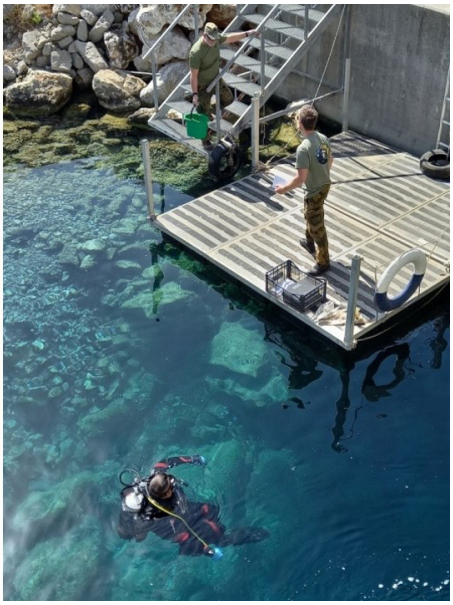
NATO Maritime Operational Law Course was conducted from 23rd to 27th May 2022 at NMIOTC premises under the auspices of NATO SCHOOL Oberammergau (NSO) in cooperation with the United States Naval War College (USNWC), the Centre of Excellence for Operations in Confined and Shallow Waters (CSW COE) and NMIOTC. It was attended by 29 participants from 11 Nations.

Course 15000 "Managing Migrant related Incidents at Sea"

Resident Course 15000 "Managing Migrant related Incidents at Sea" was conducted from May 30th to June 3rd 2022 at NMIOTC premises. It was attended by 9 participants from 3 Nations.

Course 23000
"Weapons Intelligence Team (WIT) Supplement in the Maritime Environment"

Resident Course 23000 Weapons Intelligence Team (WIT) Supplement in the Maritime Environment was conducted from May 23rd to Jun 3rd 2022 at the NMIOTC premises. It was attended by 24 participants from 7 Nations.



13th NMIOTC ANNUAL CONFERENCE 2022

The 13th NMIOTC Annual Conference titled: "Countering Terrorism Threats in Maritime Domain: How effective Interdiction strengthens Alliance's Deterrence and Defence Objectives" took place from 7th to 8th June of 2022 at the NMIOTC premises. It was attended by one hundred twenty (120) participants from twenty four (24) Allied and Partner Nations, International Organizations, the academic community and representatives from the shipping and defence industry.

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

From June 27th to July 1st 2022, the Resident Course 25000 “Drafting Production and Maintenance of NATO Standards”, was conducted at the NMIOTC premises. It was attended by 29 participants from 14 Nations.

15th Allied Cryptographic Task Force (ACTF) Meeting

From 5th to 9th of September 2022, the 15th Allied Cryptographic Task Force (ACTF) Meeting, led by Alliance Strategic Command, took place at the NMIOTC premises. It was attended by 70 participants from 21 Nations.

Course 5000 “Maritime Operational Terminology Course (MOTC)”

From 12th to 23rd of September 2022, the NMIOTC Maritime Operational Terminology Course (MOTC) was conducted at NMIOTC premises with the support of NATO Allied Command Transformation and USNR. It was attended by 10 participants from 7 Nations.

Course 21000 “Medical Combat Care in Maritime Operations”

From the 12th to 23rd of September 2022, the Resident Course “21000” Medical Combat Care in Maritime Operations was conducted at the NMIOTC’s premises. It was attended by 24 participants from 10 Nations.

6th NMIOTC CYBER SECURITY CONFERENCE

From 27th to 28th September 2022, the 6th NMIOTC Cyber Security Conference in maritime domain took place at the NMIOTC premises. It was attended by more than 100 participants from 21 Allied and Partner Nations.

Course 28000 "Radiological Search in Maritime Environment"

From 26th to 30th of September 2022, the Resident Course "28000", Radiological Search in Maritime Environment, was conducted at the NMIOTC premises. It was attended by 24 participants from 3 Nations.

Course 8000 "C-IED Considerations in Maritime Force Protection"

From 19th to 30th of September 2022, the Resident Course 8000 "C-IED Considerations in Maritime Force Protection" was conducted at the NMIOTC Premises. It was attended by 22 participants from 13 Nations.

7th International Senior Course of Hellenic National Defence College:
"Contemporary Maritime Security Threats" Module

From 3rd to 7th of October 2022 the students of the 7th International Senior Course of the Hellenic National Defence College (HNDC) attended the "Contemporary Maritime Security Threats" module delivered by NMIOTC SMEs, during their educational week trip. It was attended by 15 participants from 5 Nations.

Course 12000 “C-IED in Maritime Interdiction Operations”

From 10th to 14th of October 2022, the Resident Course 12000 “C-IED in Maritime Interdiction Operations” was conducted at the NMIOTC premises. This “NATO Approved” Course fills an operational gap in capability and contributes to operations conducted by Boarding Teams when searching and exploiting evidence, which are fundamental to the C-IED process. It was attended by 9 participants from 8 Nations.

ACT’s “MARITIME INFORMATION SERVICES CONFERENCE 22”

From 8th to 11th November 2022, the Maritime Information Services Conference (MISC 22), organized by the Allied Command Transformation (ACT), was conducted at the NMIOTC premises. The conference was attended by 87 participants, coming from NATO HQs and 17 NATO countries.

Course 19000 “Cyber Security Aspects within Maritime Operations”

From 14th to 18th of November 2022, the Resident Course 19000 “Cyber Security Aspects within Maritime Operations” was conducted at the NMIOTC premises. It was attended by 15 participants from 6 Nations.

Course 7000 “Maritime Interdiction Operations in Support to Counter Piracy And Armed Robbery at Sea Operations”

From 14th to 18th of November 2022, the Resident Course 7000 “Maritime Interdiction Operations in Support to Counter Piracy and Armed Robbery at Sea Operations” was conducted at the NMIOTC premises. It was attended by 11 participants from 6 Nations.

Multinational Exercise "CUTLASS EXPRESS 2022"
February 4 - 17, 2022

Multinational Exercise "ARIADNE 22"
March 9 - 18, 2022

UPX "Underwater Post Blast Exploitation Training"
May 23 - 27, 2022

Training of Estonian Police and Border Guard Team
July 4 - 15, 2022

Lessons Learned Tailored Training by JALLC
July 19 - 21, 2022

Training of German Navy Boarding Team (DEU BT MOC 1)
August 29 - September 9, 2022

CyberHOT Summer School
September 29 - 30, 2022

Training in the context of the Invitational Exercise (INVITEX) 'NIRIIS 2022'
November 6 - 7, 2022

Visit of Deputy Minister of the Hellenic Ministry of Defence
January 18, 2022

Visit of Congressional Delegation (CODEL), consisting of
Rep Salud Carbajal (D-CA), Rep Rick Larsen(D-WA)
and Rep Tony Gonzales(R-TX), hosted by the
Minister of Defence Nikolaos Panagiotopoulos and the Chief of the
Hellenic National Defence General Staff General Konstantinos Floros
April 14, 2022

Visit of Congressional Delegation (CODEL), headed by
Rep. Frank Pallone (D-NJ),
Chairman of Committee on Energy and Commerce
April 21, 2022

Visit of National Defence College of India
June 9, 2022

Visit of the Minister of Foreign Affairs of Greece, Nikos Dendias
July 19, 2022

Visit of the Military Representative of Qatar to NATO,
Brigadier General Ali Abdulaziz Al-Mohannadi
August 31, 2022

Visit of the Deputy Chief of Mission at the U.S. Embassy in Athens,
Mrs. Maria dG Olson
September 20, 2022

Visit of the Vice President of the European Commission,
Mr. Margaritis Schinas
September 29, 2022

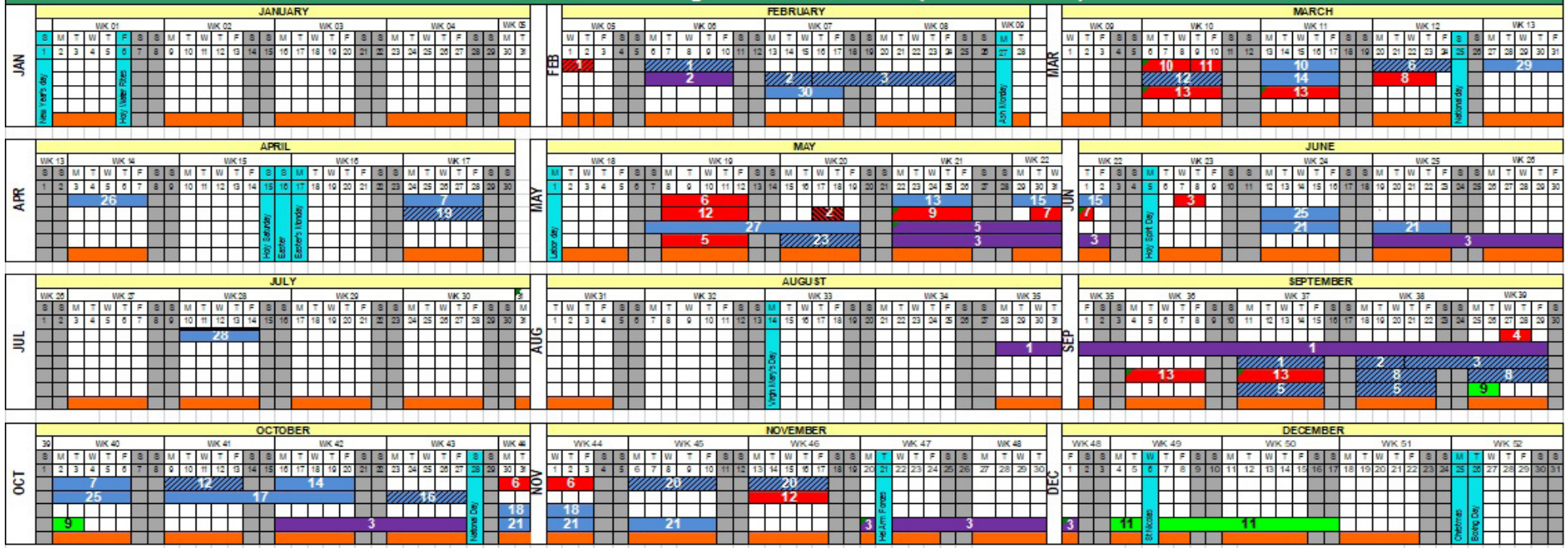
Visit of Congressional Delegation (CODEL), headed by
Rep. Adam Smith (D-WA),
Chairman of the House Armed Services Committee
April 21, 2022

Visit the Supreme Headquarters Allied Powers Europe (SHAPE)
National Military Representatives (NMRs)
October 6, 2022

Visit of the Secretary of the United States Navy (SECNAV),
Honorable Carlos Del Toro
November 15, 2022

Visit of the Israel Defence Forces' (IDF) Delegation,
headed by Colonel Gil Dolov
November 22, 2022

Draft NMIOTC Program of Work 2023 (DNPOW 2023)



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) (TBD)
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)
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

EVENTS

1. NAB (NMIOTC)
2. NCB (HNGS)/ACT
3. NMIOTC Annual Conference
4. NMIOTC Cyber Security Conference
5. UPX Training
6. IAMD CET-P 2023
7. MPC FOR NOSP23 AND TC&S WS
8. IP CAT
9. NATO Maritime Operations Law Course
10. Crypto Capability Team meeting
11. Info. Assurance and Cyber Def. Capab.Panel (C
12. NSHQ SOMTG HOSTED PILOT COURSE
13. NSHQ SOMTU HOSTED PILOT COURSE

EXERCISES / METTs

1. CUTLASS EXPRESS METT (TBD)
2. SEA SHIELD METT (TBD)
3. ADRION METT (TBD)
4. SEA BREEZE METT (TBD)
5. BREEZE METT (TBD)
6. Exercise MARSEC (TBD)
7. NORTHEN SPIRIT (TBD)
8. PHOENIX EXPRESS METT (TBD)
9. OSG FOCOPS METT (TBD)
10. MEDUSA (TBD)
11. NIRIIS (TBD)
12. DYNAMIC MESSENGER (TBD)
13. STEADFAST INTEREST (TBD)

TAILORED TRAININGS

1. PHL Teams
2. HCG Teams (TLCC)
3. DEU Teams
4. GRC Teams
5. GRC Naval Units

? **Updated 11 November 2022**

Cancelled

Training Courses | Tailored Trainings | NATO Events | Exercise / MTTs | Trial Courses | Events | Naval Unit Training | National Holidays | Available Period for Training | Evaluation of Courses / Maintenance

NMIOTC
Souda Bay 732 00 Chania
Crete, GREECE

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

Webpage: https://nmiotc.nato.int/