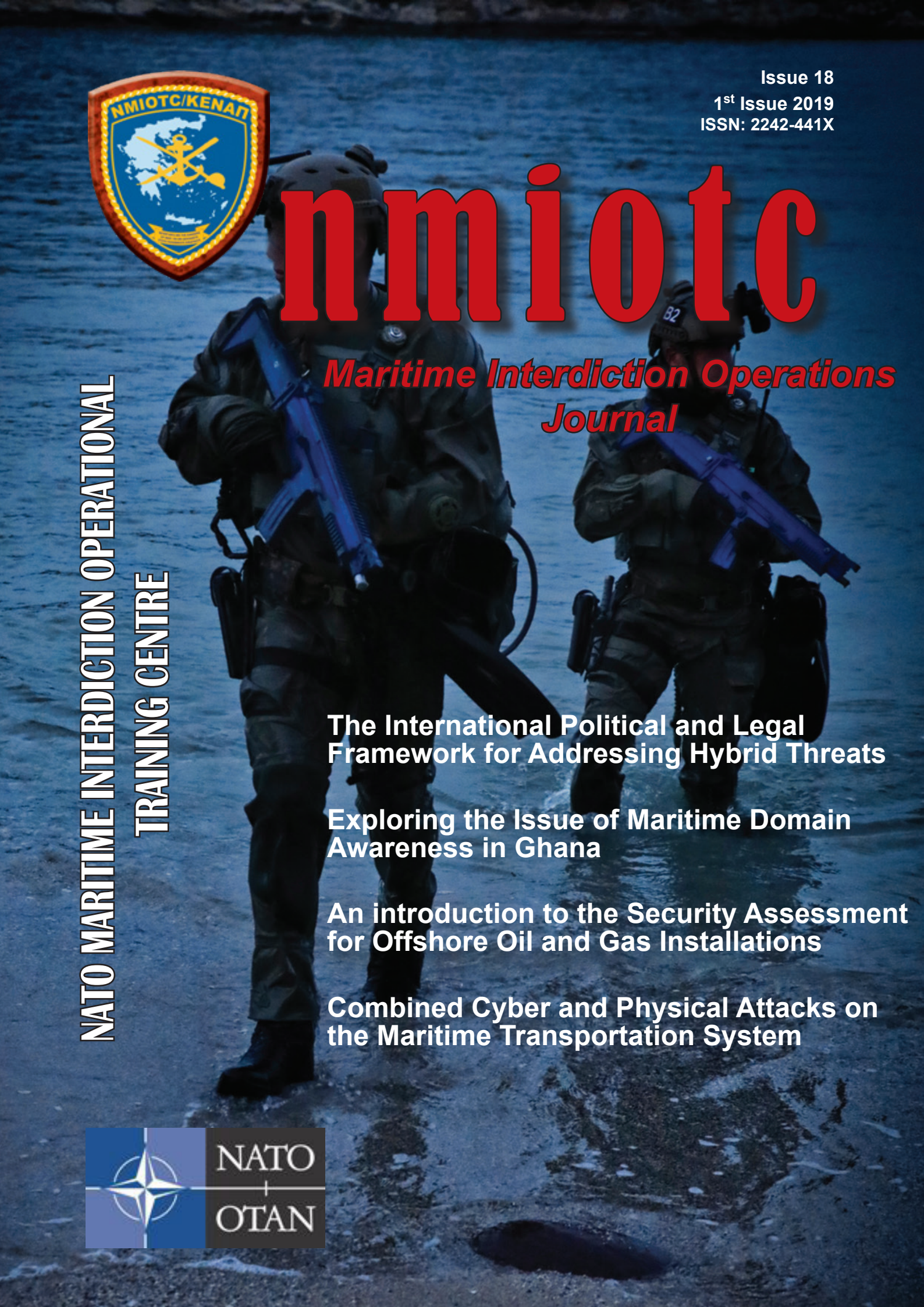
Issue 18
1st Issue 2019
ISSN: 2242-441X

nmiotc

Maritime Interdiction Operations Journal

NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE



The International Political and Legal Framework for Addressing Hybrid Threats

Exploring the Issue of Maritime Domain Awareness in Ghana

An introduction to the Security Assessment for Offshore Oil and Gas Installations

Combined Cyber and Physical Attacks on the Maritime Transportation System

NATO OTAN

NATO
Maritime Interdiction Operational Training Centre

Hosted Event

SAVE-THE-DATE
Littoral OpTech-EASTMED Workshop
Chania/Souda Bay, Crete
5-7 November 2019

Littoral OpTech-EASTMED Workshop is the fifth in a series of OpTech workshops. It follows the successful Littoral OpTech-NORTH workshop held in Halifax, Nova Scotia in October of 2018.

Under the Intellectual leadership of the Littoral Operations Center at the U.S. Naval Postgraduate School and with the support of the U.S. Navy's Office of Naval Research Senior National Representative, and the NATO Maritime Interdicton Operational Training Centre, this workshop will gather international defense leaders, scientists, reseachers, analysts, and think tank experts to explore the unique operational and technological challenges to security & defense in the Eastern Mediterranean littorals.

NMIOTC Event

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

SAVE THE DATE!

11th NMIOTC ANNUAL CONFERENCE 2020

"Interagency and whole of society solutions to maritime security challenges"

Date: Tuesday 2nd to Thursday 4th of June 2020.

Location: Chania, Crete, Greece at the NATO Maritime Interdiction Operational Training Centre.

Event Description: The aim of the upcoming 11th NMIOTC Annual Conference is to discuss issues and share perceptions of the international community how to improve maritime security and forward proposals and solutions for countering the maritime security challenges.

Security Classification: The Conference is unclassified and open to Partner Nations. The Chatham House Rules will apply throughout the Conference.

Language: The working language will be English. No translation will be provided.

CONTENTS

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Commodore S. Kostalas GRC (N)
Commandant NMIOTC

Executive Director
Captain R. Lapira ITA (N)
Director of Training Support

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

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

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

NMIOTC
Commandant's Editorial

Cyber has changed our world. The ongoing digital revolution has fueled unprecedented prosperity and efficiency in our globalized economy, and has become inextricably linked with all aspects of our modern life. These innovations will continue to drive global progress for the foreseeable future, and by most perspectives will continue to evolve at astonishing speeds.

Today, a nation's power – militarily as economically - rests on data. Digital transformation has deeply affected all areas of society, including industry and economy, as well as governmental domains, such as defense and security. Via data and communication networks, computers and automation come together in a new way with remotely connected robotics. In a world of constant connectivity, data is the new oil.

In the wake of this progress, lies a growing number of challenges and risks that threaten the very core of the global security and prosperity. The recognition of the cyberspace as an operational domain, in analogy to land, air, maritime and space domains by NATO marks a new era. The cyberspace has become an operational domain that various sectors (industry, commercial, civilian, military) interact and operate on.

On the other hand Cyber criminals become more and more intelligent and cybercrime evolves at an astonishing pace. Countering cyber threats, calls for a holistic and collaborative approach, and the ability to join the dots between seemingly separate, but effectively interconnected events.

Synergies among all protagonists are needed to effectively defend against advanced attacks and avoid catastrophic impacts to our nations, industries and peoples. NATO assists its

individual member states to become more cyber resilient. Some members have offered NATO access to their cyber capabilities and the Alliance trains and exercises them to take part in crisis or conflict.

Cyber information sharing, collaborative incident handling and cyber situational awareness are the most essential areas that NATO and EU collaboration will lead to successful civilian, industrial, commercial and military cyber security strategies and operations.

And because the actual protagonists of the Seas (Naval and Law Enforcement Operators, Mariners and the people of the shipping industry), ARE in the epicenter of our concerns, the "Q" to us is what keeps those Protagonist of the maritime domain awake at night. This is our call: To Be the Solution Providers "To find through Experimentation, NATO doctrines, Simulation and Modeling all the answers In Order To improve the Capabilities and TTPs in both NATO members but also to the International Community in all challenges in the Maritime Domain".

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. How will this dependence that navies possess on information technologies affect their ability to maintain security at sea?

To operate effectively within the cyber domain, we must develop and leverage a diverse set of cyber capabilities and authorities. Cyberspace operations, information and communications networks and systems, can help detect, deter, disable, and defeat adversaries.

Robust intelligence, law enforcement, and maritime and military cyber programs are essential to enhancing the effectiveness of Maritime Operations, and deterring, preventing, and responding to malicious activity targeting critical maritime infrastructure.

We should recognize that cyber capabilities are a critical enabler of success across all missions, and ensure that these capabilities are leveraged by commanders and decision-makers at all levels.

Besides the challenges, there are opportunities for collaboration especially in the maritime domain. Alliance relies on strong and resilient cyber security policies to fulfill the core tasks of collective defence, crisis management and cooperative security. Our Partners could be engaged as well. Building a secure, trusted and humane cyberspace that empowers individuals rather than enslaves them is needed.
An eco-system driven by data and complexes must be governed by norms and codes of conduct. Cyber is the ultimate team sport where the larger the network and the more diverse the set of partnerships, the more successful you are likely to be. International actors, governments, private sector and civil society need to effectively cooperate in order to deal with the emerging threats.
We are all aware that there is no normal transition from Peace to Crisis and from Crisis to War in Maritime Interdiction Operations but also in cyber attacks. That's why we need to train as we fight in order to fight as we have been trained. There are no discounts in safety and in procedures for all of us.
While, irregular tactics and protracted forms of conflict have mostly been marked as tactics of the weak in the past, today and in the future, opponents may exploit hybrid and cyber opportunities because of their effectiveness.
The art of Cyber warfare is not found in front line maneuvers, but rather in the grey zones of security: grey is the new color of war.
Having said that allow me to highlight that the NMIOTC Cyber Conference is the ongoing commitment of NMIOTC, to tackle the cyber security issues in the Maritime Domain, which will dominate our efforts intensively, at least for the next decade. This will be another stepping stone for NMIOTC in order to engage with the international community, create opportunities for a better understanding and support cyber security at sea. All these will eventually reduce potential cyber threats to the international maritime community for the years to come.
As they say: We cannot direct the wind, but we can adjust the sails.

Stelios Kostalas
Commodore GRC (N)
Commadant NMIOTC

The International Political and Legal Framework for Addressing Hybrid Threats

by Ambassador John H. Bernhard

In this paper, I will give a brief overview of the existing international political and legal framework for addressing hybrid threats, and ways to strengthen the framework, focusing on how and in which fora the international community, and, in particular, NATO, the EU and their Member States, could contribute to such strengthening.

Mostly, the term hybrid threats is applied to a combination of military and non-military activities, which aim at achieving political objectives, e.g. undermining and destabilizing our societies and their security.

As hybrid threats are diverse, the means to counter them also have to be diverse, depending e.g. on whether we are addressing threats from States or from non-State actors like terrorists. Likewise, the means and procedures applied to counter threats depend on the type of threats, e.g. whether they come from conventional or nuclear weapons, chemical, biological or radiological weapons.

Relatively new areas of rapidly growing concern, when dealing with hybrid threats, are cyber-attacks and spreading of fake news. Obviously, these new transboundary threats and ways to defend our societies against them must also be dealt with through international cooperation, in the first place and in particular among likeminded countries like NATO and EU members and our partners. At the same time, the possibilities for a meaningful and effective cooperation with a wider circle of countries should also be considered.
I will focus on threats, which are "traditional" in the sense that they are based on various types of weapons and materials, which are already subject to some international regulation and cooperation. However, I see a clear need for the international community, to expand and strengthen the existing international framework regarding these threats, and it is important to discuss how best to do this.

Most of the international regulation and cooperation is of a general nature, and not specifically aimed at threats to maritime security, but, the extent to which general security challenges are addressed, naturally has a very strong impact on transportation aspects and therefore also on maritime security.

Which international rules are governing WMD and CBRN Material?

1. First **Nuclear Weapons:** The most important global agreement on nuclear weapons is The Treaty on the Non-Proliferation of Nuclear Weapons, often just called the NPT, from 1968. It is **the** crucial document in the efforts to prevent the spread of nuclear weapons.

Now 191 States have accepted it, i.e. the entire world community, except Israel, India and Pakistan. Originally, North Korea was also a party to the treaty, but in 1993, it cancelled its participation.

The NPT distinguishes between two categories of States, viz. **Nuclear Weapon States** and **Non-nuclear Weapon States**. A State belongs to the first category, if it has manufactured and exploded a nuclear

weapon before January 1, 1967. Only five States belong in this category: China, France, Russia the UK and the US.

The non-proliferation obligation according to the NPT basically is not to transfer to any recipient whatsoever nuclear weapons, other explosive devices or control over such weapons or devices, directly or indirectly.

Therefore, the NPT has in fact established a monopoly to possess nuclear weapons for the States that already had them, while all other States are not allowed to possess or produce them.

The so-called Nuclear-armed States, Israel, India and Pakistan , are not parties to the NPT and, therefore, not formally bound by its prohibition on nuclear weapons.

An additional group are so-called "Nuclear-umbrella States", i.e. States, which are covered by other States' nuclear weapons, like e.g. the NATO members.

The **IAEA**, i.e. The International Atomic Energy Agency in Vienna has been given the task to supervise that States fulfill their obligations in the NPT. For this purpose, virtually all States have concluded so-called Safeguards Agreements with the IAEA, thereby allowing IAEA inspectors access to control that nuclear material is not diverted from peaceful nuclear power plants to be used for nuclear weapons. To supplement the Safeguards agreements, many States have also concluded additional protocols, which give IAEA inspectors additional rights of access to information and sites.

How was it possible, in the NPT negotiations, to convince the Non-nuclear weapon States to give up the possibility to possess nuclear weapons? The price for this was mainly that the NPT should also contain an obligation about nuclear disarmament, including negotiating a treaty on general and complete nuclear disarmament.

For many years, discussions and negotiations on a general ban on nuclear weapons have been going on, without much progress, but in 2017 a **Treaty on the Prohibition of Nuclear Weapons** was adopted in the UN General Assembly, with 128 votes in favour.

None of the Nuclear-weapon States or Nuclear-armed States participated, and the NATO members also refrained from participating, inter alia because of the NATO Deterrence Strategy, which includes the possible use of nuclear weapons.

The Treaty will enter into force, when 50 States have ratified it. So far, only eight States have done that, so it is still very far from entering into force.
But in any case, the adoption of the Treaty was a major event politically and diplomatically.

Another question is whether it really would make the world a safer place? During the cold war it was often argued that the nuclear deterrence strategies of both the US and the Soviet Union provided a certain guarantee against a major military confrontation between the two military blocs, but is this argument still valid today? I think opinions are divided on the question whether the existence of nuclear weapons can have a certain peacekeeping effect in today's rather different world.

No matter how you look at that, the Treaty banning nuclear weapons has now come into existence, and the big question is, which effect and influence will it have, politically, practically, and legally ? Once it enters into force, the States Parties to it will, of course, be bound by it, while non-Parties cannot legally be bound by it. So, in the short term the Treaty will mostly have a political and symbolic significance.

A somewhat related issue, which, in practice, may pose a more likely threat to maritime security, is the illegal trafficking of nuclear material. This challenge is dealt with under the concept of Nuclear Security:

2. Nuclear Security, i.e. measures against Nuclear Terrorism

To start with, a clarification of two expressions, which may look and sound rather similar:

First, Nuclear Safety, which covers measures to protect people and property from harmful effects from nuclear facilities and materials, e.g. as in the Chernobyl and Fukushima accidents.

Secondly, Nuclear Security, which covers measures to protect nuclear facilities and materials from malicious acts by persons, typically terrorists or other criminals.

It is **nuclear security** I will deal with here, i.e. the measures taken and to be taken against nuclear terrorism.
In a speech in Prague in 2009, President Obama highlighted the threat of nuclear terrorism, calling nuclear terrorism the most immediate and extreme threat to global security. He then launched a series of Nuclear Security Summits, with more than 50 Heads of State and Government meeting in Washington D.C., Seoul, The Hague, and finally Washington D.C. again, in 2016.

Also before that speech and initiative, the threat of nuclear terrorism was well known, and so was the need to deal with it. Still, the problem had not been very high on the international agenda.
This is difficult to understand, when you take certain facts into consideration and add the ruthlessness of many terrorist groups: There is enough nuclear material in the world to build 20.000 new weapons like the one that levelled Hiroshima and almost 80.000

more like the one that destroyed Nagasaki. A grapefruit sized amount of plutonium, or enough highly enriched uranium to fit into a five-pound bag of sugar, can be fashioned into a nuclear weapon, which could instantly kill and injure hundreds of thousands of people.

But less advanced devices can also have highly dramatic effects. Only a small amount of radiological material that gives off dangerous radiation is enough to create a so-called "dirty bomb", i.e. a bomb composed of radioactive material and a conventional explosive, i.e. not a nuclear explosive. The radioactive material is dispersed by the detonation, which is less powerful than a nuclear blast, but can produce considerable radioactive fallout, which in a large city could cause fear and panic, in particular because of the threat of radiation poisoning, and it would contaminate the immediate area for some time, disrupting attempts to repair the damages. Besides, the economic losses and effects even on world economy could be enormous.
Many so-called "soft" locations, including hospitals, research facilities and factories, contain radioactive materials, which are not always kept under sufficiently secure conditions. In the US alone, there are almost 3.000 buildings containing high-intensity radioactive sources.

That we are not talking of a theoretical problem is easily seen from the fact that since the early 1990s, according to the IAEA, there have been more than 2.300 cases of illicit or unauthorized trafficking or disappearance of nuclear or radioactive materials.

In at least 18 cases, there have been thefts or losses of weapons-grade nuclear material. Especially after the collapse of the Soviet Union, such material was sometimes stolen from military installations and sold or smuggled to criminals or potential terrorists abroad. There are today no mandatory international requirements for the control of these dangerous materials or for how to transport them. The IAEA has only issued recommendations, in the form of a voluntary Code of Conduct on the Safety and Security of Radioactive Sources. The disconnect between rules for the handling of these dangerous materials and the terrorist threat leaves significant security vulnerabilities. However, many States are hesitant towards binding international regulations and control regarding these matters, which they see as belonging to the nucleus of national sovereignty.

This also influenced the Nuclear Security Summit Process, which produced a number of important results, though mostly limited to political commitments. They have certainly improved the security situation and the political attention to it, but the most important element is still lacking, viz. an international legally binding treaty on nuclear security, which obliges States to maintain effective security standards for nuclear and other radioactive materials, and which establishes a review mechanism, which can secure that common standards and other obligations are duly implemented by States. This, of course, would be an obvious task for the IAEA, as the so-called "Nuclear Watch Dog of the United Nations". Unfortunately, so far it has not been possible to achieve the support of a sufficiently big number of States to start working towards the goal of a universal legally binding Convention aimed at preventing nuclear terrorism. Hopefully, this will happen before a serious nuclear terrorist attack provides a brutal wake-up call, which would make the public, media and politicians ask, why more was not done before?
At the end of this overview some brief remarks on the rules governing Chemical and Biological Weapons.

3. Chemical Weapons

The use of Chemical Weapons goes far back in history, and especially mustard gas and chlorine gas were used for the first time as a method of warfare on a large scale during World War I, by both parties to the war. It is estimated that they caused almost 100.000 deaths and more than a mil-

lion wounded. Since then, they have been considered especially inhumane weapons, whose use is against international humanitarian law.

In the years between the two World Wars, there were several cases of use of chemical weapons, e.g. by Italy in Ethiopia and Japan in China, but during the Second World War they were not used. During the Cold War, they were produced and stored in a number of countries, and they were used in the Iraqi-Iranian war, as well as domestically in Iraq and Syria.

In 1992, a comprehensive ban on chemical weapons was adopted in the form of the Convention on the Prohibition of Chemical Weapons, which entered into force in 1997.

The Convention laid the foundation for the establishment of the OPCW, The Organization for the Prohibition of Chemical Weapons in The Hague, whose task it is to oversee the implementation of the Convention, by way inter alia of a strong inspection regime, including in cases of suspicion of violation of the Convention. In some cases, a Conference of the States Parties to the Convention may recommend collective measures, including sanctions. In particularly serious cases, the issues can be brought to the attention of the UN Security Council.

The OPCW is thus well equipped to deal with the threat of the use of chemical weapons by States.

However, the most serious threat in the chemical field probably comes less from States than from terrorists, who may not easily be able to produce or store proper chemical weapons, but might more likely get access to chemical production sites and to transportation of hazardous chemicals. Therefore, it would seem advisable, both internationally and domestically, to focus more on the level of security measures at chemical industry plants and during transportation of chemicals.

4. Biological Weapons

The usual definition of biological weapons is the "deliberate use of biological agents, e.g. in the form of bacteria, viruses, parasites or toxins to cause disease, death, disability or other related harm.

The 1975 Convention on the Development, Production and Stockpiling of Bacteriological (Biological) Weapons and their Destruction contains a total ban on biological and toxin weapons, and this is the first example of a total ban on any category of weapons.

A major weakness of the Convention, however, is that it does not provide for the creation of an international organization to monitor, verify and ensure national implementation of it, such as the OPCW for the Chemical Weapons Organization and the IAEA with regard to nuclear non-proliferation.

Conclusion

Progress to strengthen our defense against hybrid threats has been achieved. Still, much remains to be done to counter such threats, which are often of a transboundary nature and therefore call for international cooperation. This is best done by establishing comprehensive and binding international agreements and effective review mechanisms, to make sure that obligations are also implemented in practice. I believe the need for this is especially urgent with regard to measures against nuclear terrorism, which as President Obama said, is the most immediate and extreme threat to global security. I am convinced that the NATO and EU countries could play a constructive and influential role by cooperating about initiatives in this and other fields within or outside the relevant international organizations. In the beginning of such processes, it will often be difficult to convince a large number of States to take on binding obligations, and sometimes you may have to choose between a strong agreement with rather few participants or a softer one with more participating States, but the first challenge is to take the initiatives needed to get started, and I think NATO and EU members are good and credible candidates for taking up this challenge.

Curriculum Vitae
Ambassador John Hartmann Bernhard

Education:
Master's Degree in Law and Bachelor's Degree in Roman languages from Copenhagen University 1974
37 Years Career in the Diplomatic Service of Denmark 1974-2011:
Ambassadorial Postings:
Ambassador and Permanent Representative of Denmark to the OSCE (Organisation for Security and Cooperation in Europe) and the IAEA (International Atomic Energy Agency) in Vienna (2005-2011)
Ambassador to the Netherlands and Permanent Representative to the OPCW (Organisation for the Prohibition of Chemical Weapons) in The Hague (2001-2005)
Ambassador to Spain (1994-2001)
Ambassador to Venezuela (1989-91)
Postings in the Ministry of Foreign Affairs:
Legal Adviser (International Law and EU Law)
Permanent Undersecretary for Administration, Consular Affairs, Press and Information
Currently working as an Independent Adviser on International Political and Legal Issues and as a Senior Associate of the think tank "Partnership for Global Security" in Washington D.C., dealing especially with nuclear security.

An introduction to the Security Assessment for Offshore Oil and Gas Installations

by Professor NikitasNikitakos and Iosif Progoulakis (PhD Candidate) (iprogoulakis@aegean.gr), Department of Shipping, Trade and Transport, University of the Aegean, Chios, Greece.

Abstract

This paper provides an outline of security assessment for offshore oil and gas installations focusing in the use of tools to assess, identify and mitigate security risks. Statistics for the recorded security incidents for offshore oil and gas assets are briefly presented to illustrate the necessity of security assessment in the oil and gas and maritime industry. An overview of various security assessment methods is given and the more applicable ones for offshore oil and gas assets are presented. The importance of the integration of Process Safety Management and Security Assessment is highlighted. An example of a qualitative security assessment tool is given proving the necessity for a multidisciplinary approach in mitigating security hazards.

1 Introduction

Security of offshore oil and gas installations is defined as the process in which the oil and gas operational assets and the exploration and production sectors are actively and passively protected with the assistance of stringent physical and network security measures to ensure operational efficiency and minimize losses associated with security breaches. The major forces driving this need for the implementation of security measures for the protection of offshore oil and gas assets are the international legislative framework and national regulations concerning security compliance as well as the current and emerging threats to include terrorism, piracy, inter-territorial crime, etc. The aim of this article is to provide a general overview of the multi-disciplinary approach required for the security assessment of oil and gas installations. The main focus will be in physical security, the engineering and operational aspects for these assets, excluding the cyber domain. For the further analysis of the concept of Security Assessment it is important for the key terms to be understood. An offshore oil and gas installation can be defined as: “Any artificial island, facility or other device permanently or temporarily attached to the subsoil or seabed of offshore locations, erected for the purpose of exploring for, de-

veloping or producing oil, natural gas or mineral resources." (API RP 70[1]). Offshore oil and gas installations vary in shape, size and type depending on the type of work they are designed to undertake. Offshore installations can broadly be categorized in fixed structures that extend to the seabed and structures that float near the water surface. Such installations can be seen in Figures 1.0.1 and 1.0.2.

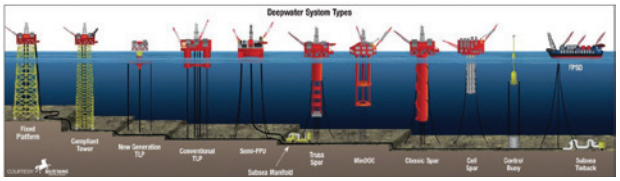


Figure 1.0.1: Deepwater installations
(© Mustang - Wood Group Company)

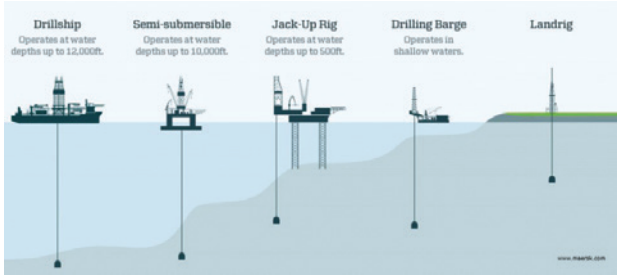


Figure 1.0.2: General overview of installations
(© www.maersk.com)

It should be noted that all offshore oil and gas installations are deployed in the maritime domain and thus suffer from being subjected to the main operational parameters and threats existing in the shipping industry. Despite their common domain of deployment though, the application of security protection measures for each of these installation can vary due to the different engineering design implemented, operation and actual layout. Also one has to consider that these installations cannot be classified as purely maritime assets but also as industrial facilities with complex and hazardous engineering processes. The application and assessment of security for these installations requires a different approach to include risk and vulnerability analysis.

1.1 Statistics, threats and effects

Here some statistics regarding the number of attacks against offshore oil and gas installations from 1899 to 2018 in various regions of the world will be presented. The information has derived from various academic sources [2][3][4].The aim of these statistics is to illustrate the existence of security incidents around the world involving offshore oil and gas installations. Figure 1.2.1 illustrates the number of documented attacks on offshore oil and gas assets in various countries of the world. Figure 1.2.2 illustrates the number and types of documented security incidents involving offshore oil and gas installations from 1899 to 2018. From the type of documented attacks it can be determined that threats can be generally categorized as: Terrorists (international or domestic),Activists, Disgruntled employees or

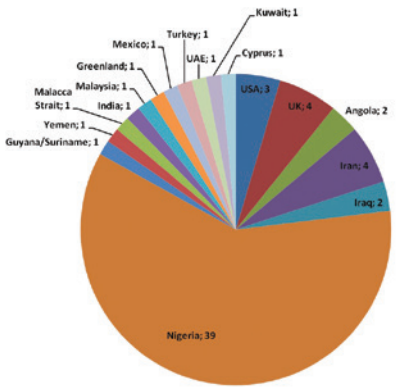


Figure 1.1.1: World security incidents (1899-2018). ([3][4][5]. Information elaborated by authors.)

contractors, Criminals (cyber criminals, pirates) and Inter-state adversaries. Adversaries initiating threats can be generally categorized in Insider or External or Colluded (Insiders working on behalf of External adversaries). Threats can be symmetric or asymmetric depending on their complexity, predictability, attack probability and severity. Considering the operational and technical complexity of the oil and

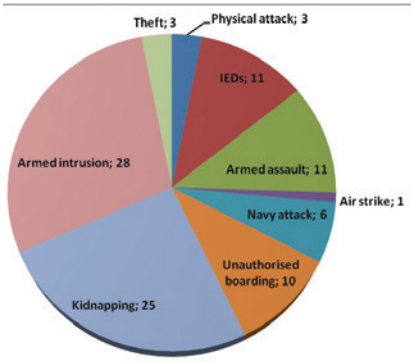


Figure 1.1.2: Types of documented security incidents involving offshore oil and gas installations (1899-2018).([3][4][5]. Information elaborated by authors.)

gas installations deployed in the offshore maritime environment, as well as industrial disasters suchas the Piper Alpha and Deep Water Horizon it is obvious to state that the effects of a security incident to offshore installations can be the following: Injury or death of personnel, Damage or loss of assets, Pollution to the environment, Disruption of oil and gas production operations, Disruption of oil and gas supply to the market, Loss of income for companies, Increase of oil prices, Effect on global economies and stock exchange.

2 Current status

A preliminary literature review in the subject of security for offshore oil and gas installations was carried out and the results that derived appeared to be scattered. The research results were compiled in two main categories: industry and government, and are described below:

2.1 Industry (e.g. industry associations, standardization organizations)

The American Petroleum Institute (API) created two major Recommended Practices, API RP 70 [1] and API RP 70I [5] in 2003. Both use the Security Vulnerability Assessment (SVA) method and are intended for oil and gas companies in preparing procedures and operations for their offshore oil and gas assets in the USA

and worldwide. Other API guidelines were published in 2004 [6] and 2005 [7] utilizing the SVA methodology in general for the petroleum industry. Finallyin 2013, the API Standard (STD) 780 [8] was published as an update to previous SVA publications. API RP 780 was intended for the petroleum and petrochemical industry and outlined a Security Risk Assessment (SRA)methodology in replacement to the previously used SVA methodology.

The International Association of Oil & Gas Producers (IOGP) has issued a number of reports and guidelines in the subject of security, acting as an advisory and recommendation body for IOGP member companies. More specifically IOGP Reports 537 [9], 512 [10] and 494 [11] tackle the issues of armed guards onboard offshore assets, security management systems and the integration of security planning and execution into an oil and gas project lifecycle.

The International Maritime Organisation (IMO) issued the International Ship and Port Facility Security (ISPS) Code in 2002 in response to the terrorist attacks of September 11, 2001 [12][13]. Along with the issue of the ISPS code the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) amendments to chapter XI-1 and a new chapter XI-2 were also implemented. In general, the ISPS Code and SOLAS 74 amendments have direct application to the offshore oil and gas sector covering however, only cargo ships, offshore support vessels (OSVs) and mobile offshore drilling units (MODU), excluding fixed oil and gas platforms and other offshore assets.

2.2 Governmental (e.g. government organizations and the military)

In the Unites States of America (USA) the initiative for the security of offshore oil and gas assets is lead primarily by the Department of Homeland Security (DHS) along with the U.S. Coast Guard (USCG) and Department of Energy (DOE).The U.S. Department of Homeland Security (DHS) treats offshore oil and gas assets in the context of Critical Infrastructure through the legislative framework of the Homeland Security Act of 2002 [14] and focuses primarily in the generic chemical industry. The DHS has also introduced anti-terrorism standards for chemical facilities [15] aiming in the implementation of protective measures and practices for designated high-risk facilities. The U.S. Coast Guard (USCG) under compliance to the Maritime Transportation Security Act of 2002 [16] and 33 CFR part 106 [17] is enforcing legislation requirements for security for offshore oil and gas assets through Navigation and Vessel Inspection Circulars (NVIC) No. 03 03 [18] and No. 05 03 [19]. Finally the U.S. Department of Energy (DOE) and Sandia National Laboratorieshave developed security assessment methodologies for chemical facilities [20].

In Canada the security of offshore installations (including oil and gas assets) is governed by the Marine Transportation Security Act (MTSA) [21] and its Marine Transportation Security Regulations (MTSR) [22]. Canada's main offshore oil and gas assets are monitored by the Canada-Newfoundland and Labrador Offshore Petroleum Board (C-NLOPB)[23] and the Canada-Nova Scotia Offshore Petroleum Board (C-NSOPB)[24]. Both entities conform to the Marine Transportation Security Act (MTSA) and its Marine Transportation Security Regulations, as well as the Government of Canada's National Critical Infrastructure Assurance Program initiative [25] assuring that these measures for protecting the security of offshore oil and gas installations and support vessels are appropriately implemented. In addition to the above offshore oil and gas operators are required to comply with the International Ship and Port Facility Security (ISPS) Code as well as the American Petroleum Institute (API) Recommended Practice 70 I (Security for Worldwide Offshore Oil and Natural Gas Operations).

The European Union (EU) covers the subject of security of oil and gas assets through the concept of Critical Infrastructure Protection (CIP). EU Directive 2008/114/EC [26] requires the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. EU Directive 2008/114/EC classifies oil and gas production facilities as critical infrastructure assets and European Critical Infrastructure (ECI) but it does not cover oil and gas exploration facilities.

In Norway the Norwegian Oil and Gas Security network, the HSE Managers Forum, and the Norwegian Oil and Gas Operations Committee, with the approval of the Director General of the Norwegian Oil and Gas Association, have issued Recommended Guideline 091 for securing supplies and materials in the oil and gas industry [27]. Other related Recommended Guidelines 104 [28] and 110 [29] relate to the cyber-security of oil and gas assets and operations.

In Australia preventive security arrangements for offshore facilities are regulated under the Maritime Transport and Offshore Facilities Security Act 2003 [30] and the Maritime Transport and Offshore Facilities Security Regulations 2003 [31]. This legislation provides a framework for operators of certain offshore facilities, ports, and ships, and a range of associated service providers, to undertake security risk assessments and implement preventive security plans.

The North Atlantic Treaty Organization (NATO) is also providing oversight in the protection of oil and gas assets of NATO member counties and allies [32, 33]. NATO implements optimization acts for critical infrastructure (including offshore assets) for member counties and provides technical, operational

and training support to enhance critical energy infrastructure protection. The NATO Maritime Interdiction Operational Training Center (NMIOTC) has also introduced training in the security of critical maritime infrastructure to include offshore oil and gas assets [34].

3 Security assessment approaches

The authors carried out further research on the different assessment approaches for security assessment. In general security for offshore oil and gas assets can be assessed using three (3) approaches:

1) Maritime Security
2) Industrial Security
3) CIP (Critical Infrastructure Protection)

Each approach uses a number of security assessment methodologies from which some are more applicable to maritime and offshore oil and gas assets than others. Below a number of more suitable methods will be presented.

3.1 Maritime security

Methodologies for maritime security assessment are the following:

a) Ship Security Assessment (SSA)/ Port Facility Security Assessment (PFSA) as described by the International Ship and Port Facility Security (ISPS) Code.

b) MSRAM (Maritime Security Risk Analysis Model) used by the United States Coast Guard (USCG).

3.1.1 International Ship & Port Facility Security (ISPS) Code

The application of the ISPS code involves three (3) major phasesto include the SSA and PFSA [12,13] as described in Figure 3.1.1.1:

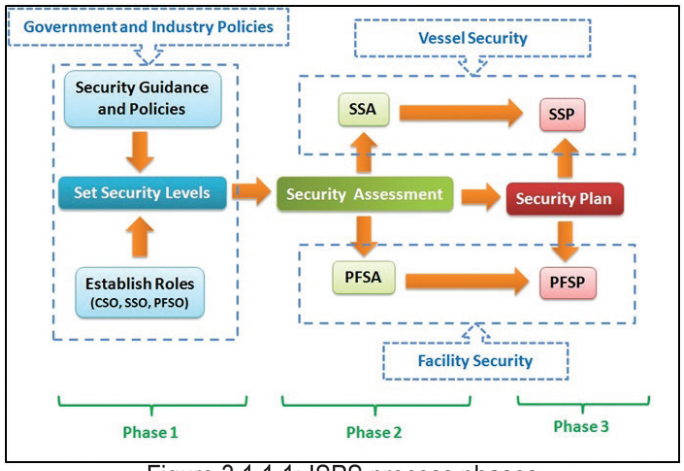


Figure 3.1.1.1: ISPS process phases

3.1.2 MSRAM (Maritime Security Risk Analysis Model)

MSRAM [35] is a terrorism risk analysis tool used by USCG to understand and mitigate the risk of terrorist attacks on targets in U.S. ports and waterways. MSRAM assesses security risk based on scenarios involving a combination of target and attack mode in terms of threat, vulnerability, and consequence. The general methodology can be found in Figure 3.1.2.1.

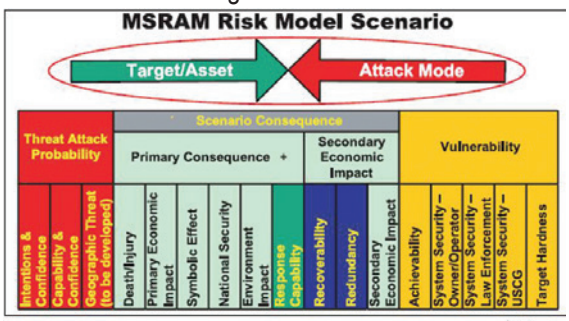


Figure 3.1.2.1: MSRAM analysis process (© USCG, [35])

3.2 Industrial security

The Industrial Security approach includes a number analysis methods to include the following [36]:

1) Security Risk Assessment (SRA)/ Security Vulnerability Assessment (SVA) (API – American Petroleum Institute),
2) VAM-CF (Vulnerability Assessment Methodology for Chemical Facilities),
3) PRAF (Process Resiliency Analysis Framework),
4) FVIKOR (Fuzzy Analytic Hierarchy Process with fuzzy Vikor),
5) VAM (Vulnerability Assessment Model)

From the above the Security Risk Assessment (SRA) and Security Vulnerability Assessment (SVA) from the American Petroleum Institute (API) will be described.

3.2.1 API Security Risk Assessment (SRA)

The Security Risk Assessment (SRA) method is described in API (American Petroleum Institute) Standard (STD) 780 [8] as a 5-step process as shown in Figure 3.2.1.1.

3.2.2 Security Vulnerability Assessment (SVA)

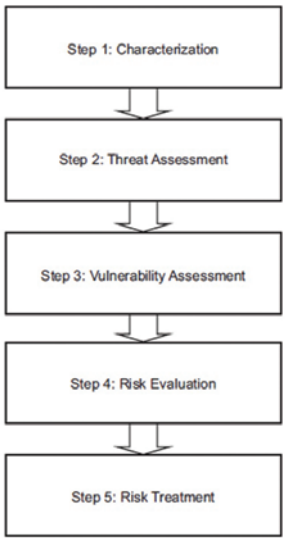


Figure 3.2.1.1: API SRA process (© API [9])

Security Vulnerability Assessment (SVA), as described by API Recommended Practices API RP 70 and API RP70I, examines a facility's characteristics and operations to identify potential threats or vulnerabilities and existing and prospective security measures and procedures designed to protect it. The SVA methodology has 5 steps as shown in Figure 3.2.2.1.

Figure 3.2.2.1: API SVA process

3.3 Critical Infrastructure Protection (CIP)

The Critical Infrastructure Protection (CIP) approach includes a number analysis methods [36, 37] to include the following:

1) RAMCAP (Risk Analysis and Management for Critical Asset Protection),
2) MBVA /MBRA (Model-Based Vulnerability/Risk Assessment) ,
3) CIMS (Critical Infrastructure Modeling Simulation),
4) CIPDSS (Critical Infrastructure Protection Decision Support System),
5) CIPMA (Critical Infrastructure Protection Modeling and Analysis,
6) BIRR (Better Infrastructure Risk and Resilience) ,
7) RVA (Risk and Vulnerability Analysis),
8) NSRAM (Network Security Risk Assessment Modeling),
9) NEMO (Net-Centric Effects-based operations Model),
10) N-ABLE (Agent-Based Laboratory for Economics),
11) MDM (Modular Dynamic Model),
12) MIN (Multilayer Infrastructure Network),
13) FAIT (Fast Analysis Infrastructure Tool),
14) EURACOM (European Risk Assessment and Contingency Planning Methodologies for Interconnected Energy Networks),
15) COUNTERACT (Cluster of User Networks in Transport and Energy relating to Anti-terrorist Activities),
16) CARVER (Criticality Accessibility Recoverability Vulnerability Espyability Redundancy),
17) CRISRRAM (CRitical Infrastructures & Systems Risk and Resilience Assessment Methodology)

From the above those methods that have a proven track record or represent a new way forward in the field of security assessment have been selected to be described briefly.

3.3.1 RAMCAP

RAMCAP [38] was developed by ASME (the American Society of Mechanical Engineers) at the request of The White House and the US DHS shortly after the attacks of September 11, 2001. RAMCAP is a bottom-up SVA process. comprised of seven (7) interrelated areas/steps of analysis as illustrated in the Figure 3.3.1.1.

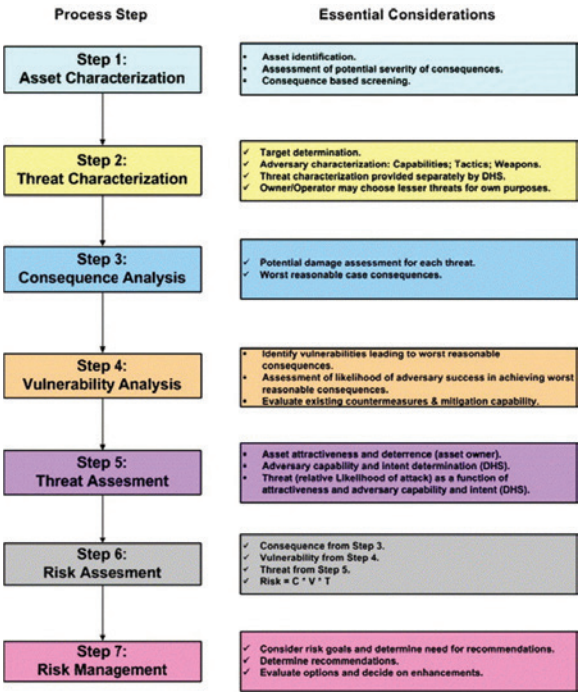


Figure 3.3.1.1: Description of RAMCAP methodology [38].

3.3.2 Model-based Vulnerability Analysis (MBVA)

The Model-Based Vulnerability Analysis (MBVA) has been developed by Ted G. Lewis [39] from the

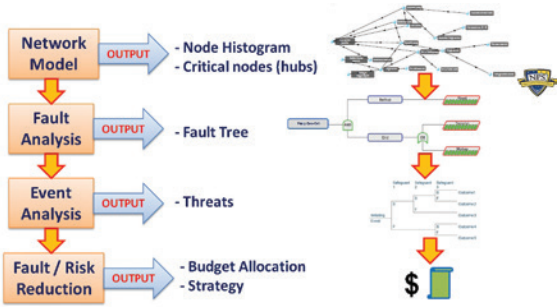


Figure 3.3.2.1: Description of Model-based Vulnerability Analysis (MBVA) methodology.

NPS (Naval Post Graduate School Monterey California) and the Center for Homeland Defense and Security (CHDS). It is also known as the Model-Based Risk Assessment (MBRA) technique and it calculates risk, computes optimal resource allocation, and simulates single-asset failures and their resulting cascade effects on networks. In MBVA, hubs are identified, hub vulnerabilities are

organized and quantified using a fault tree, all possible outcomes are organized as an event tree, and then an optimal investment strategy is developed that minimizes risk. MBVA is a 4 (four)step stage process as described in Figure 3.3.2.1.

3.3.3 CRitical Infrastructures & Systems Risk and Resilience Assessment Methodology (CRISRRAM)

Critical Infrastructures & Systems Risk and Resilience Assessment Methodology (CRISRRAM) was developed by the EU JRC (European Union Joint Research Council) [36, 37] after a thorough assessment of all relevant risk assessment methods for Critical Infrastructure. It adopts a system of systems approach and aims to address issues at asset level, system level and society level.It follows an all-hazards approach and was developed considering gaps of existing risk assessment methods in the industry and to be applicable nationally and internationally.CRISRRAM functions within three layers of approach: Society, Asset and System. Figure 3.3.3.1 shows a generic layout of the CRISSRAM methodology.

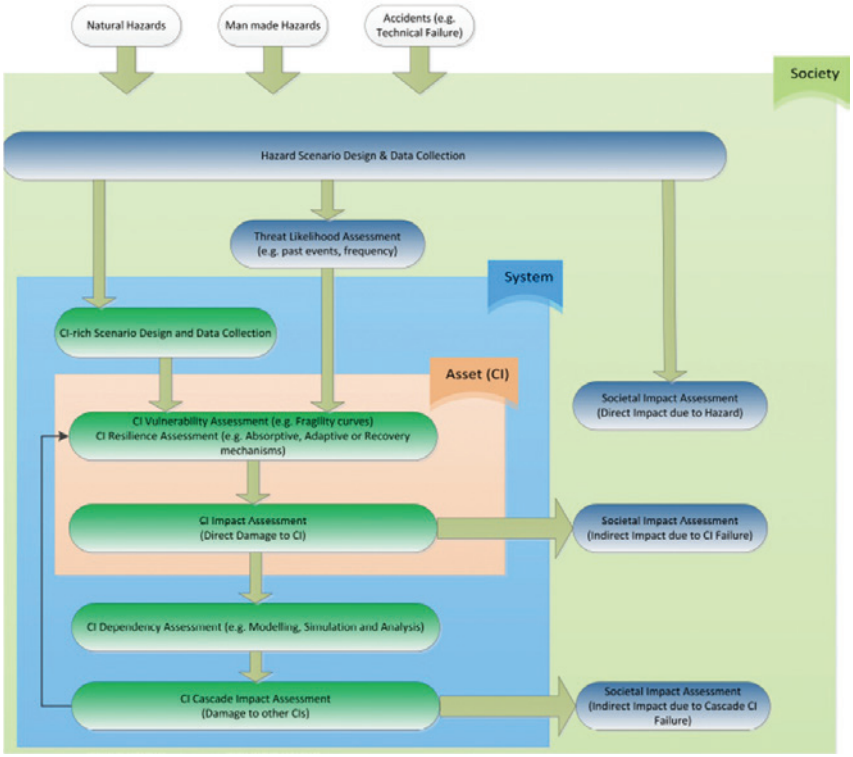


Figure 3.3.3.1: CRISSRAM methodology layout.

4.0 Security Assessment and Process Safety Management (PSM)

4.1 Process Safety Management (PSM) basics

Process Safety Management (PSM) involves the review of safety utilizing quantitative and qualitative methods to define risks, hazards and consequences of security incidents in offshore oil and gas systems, equipments, processes and operations.

The quantitative process review methods include [40]: Checks lists, PHA (Process Hazard Analysis), What-If reviews, HAZOP (Hazard and Operability) review, Bow-Tie Analysis(BTA and barrier analysis).

The quantitative process review methods include [41]: ETA (Event Tree Analysis), FTA (Fault Tree Analysis), FMEA (Failure Modes and Effects Analysis).

It needs to be highlighted that Safety hazards such as system failure, poor reliability and security threats such as sabotage, physical attack and subsequent damage of systems/ equipment, cyber attacks, have the same preventive barriers (such as procedures, processes, systems, etc) and consequences (such as catastrophic failure, fire, explosion, loss of containment, environmental spill, loss of life, etc). So Process Safety Management (PSM) and Security Assessment and Management for oil and gas assets have the same objectives: to protect the asset, the operations, the personnel and the environment.

4.2 Example of PSM tool for security assessment

Bow-Tie Analysis can be utilized for the identification of security barriers and measures for assets in the micro-

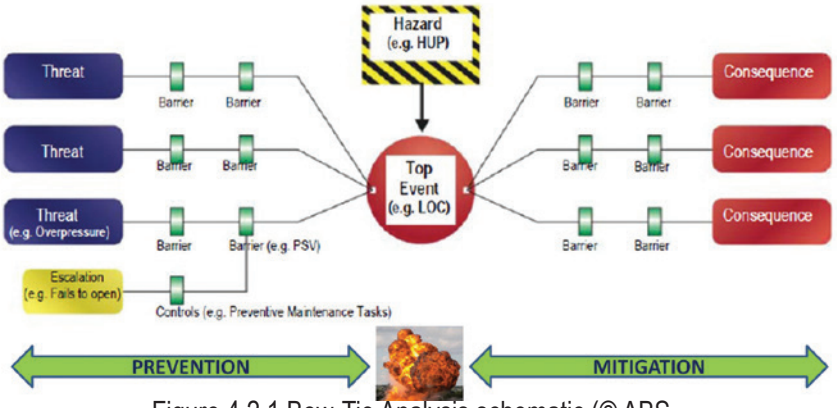


Figure 4.2.1 Bow-Tie Analysis schematic (© ABS, with information edited by the authors)

and macro- scales.

- Micro-scale: components, equipment, sub-assemblies, instruments
- Macro-scale: assemblies, assets, larger equipment

Bow-Tie Analysis (BTA) is a type of qualitative safety review [40] where cause scenarios are identified and depicted on the pre-event side (left side) of a bow-tie diagram. Credible consequences and scenario outcomes are depicted on the post-event side (right side) of the diagram, and associated barrier safeguards are included. The 'Bow Tie' Model illustrates the importance of both preventive and recovery measures in dealing with risk. In Bow-Tie Analysis, Risk is defined as the likelihood that a Top Event (hazard release) will occur, combined with the severity of the consequences of the event. Figure 4.2.1 shows an example of a Bow-Tie Analysis schematic.

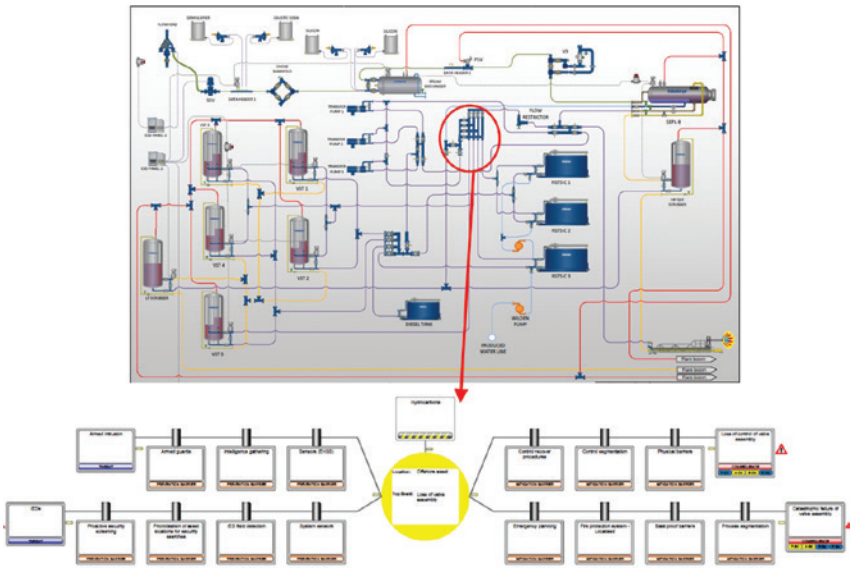


Figure 4.3.1 Bow-Tie analysis example

The main reasons the use of the Bow-Tie Analysis method is suggested are the following [41]:

- Simple & pragmatic approach
- Emphasis on effectiveness of risk reduction measures
- Effective visualization
- Allows better communication of hazards
- Can be applied for all types of hazards
- Increasingly becoming the preferred techniques by regulatory bodies & leading companies
- Efficiently aided by user-friendly software

Bow Tie Analysis is one method among many. It does not replace any specific method. It does present though an effective methodology to assess security hazards, risks, consequences and mitigation.

4.3 Bow-Tie Analysis example for security assessment

An example of the use of Bow-Tie Analysis will be described below focusing in the micro-scale of an asset.The example involves a valve assembly in an offshore oil and gas asset (FPSO, platform, etc) which is critical to the upstream (exploration and production) phase of operations. This valve assembly controls the flow of hydrocarbons to various systems, storage tanks, valves, pumps, etc. See Figure 4.3.1 for details.Two possible security incident scenarios will be investigated: 1) Armed intrusion and take over of valve assembly. 2) Planting of an IED to damage the asset.The Top Event is the loss of the valve assembly meaning the disruption or ending of the upstream operations. The consequences are the loss of control and the catastrophic failure of the valve assembly.

The prevention and the mitigation barriers for the threats and consequences respectively, for both types of scenarios, are presented in Figure 4.3.2.

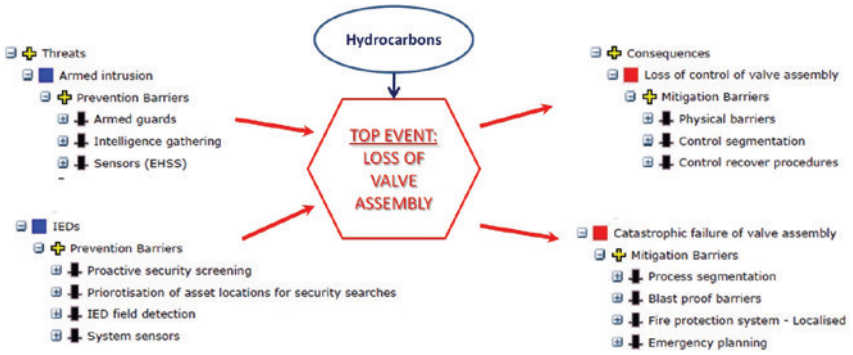


Figure 4.3.2 Bow-Tie Analysis example details

5 Conclusion

It is important to understand that Safety and Security are terms with common disciplines, deficiencies and preventive and mitigation barriers. For the efficient and successful assessment of security for offshore oil and gas assets, a multi-disciplinary approach where safety, maritime and engineering operations are analyzed and protected, has to be considered. Any use of security assessment methods shall consider the industrial complexity and the subsequent interrelation of systems, equipment and operations. The incorrect assessment of security risks can lead to a series of domino effects within the offshore oil and gas assets which can lead to catastrophic failure, the loss of lives and harm to the environment.

6.0 References

1. API RP 70: Security for Offshore Oil and Gas Operations, American Petroleum Institute, March 2003.
2. Mikhail Kashubsky, "Offshore Petroleum Security: Analysis of Offshore Security Threats, Target Attractiveness, and the International Legal Framework for the Protection and Security of Offshore Petroleum Installations", PhD Thesis, Australian National Center for Ocean Resources and Security, Faculty of Law, University of Wollongong, Australia, 2011.
3. Global Terrorism Database, The University of Maryland (USA): https://www.start.umd.edu/gtd/
4. Global Terrorism Research Project, The Political Science Department, Haverford College (USA): http://gtrp.haverford.edu/
5. API RP 70I: Security for Worldwide Offshore Oil and Gas Operations, American Petroleum Institute, March 2003.
6. Security Vulnerability Assessment Methodology for the Petroleum and Petrochemical Industries, American Petroleum Institute, October 2004.
7. Security Guidelines for the Petroleum Industry, American Petroleum Institute, April 2004.
8. API Standard (STD) 780: Security Risk Assessment Methodology for the Petroleum and Petrochemical Industries.
9. IOGP Report No. 537: Effective guard force management –Principles and guidelines, International Association of Oil & Gas Producers (IOGP), Revision July 2015.
10. OGP Report No. 512: Security Management System – Processes and concepts in security management, International Association of Oil & Gas Producers (IOGP), Revision July 2014.
11. OGP Report No. 494: Integrating security in major projects – Principles and guidelines, International Association of Oil & Gas Producers (IOGP), Revision April 2014.
12. "International Ship and Port Facility Security (ISPS) Code and Solas Amendments 2002", International Maritime Organisation (IMO), 2002.
13. Herbert-Burns, Rupert, Sam Baterman and Peter Lehr, Lloyd's MIU Handbook of Maritime Security, CRC Press, 2009.
14. The Homeland Security Act of 2002, U.S. Public Law 107–296, 107th Congress, Nov. 25, 2002.
15. U.S. Department of Homeland Security Guidance Document: Risk-Based Performance Standards Guidance: Chemical Facility Anti-Terrorism Standards, Department of Homeland Security, Office of Infrastructure Protection, Infrastructure Security Compliance Division, May 2009.
16. The Maritime Transportation Security Act of 2002, U.S. Public Law 107–295, 107th Congress, Nov. 25, 2002.
17. Code of Federal Regulations, Title 33, Chapter I, Subchapter H, Part 106 - Marine Security: Outer Continental Shelf (OCS) Facilities
18. U.S. Department of Homeland Security, U.S. Coast Guard, Navigation and Vessel Inspection Circular (NVIC) No. 03-03: Implementation Guidance For The Regulations Mandated By The Maritime Transportation Security Act Of 2002 (MTSA) For Facilities, Change 2, 28 February, 2009.
19. U.S. Department of Homeland Security, U.S. Coast Guard, Navigation and Vessel Inspection Circular (NVIC) No. 05-03: Implementation Guidance for the Maritime Security Regulations Mandated by the Maritime Transportation Security Act Of 2002 For Outer Continental Shelf Facilities, Change 2, 15 December, 2003.
20. NCJ 195171 U.S. Department of Justice Special Report: A Method to Assess the Vulnerability of U.S. Chemical Facilities, U.S. Department of Justice, Office of Justice Programs, National Institute of Justice, November 2002.
21. Transport Canada. "Marine Transportation Security Act". December 15, 2016. http://www.tc.gc.ca/eng/marinesecurity/regulations-362.htm
22. Transport Canada. "Marine Transportation Security Regulations". December 15, 2016. http://www.tc.gc.ca/eng/marinesecurity/regulations-363.htm
23. Canada-Newfoundland and Labrador Offshore Petroleum Board (C-NLOPB). "Requirements Respecting the Security of Offshore Facilities". December 1, 2016. www.cnlopb.ca/pdfs/secfac.pdf
24. Canada-Nova Scotia Offshore Petroleum Board (C-NSOPB). "Safety Directive: Security of Offshore Installations and Facilities". April 4, 2011. www.cnsopb.ns.ca/pdfs/Security_Directive.pdf.
25. Public Safety Canada. "National Strategy for Critical Infrastructure". December 10, 2016. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-eng.aspx
26. European Council. "Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection". November 10, 2016. http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1483530166126&uri=CELEX:32008L0114.
27. Norwegian Oil and Gas Recommended Guidelines No: 091: Securing Supplies And Materials In The Oil And

Gas Industry, Norwegian Oil and Gas Association, Revision no: 3 Rev date: 01.09.2015.
28. Norwegian Oil and Gas Recommended Guidelines No: 104: Information Security Baseline Requirements For Process Control, Safety And Support ICT Systems, Norwegian Oil and Gas Association, Revision no: 05 Date revised: 15.01.2009
29. Norwegian Oil and Gas Recommended Guidelines No: 110: Implementation Of Information Security In Process Control, Safety And Support ICT Systems During The Engineering, Procurement And Commissioning Phases, Norwegian Oil and Gas Association, Revision no: 02 Date revised: 15.01.2009
30. Maritime Transport and Offshore Facilities Security Act 2003, Office of Legislative Drafting and Publishing, Attorney-General's Department, Canberra, Australia.

31. Maritime Transport and Offshore Facilities Security Regulations 2003, Office of Parliamentary Counsel, Canberra, Australia.
32. NATO. "Emerging threats to maritime energy infrastructure". January 2, 2017. http://www.nato.int/cps/en/natohq/news_124544.htm?selectedLocale=en
33. NATO. 'NATO's role in energy security". October 22, 2015. http://www.nato.int/cps/natolive/topics_49208.htm
34. http://www.nmiotc.nato.int/files/DNPOW%202019%20(updated%2013%20Nov%202018).pdf
35. Maritime Security Risk Analysis Model, USCG brochure. Available at: http://aapa.files.cms-plus.com/PDFs/MSRAMBrochureTrifold.pdf
36. Georgios Giannopoulos, Roberto Filippini, Muriel Schimmer, "Risk assessment methodologies for Critical Infrastructure Protection. Part I: A state of the art", JRC Science and Policy Report, 2012.
37. MarianthiTheocharidou, Georgios Giannopoulos, "Risk assessment methodologies for critical infrastructure protection. Part II: A new approach", JRC Science and Policy Report, 2015.
38. David A. Moore, Brad Fuller, Michael Hazzan, J. William Jones, "Development of a security vulnerability assessment process for the RAMCAP chemical sector", Journal of Hazardous Materials, Vol.142, pp 689-694, 2016.
39. Ted G. Lewis, "Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation", 2nd Edition, John Wiley & Sons, 2015.
40. Dennis P. Nolan, Safety and Security Review for the Process Industries, Gulf Professional Publishing, 2012.
41. Syed ZaifulHamzah (ABS Consulting), "Use Bow Tie Tool for Easy Hazard Identification", Presentation to the 14th Asia Pacific Confederation of Chemical Engineering Congress, 2012.

Curriculum Vitae

Prof. N. Nikitakos is a graduate of Hellenic Naval Academy (1980) and holds a B.Sc. in Economics (University of Piraeus 1986) and 2 M.Sc. from Naval Postgraduate School, Monterey, CA, USA (M.Sc. Electrical Engineering. and M.Sc. in Appl. Mathematics). He spent 25 years as Naval Officer (Captain H.N. ret.) He received a Ph.D. in Electrical and Computer Engineering from National Technical University of Athens (1996). He is Professor of Shipping Informatics and Communications. He holds 3 international patents and he was awarded from Lloyd's List on Maritime Technological Innovation. He has published 5 books and many articles in international referred journals and conferences. He holds ISPS, PMP and PMI-RPM certifications.

Mr. Iosif Progoulakis is a PhD candidate in the Department of Shipping, Trade and Transport of the University of the Aegean in Greece. His subject of research is the security for offshore and maritime assets focusing in the oil and gas sector. He holds a Bachelor's degree (BEng Hons) in Mechanical and Electrical Engineering from the University of Lincoln, UK, an MPhil in Advanced Composite Materials from the University of Plymouth, UK and a Post Graduate Certificate from the Aristotle University of Thessaloniki in Offshore Structures. He is currently working as a Design Manager for NAVFAC (Naval Facilities Engineering Command) at U.S. Navy Naval Support Activity Souda Bay in Crete, Greece. His experience stems from the oil and gas, aerospace, processing and construction industries in the U.K. and Greece. He has worked for Shell, GKN Aerospace Services, Kimberly Clark and the USN.

EXPLORING THE ISSUE OF MARITIME DOMAIN AWARENESS IN GHANA

by By Michael Agyare Asiamah & Dimitrios Dalaklis

Abstract

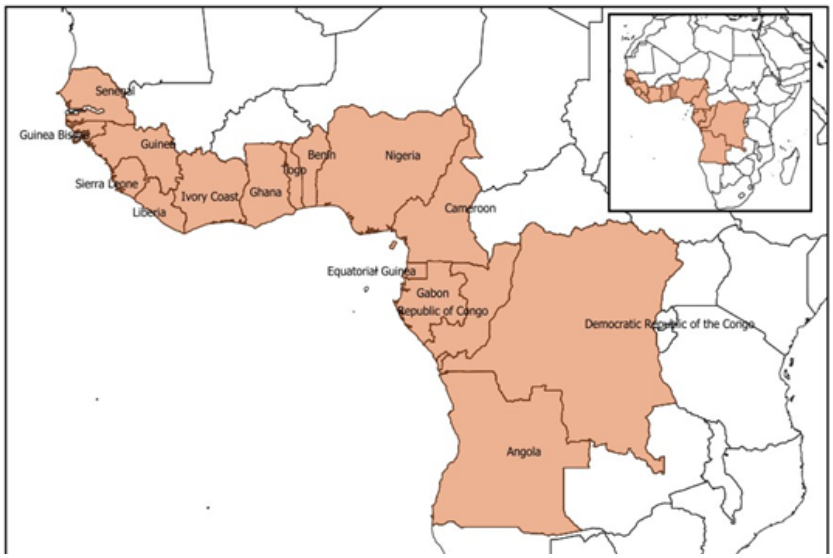
The analysis in hand is discussing how certain relevant agencies collaborate in the issue of Maritime Domain Awareness (MDA) in order to enhance safety and security in the (maritime) space of Ghana in particular and the Gulf of Guinea in general. The purpose was to investigate Ghana's MDA capabilities, ascertain the current technical and operational capacity and to bring to the fore major challenges that prevent effective collaboration between those agencies, while identifying workable solutions. This research effort further identified the actions/initiatives required to improve the conduct of maritime safety and/or security operations by the law enforcement agencies in the country under discussion. Conclusively worth highlighting is that it is necessary to increase Ghana's maritime security capacity by appropriately taking advantage of the current MDA available tools within Ghana's maritime related agencies and optimize performance by establishing a framework of special cooperation and standard operating procedures applicable to all relevant stakeholders.

Introduction

The Gulf of Guinea (GoG) is a rather busy shipping area; it connects an extended number of countries and also provides a major source of revenue for oil producing countries along its coastline. It is located partly in the North and partly in the South Atlantic Ocean, along the Western and Central African coasts with 17 coastal and 2 island states, as illustrated in Figure 1. The heavy maritime traffic within the GoG region is associated with safety, security and environmental challenges to the coastal and island nations.

With an increasing number of vessels operating in the GoG, regulatory and law enforcement agencies are under pressure to mitigate pressing problems such as Illegal, Unreported, Unregulated (IUU) fishing, piracy and armed robbery as well as the trafficking of drugs and people, and transport of illegal goods by sea (Hoyle, 2015). The Republic of Ghana, being the gateway to West Africa and a new entrant in the production of oil in commercial quantities, has a vested interest in the developments within the region. As a result, there is an important role to play in addressing maritime safety and security issues in the GoG.

Ghana is a littoral State located in West Africa. The country shares a border with Togo to the East, Cote d'Ivoire to the West, Burkina Faso to the North and the GoG to the South. Its coastline of 300 nautical miles (nm) is stretching from Aflao on the East to New Town on the West. Because of its diverse maritime interests, Ghana has established 12nm of Territorial Waters, followed by 12nm of Contiguous



Zone, resulting in a 200nm Exclusive Economic Zone (EEZ) (CIA, 2018) and 350nm Continental Shelf (Daily Graphic, 2018), in full accordance with provision of UNCLOS , as depicted in Figure 2. Shipping and sea-borne trade are vital to the economic development of the country with nearly 90% of both imports and exports carried through the sea lines of communication (Shou, 2017).

Figure 2: Ghana's maritime boundary
Source: Created by authors, as a modification from Ghanaweb.com

The territorial waters of Ghana abound in enormous natural resources, including fisheries, minerals and hydrocarbon deposits. Moreover, Ghana has become a major maritime trading hub for West Africa in recent years (GPHA, 2015). It is indicative that since 2010, there has been the issue of oil production in commercial quantities, with several explorations still on-going in the western part of the EEZ. The protection of the oil installations and vessels engaged in the vibrant fishing industry as well as tourism and other commercial activities have created the need for constant monitoring of the maritime area.

This research effort, among other things, sought answers to what Ghana's policies and priorities on MDA are, what Ghana's current MDA capabilities and assessments are, what challenges the various maritime stakeholders face in collaboration and information sharing, whether adequate training has been given to operators of the various MDA tools, and how the situation could be improved.

3. Ghana's Maritime Safety and Security Threats

Ghana's maritime domain has changed significantly in the last decade. The discovery of hydrocarbon deposits has created a different economic environment and has become the engine of national progress. Ghana like any other GoG country, is faced with increasing maritime safety and security threats, evident among them being piracy (Dalaklis, 2012). The major threats mostly identified in the maritime domain of Ghana include the following:

Environmental. The effect on the environment of the activities associated with oil production (oil pollution), illegal discharges from ships as well as illegal dumping is enormous and the necessary attention must be given. Pollution of the environment by the exploration/drilling of oil is mainly in the form of oil spillage into the sea, accidental discharges at sea and the accidental spill process of the oil. Finally, the dumping of toxic waste must be included in the complete environmental protection equation.

Fisheries. The fishing industry in Ghana is threatened with extinction as a result of over-fishing and IUU. Industrial fishing vessels are not allowed to fish in the Inshore Exclusive Zone, which corresponds to areas from the coastline to 6nm seaward or below 30m depth, while artisanal fishing canoes are permitted to fish within those areas. However, many industrial fishing vessels simply defy this provision, resulting in the depletion of the fish resources. Often, IUU fishing fleets illegally scoop-up hundreds of millions of dollars' worth of fish from Ghanaian waters, a basic reason why import restrictions were imposed on Ghana's fisheries products in 2012 and 2013 by the European Union (EU) (MOFAD, 2014).

Illegal Bunkering/Crude Oil Theft. Illegal bunkering includes the purchase of illegally acquired or refined oil products mostly at cheaper rates. It is typically acquired from stolen oil and the destruction of oil pipelines with criminal intent for mischief or for

monetary gains. It also involves the diversion of crude and refined products by unauthorized persons at sea. When companies continue to patronise these cheap products, illegal bunkering has the tendency to increase criminal activities like piracy and armed robbery at sea (Akah and Dalaklis, 2017). It is against this backdrop that MT Mammy Mary and MT Metrix 1 were both arrested by the Ghanaian Navy when they illegally traded oil consignment about 5nm from Tema Harbour on 14 April 2018 (Ocloo, 2018).

Piracy/Robbery at Sea. Piracy and robbery at sea are set to be on the rise in the GoG region at an alarming rate (IMB, 2018), surpassing that in the Horn of Africa. These pirates and robbers usually target ships' crews, cargo and other valuables. The first quarter of 2018 saw a string of 22 piratical attacks in the GoG region, in the maritime domains of Ghana (1 hijacked), Benin (2 hijacked) and Nigeria (1 hijacked), with very high success rates (IMB, 2018). The number of incidences surpassed those from all other regions in the first quarter of 2018.

Trafficking. Ghana in 2016 was identified among the major cocaine transit points, with about 61% being transported out of the country by sea (UNODC, 2016). Drug trafficking, a transnational crime, has an impact on national security and is also directly related to other types of organised crime such as money laundering and terrorism. Moreover, it has the potential to corrupt state institutions and to affect the stability of state systems and society. Also, humans and weapons may be trafficked through Ghanaian waters if criminals find that these waters are not properly secured.

2. The Yaoundé Code of Conduct

The Code of Conduct concerning the repression of piracy, armed robbery against ships and illicit maritime activity in West and Central Africa, also widely known as the Yaoundé Code of Conduct, was adopted at the Yaoundé summit in Cameroon on 25 June 2013. This regional framework is an initiative of Economic Community of West African States (ECOWAS), Economic Community of Central African States (ECCAS), the Gulf of Guinea Commission (GGC) and the Maritime Organisation of West and Central Africa (MOWCA), and contains a comprehensive strategy that seeks to counter maritime threats within the GoG region (IMO, 2013).

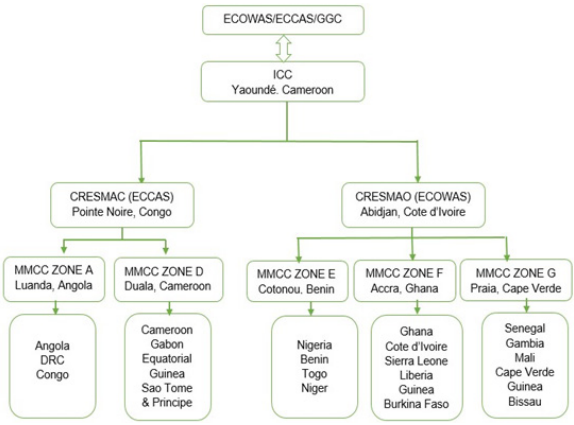


Figure 3: Gulf of Guinea Information Sharing Architecture
Source: Created by the authors

This Code of Conduct brings signatory states together to take appropriate measures to combat maritime threats, in accordance with international standards, and also commit to maritime information sharing among states. It is of interest to note that the leading pillar of the strategy is interoperability between stakeholders to gather timely intelligence and share it among themselves at national or international levels. Through that, the various countries have developed and operationalized Maritime Operation Centre (MOC) for their navies and/or coast guards, to facilitate information sharing.

For effective monitoring and enforcement capabilities, the Inter-Regional Coordination Centre (ICC) was established at the strategic level to implement the regional integrated strategy for maritime safety and security, contained in the Yaoundé Code of Conduct. At the sub-regional level, there is the establishment of the Regional Maritime Security Centre for Central Africa (CRESMAC), located in Pointe-Noire, Republic of the Congo for the ECCAS region. In addition, the Regional Maritime Security Centre for West Africa (CRESMAO), located in Abidjan, Cote d'Ivoire serves the ECOWAS region. The multi-national level has a zonal approach system, established to coordinate activities within the zones known as Multi-National Maritime Coordination Centres (MMCC). These centres group states together, to pursue common maritime security interests. The national level, represented by MOCs of the various representing countries, will be required to contribute immensely and work towards the realisation of the overall aim of the integrated maritime strategy.

3. Agencies Concerned with Issues of MDA in Ghana

MDA involves the interaction between several maritime agencies confronted with the challenge of ensuring safety and security as well as clean and environmentally friendly seas (Bueger, 2015). It is interesting to note that each one of these agencies has its specific mandate, internal bureaucracy and organisational culture. The problems encountered with internal red-tape are often translated into the national level. The maritime stakeholders are cross-sectoral in nature. The agencies include the Ghana Maritime Authority (GMA), the law enforcement agencies (Navy, Police) and other regulatory agencies (Environmental Protection Agency (EPA), Monitoring, Control and Surveillance (MCS) unit of the Ministry of Food and Agriculture (MOFAD), Ghana Ports and Harbours Authority (GPHA), National Security

Coordinating Council (NSCC), National Disaster Management Organisation (NADMO) and Narcotics Control Board (NACOB)).

4. Initiatives Contributing to MDA in Ghana

Piratical attacks (including armed robbery at sea) have been increasing in the GoG region at an alarming rate since 2007, with incidences exceeding a quarter of worldwide reported attacks. Maritime insecurity in the region affects the transport of about 5 million tons of oil per day, which is more than half of Africa's total production per day and about 30% of the United States of America's oil imports (Vircoulon and Tournier, 2014). To address the situation, there have been a series of political level initiatives by member states of the region to implement a regional strategy for the safety and security of the maritime domain of both West and Central Africa. For Ghana, of particular interest was the operationalisation of a Vessel Traffic Monitoring Information System (VTMIS). The main components of the VTMIS in Ghana are Eight (8) Remote Sensor Sites (RSS) located along the coast of Ghana from East near Togo to West near Cote d'Ivoire (GMA, 2014), with all associated infrastructures explained below:

Eight (8) Remote Sensor Sites (RSS) located along the coast of Ghana from East near Togo to West near Cote d'Ivoire. The RSS are equipped with radio communication towers, radars, Automatic Identification System (AIS) receivers, as well as Closed Circuit Television (CCTV) for detecting and identifying ships and fast moving boats. The sites are equipped with marine radio communication equipment i.e. MF/HF and VHF, which complies with the International Maritime Organisation (IMO) standard provisions for Global Maritime Safety and Distress Systems (GMDSS) and Long Range Identification and Tracking (LRIT) to enable regular receipt of ship reports.

Three (3) Remote Base Stations for inland waterways located along the River Volta.

Three (3) Area Control Centres for the West, Central and East sectors, and one (1) National Control Centre sited in Accra.

There are provisions to further equip the RSS with meteorological and hydrological sensors. When that equipment are integrated in the system, it will provide local weather data from the respective sites to the Control Centres for broadcasting.
The data gathered from the Remote Sites is transmitted to the Control Centres. The VTMIS operators are then able to display that vessel traffic information on screens.

The Ghanaian Navy has established its VTMIS control station at the headquarters in Accra, with two (2) other monitoring stations in Tema and Takoradi respectively. The Tema port which is operated by GPHA, NSCC, MCS and NACOB also have monitoring stations to monitor vessel traffic. In addition, there are provisions for Monitoring Station facilities to be implemented in the Takoradi port. The system is yet to be reconfigured for Customs, Immigration and the Marine Police; this will be performed after they have all relocated to their new offices in various locations. It is of interest to note that a control centre can utilize all the functionalities of the VTMIS equipment, while monitoring centres have limited use of functionalities like flagging a vessel of interest.

5. Ghana's Maritime Operations Centres

For the Ghanaian Navy to perform its functions well, surveillance and intelligence gathering is pivotal. For that reason, the US Navy in various forms assisted the Ghanaian Navy to set up three (3) Maritime Operation Centres (MOCs). There is a main national MOC located in Accra. There are also the East MOC in Tema and West MOC in Takoradi. Plans are in place for two (2) additional MOCs to be established in locations near the borders to the East and West. With the VTMIS framework, the national MOC has a "control centre" status, while the others are only monitoring centres. The MOCs are further equipped with the "SeaVision" and "Time Zero" Coastal Monitoring Systems, provided by the US Navy. "SeaVision" is a surveillance system that was specifically developed for the US Navy and allied partner nations to coordinate and track vessels of interest around the world. "Time Zero" coastal monitoring system is a maritime surveillance solution that is optimally configured for the coastal surveillance of Ghana.

6. Vessel Monitoring Systems (VMS)

To ensure food security and sustain the socio-economic development of the country, the MCS department of MOFAD operates a Vessel Monitoring System (VMS) to control fishing vessel activities for the protection of Ghana's fishing stock. The use of this VMS is intended to curb the problem of overfishing, so that Ghana's fishing stock will not be woefully depleted. A VMS is usually employed by fisheries regulatory authorities for the monitoring of position, course and speed, including time at position, of registered fishing vessels (Interpol, 2014). Unlike AIS, VMS data is limited to the government agency that installed it. All industrial fishing trawlers in Ghana are mandated by law to install VMS transmitters on-board. With that provision, the MCS is able to monitor the activities of the fishing fleet and query any suspicious activity the vessels may engage in. The vessels' details are transmitted even 72 hours after the transmitter is tampered or destroyed by criminals at sea so that authorities will be able to

track the vessel in all circumstances.

7. Challenges of Collaboration for MDA in Ghana

Ghana acknowledges the importance of MDA in its activities; in response, there is equipment operated by various maritime agencies to enhance MDA capabilities in its waters. However, there is no formally documented Policy on this issue. It was identified that the lack of a comprehensive and clear Maritime Strategy seems to prevent agencies from effectively cooperating. Without a maritime strategy, which should outline the roles and responsibilities of GMA and other maritime agencies, there is no guidance for these agencies, so cooperating with other parties/ stakeholders is not mandatory to them. It is of interest to note that during the current research effort, it was identified that the various systems supporting information collection and handling are not interoperable because they were purchased from different manufacturers and for purposes independent of each other.

It was also identified that the coastal communities and Non-Governmental Organisations (NGOs) concerned with maritime activities have very little or even no knowledge about MDA. However, every activity that happens at sea spans from land. If the coastal communities and local fisher associations are effectively involved in sharing vital information, intelligence can be gained about illicit maritime activities, like armed robbery and piracy; this is essential in order to intervenes even before these criminals proceed toward the sea.

Unfortunately, Ghana does not prioritize the maritime environment as key to economic prosperity. On the positive side, the government of Ghana acknowledges the importance of transportation in supporting the productive sector of the economy. Because of that, an Integrated Transport Plan for Ghana was developed in 2011. The plan, which was hoped to inform the budgetary allocation of government for the entire transport sector, effectively outlines policies for air, rail, road, urban, motorised and intermediate forms of transport. Strangely enough, however, the plan barely touched on maritime transport even though it is recognized that plans are not legally binding on agencies. However, the significance of maritime transport for the development and prosperity of Ghana was emphatically recognised.

GMA admits shortages in its regulatory capacity as well as insufficient financial resources. There is also a shortage of local skills and capacity in the administration and management of the maritime sector that suggests the tendency to depend on foreign technical and financial support. The Ghanaian government admits that the new oil and gas discovery poses several challenges for the maritime transport sub-sector. It has, therefore, directed the GMA to develop regulations and enforcement mechanisms and procedures in good time. However, whilst GMA is already mandated to coordinate these activities, it faces additional challenges caused by the multi-agency environment in which maritime regulation is developed and enforced.

It was further identified that apart from diverse national interests spearheading collaboration through exercises and combined training during multinational initiatives, Ghana maritime stakeholders on their own do not organise any form of activity that enhances cooperation. To say the least, it is upsetting for these agencies, to allow any external actor to bring them together instead of initiating collaborative efforts themselves. It is only Exercise Obangame, intended for cooperation among countries in the GoG, which brings maritime stakeholders in Ghana together for a combined exercise. The GMA should institute an "internal programme" that helps in exercising the various surveillance systems for enhanced interoperability.

Also, the current contractual clauses are not favourable to the continuity of operations of the surveillance systems. Most of the contractual agreements require the systems to be remotely configured after minor breakdowns, and an expert to be flown in from abroad to fix major problems. Constant monitoring of activities at sea will be adversely affected when there is any type of breakdown that takes days or extended number of hours to be rectified. If there is a delay in travel arrangements or internet connection problems, the case will even be worsened.

Conclusion

Shipping activities within the GoG, and especially the maritime space of Ghana have increased significantly since 2007, when Ghana started to produce oil and gas in commercial quantities. Other reasons include expanded fishing activities, as well as the fact that Ghanaian ports of Tema and Takoradi serve as important transit hubs for neighbouring land-locked countries, especially Burkina Faso. As a matter of fact, there have been commensurate safety and security issues within the maritime domain of Ghana. To help in the surveillance of the maritime space and enforce maritime laws, various maritime agencies in Ghana operate different and unfortunately not integrated maritime surveillance systems.

This research effort was conducted in order to investigate the Ghanaian MDA capabilities and to identify the challenges in collaboration between these maritime agencies, policies and priorities on MDA, current MDA capabilities, also to pin-point surveillance operator training requirements and finally, to suggest ways of improvement. However, this study was limited to maritime surface surveillance alone; a thorough study is further recommended encompassing aviation, as well as under-water activities in order to holistically mitigate

safety and security problems in the maritime space of Ghana.

The Yaoundé Code of Conduct is a regional initiative from ECOWAS and ECCAS to help curb piracy and armed robbery against ships plying the route within the GoG region. The Code entreats interoperability between maritime stakeholders and effective sharing of maritime information. This regional aim cannot be realised if similar collaboration is not effective at the national level. The surveillance systems employed in Ghana have all the needed tools, including coastal radars, cameras, AIS receivers and LRIT embedded for effective monitoring of the maritime environment. However, the major maritime agencies like GMA, the Ghanaian Navy and MCS unit of MOFAD operate independent surveillance systems to monitor their various areas of interest. Therefore, the issue of "interoperability" and promoting cooperation, even via a "top-down" approach enforced by a national policy/guideline document are clearly standing out as priorities.

There is the perception that collaboration between these maritime agencies is effective. However, case studies reviewed indicate lack of effective cooperation between the agencies due to the absence of a national maritime policy. Even combined maritime exercises that bring the agencies together, like Exercise Obangame Express, are spearheaded by external actors/ interests. An all-encompassing maritime policy will document clear-cut roles for the maritime agencies, with the idea of achieving the national objective.

During the overall Master Thesis effort, questionnaires were administered to various maritime agencies and the responses were duly analysed. The observations and findings have been presented in line with the research objectives. The findings were summarized and necessary conclusions drawn. It was deduced that Ghana has a satisfying level of MDA capabilities that can help to deal with safety and security threats in its maritime domain. That notwithstanding, there is certain room for improvement.

In any case, technology is just a tool to enhance maritime safety and security, but a good level of performance will not be achieved until authorities take the necessary action to show commitment and willingness to document policies and procedures that can help harness the potential of technology. If the suggested remedial actions provided are implemented, most importantly when a national maritime policy is documented and sanctioned by the legislature, all the maritime stakeholders will be bound by law to adhere to the provisions of that document. They will be obliged to swiftly collaborate and ensure a collective effort to enhance maritime safety and security.

Recommendations

Ghana, as a littoral country, needs an all-encompassing Maritime Strategy, with an MDA policy clearly described in that document. This can be done when risk assessment is carried out to ascertain the best plan of action for each anticipated threat, with the corresponding roles of various maritime agencies in each plan of action clearly stipulated. It is recommended that authorities expedite action in developing and documenting strategies for effective MDA.

Once this strategy is approved and adopted, agencies will need to follow the associated strategic directives and work together to formulate implementation plans through harmonized procedures, policies, and Standard Operating Procedures (SOPs) that would be in line with the strategy. When that is accomplished, Interagency Working Groups could be assembled to devise Interagency MOCs, joint task forces and other groups to work in a harmonized manner to tackle maritime challenges. No single agency can achieve success in the domains of maritime safety and security alone.

One way to achieve inter-agency cooperation is to establish political or legislative top-down inter-agency directional approach to maritime issues. However, it becomes cumbersome if every issue is handled this way, and is subject to whim or politics in terms of which main issue is most important. A better way is to get all agencies together and outline a comprehensive list of national concerns, then work together to agree on how to address them, with required resources clearly allocated. Subject-matter expert exchanges and joint training are helpful in understanding the structure and workings of other agencies. In this case, the maritime agencies could agree to a framework outlining the biggest threats, key shortfalls in addressing those threats and available resources to address them.

Prioritizing maritime issues within government policies is also recommended. One of the most effective measures maritime agencies can take is to make sure that policy decision makers understand the importance of maritime safety and security to the greater economy of Ghana and the impact on the average Ghanaian. In that stead, "maritime oriented" seminars specifically designed for the attendance of politicians and government officials are of high urgency and importance. It is typical to focus more on land-based priorities because those tend to be more pressing and affect the day-to-day lives of citizens. Piracy, oil spills, illegal fishing and other maritime issues have huge negative impacts, but may not have direct impact on the average citizen. It is, however, the responsibility of the maritime agencies to communicate to government overseers and citizens the role that MDA and the maritime environment play in their economic well-being. Without this, the agencies will be acting in isolation and will never get the necessary resources to address

the problems.

It is further recommended that surveillance operators are trained on information technology and cyber security. There is the need to ensure that people with criminal intent do not tamper with the information exchange within the surveillance systems. It is a fact that system manufacturers have certain security features in place. Nonetheless, operators should be trained to identify spurious activities or any tempering with the systems, and be able to effect repairs in order to ensure system integrity for effective surveillance.

It is strongly recommended to conduct regular multi-agency exercises and drills in order to enhance multi-agency cooperation. Effective decision making is based on accurate information, transmitted in good time. Exercises together will go a long way to improve timely information sharing, and reduce agencies' response time to incidents. This could mitigate the negative effects of safety or security issues in the maritime space of Ghana. It will help avoid misunderstandings between agencies and possibly reduce response time of Maritime Interdiction Operations (MIO) when the need be.

A joint national maritime operations centre, that mimics the Maritime Multinational Coordinating Centre of the GoG information sharing architecture, should also be established. This centre can be staffed with representatives from all maritime agencies, and through these representatives, information sharing among the agencies could be enhanced. Staff who work at this centre can be posted to the MMCC and CRESMAO in rotation. The experience of the staff in the national centre will be beneficial when such persons are employed at the sub-regional and regional maritime centres.

Furthermore, it is recommended that certain contractual clauses are reviewed to favour continuity of operations of the surveillance systems. This stems from the fact that most of the agreements require the systems to be remotely configured after minor breakdowns, and an expert flown in from abroad to fix major problems. Instead, this arrangement could be changed for locals to be trained, and equipped with the proficiency to work effectively on those systems to fix any problem that develops on them.

Finally, another important issue for consideration is that, there could also be a network with fisher associations, fishing communities and association of fishing canoe owners created, so that they can report any illegal activity they sight at sea (Human Intelligence – HUMINT). Arrangements could be made with telecom companies to provide a dialling short code for easy reporting. This network could also be complemented by certain incentives: for example, the maritime agencies could provide life jackets or marine radios as reward for those who swiftly report incidents with malicious intents. With this arrangement, any illicit activity that goes unnoticed by the surveillance systems could be identified once sighted by the fishing canoe operators.

References

Akah Judith and Dimitrios Dalaklis. (2017). Violence within the Maritime Domain of the CEMAC Region. Maritime Interdiction Operations Journal, 17-27.

Bueger, C. (2015). From Dusk to Dawn?: Maritime Domain Awareness in Southeast Asia. Contemporary Southeast Asia: A Journal of International and Strategic Affairs, 37(2), 157-182. Retrieved from muse.jhu.edu

CIA. (2018, April 18). Retrieved from The World Fact Book: https://www.cia.gov/library/publications/the-world-factbook/geos/gh.html
Daily Graphic. (2018). Retrieved from Graphic Online: www.graphic.com.gh

Dalaklis, D. (2012). Piracy in the Horn of Africa: Some good news but a lot of work has still to be done. Maritime Security Review, 2-8.
Ghanaweb. (2018, 3 24). Retrieved from ghanawebonline: www.ghanaweb.com

GMA. (2014). Ghana Maritime Authority. Retrieved from http://www.ghanamaritime.org

GPHA. (2015). Ghana Ports and Harbours Authority. Retrieved from www.ghanaports.gov.gh

Hoyle, W. (2015). Global Maritime Domain Awareness for Pollution Monitoring. Journal of Ocean Technology, 10(2), 53-57.

IMB. (2018, August 16). ICC IMB Piracy Reporting Centre. Retrieved from Live Piracy Report: https://www.icc-ccs.org/

IMO. (2013). Prevention and Suppression of Piracy, Armed Robbery Against Ships and Illicit Maritime Activity in the Gulf of Guinea. London: International Maritime Organisation.

INTERPOL. (2014). Study of Fisheries Crime in the West African Coastal Region.

MOFAD. (2014). A National Policy for the Management of the Marine Fisheries Sector.
Ocloo, P. (2018). Navy, NPA impound 2 vessels over illegal oil transfer. Dailygrahic.com.gh.

Shou, M. (2017). Maritime Economics. Malmö: World Maritime University.

United Nations Office on Drugs and Crime (UNODC). (2016). World Drug Report . New York: United Nations Publication.
Vircoulon T. and Tournier V. (2014). Gulf of Guinea: A Regional Solution to Piracy? Retrieved from http://blog.crisisgroup.org/africa

Further Reading

Chintoan-Uta M. and J. R. Silva. (2016). Global maritime domain awareness: a sustainable development perspective. WMU Journal of Maritime Affairs, 16(1), 37–52. doi:10.1007/s13437-016-0109-5
Chintoan-Uta, M. and Silva J. (2017). Global Maritime Domain Awareness: A Sustainable Development Perspective. WMU Journal of Maritime Affairs, 16(1), 37-41.
Dalaklis, D. (2017). Improving Maritime Situational Awareness: Establishing a "Maritime Safety and Security Network". 8th NMIOTC Annual Conference 2017, (pp. 24-32). Chania. doi:10.13140/RG.2.2.24614.32329
Dalaklis, D. (2017). Safety and Security in Shipping Operations. In V. I. P, Shipping Operations Management (pp. 197-213). Malmo: Springer.
Gasu, W. (2011). Maritime Security and Safety in the Gulf of Guinea: Tackling the Challenges of Piracy and Other Maritime Transnational Threats in the Gulf of Guinea. Accra: University of Ghana.
Ifesinachi, K. and Nwangwu, C. (2015). Implementation of the Yaounde Code of Conduct and Maritime Insecurity in the Gulf of Guinea. Research on Humanities and Social Sciences, 5(21), 54-64.
Kamal-Deen, A. (2015). The Anatomy of Gulf of Guinea Piracy. Naval War College Review, 68(1), 93-118. Retrieved from http://digital-commons.usnwc.edu/nwc-review/vol68/iss1/7
Ofosu-Boateng, N. R. (2017). Oil, Risk Analysis Techniques, Maritime Security and Safe Passage in Pirate Infested Gulf of Guinea Waters. Open Journal of Social Sciences, 5(12), 98-109. doi:http://doi.org/10.4236/jss.2017.512008
Vance Capt George et al. (2006). Maritime Domain Awareness: The key to maritime security. (A. G. Jr., Ed.) The Coast Guard Journal of Safety and Security at Sea, 63(3), 2-90. Retrieved from https://www.dco.uscg.mil/Portals/9

BIOGRAPHY
NAVAL LIEUTENANT MICHAEL AGYARE ASIAMAH

I am Naval Lieutenant Michael Agyare Asiamah, born on 28 February 1983 in Kumawu in the Ashanti Region of Ghana. My parents are Samuel Mensah Asiamah and Yaa Serwaa. I had my primary and junior secondary school education at St Paul's R/C Primary and JSS, in Kumasi in the Ashanti Region of Ghana from 1989 to 1998. I proceeded to Osei Tutu Secondary School for my Senior Secondary School Certificate Examination, where I read Science from 1999 to 2001. In 2003, I gained admission into the All Nations University College, Koforidua in the Eastern Region of Ghana. I graduated in 2007 with a Bachelor of Science (Hons) in Computer Science.

I was enlisted into the Ghana Military Academy as a Naval Cadet on 16 October 2008. I commissioned into the Executive Branch of the Ghana Navy on 3 September 2010. I have since attended a number of military courses. Notable among these are Pre-Sea Deck course at the Regional Maritime University, Combat Officers Qualifying Course in SAS Simonsberg, South Africa. Others include Intelligence Train the Trainer Course in Ghana, Vessel Traffic Service Course in Finland and Legal Aspects of Maritime Border Security as well as Maritime Operations Law in Ghana.

The following are the key appointments I have held in the Ghana Armed Forces:

- Watch keeping Officer on board Ghana Navy Ship GARINGA from May 2012 to April 2013.
- Executive Officer onboard Ghana Navy Ship BLIKA from January 2014 to June 2014.
- Officer in Charge of the Maritime Operations Center at the Ghana Navy Headquarters from July 2014 to December 2015.
- Executive Officer onboard Ghana Navy Ship GARINGA from January 2016 to September 2016.
- Officer in Charge of Naval Intelligence at the Western Naval Command from October 2016 to May 2017.
- Assistant Director of Strategic Intelligence at the Defense Intelligence Department of the Ghana Armed Forces from June 2017 to September 2017.
- Assistant Command Operations Officer with additional responsibility as the Officer in Charge of the Maritime Operations Center at the Eastern Naval Command.

Currently, I am studying at the Ghana Armed Forces Command and Staff College for my Junior Staff Course.

I hold a Master of Science Degree in Maritime Affairs, specializing in Maritime Safety and Environmental Administration from the World Maritime University (WMU), Malmo, Sweden. I am a Fellow of the Friends of Sasakawa, WMU.

I am happily married to Celestine Agyare Asiamah and we are blessed with 3 children. My hobbies include swimming, listening to music and playing badminton.

Combined Cyber and Physical Attacks on the Maritime Transportation System

by Fred S. Roberts, Dennis Egan, Christie Nelson, RyanWhytlaw
CCICADA Center, Rutgers University

Abstract

For years, there has been discussion about physical security in the maritime transportation system (MTS). That discussion has led to standards, regulations, etc. In recent years, there has been an increasing interest in cyber security in the MTS that has led to discussions about best practices for cyber security. It is likely that many future attacks on the MTS (and other systems) will be multi-modal, including both a cyber and a physical component. As a simple example, hacking into security cameras at a port increases vulnerability to a physical intrusion. Thus, a cyber attack could be a precursor to a physical attack, and in fact the opposite could also be the case. This paper presents scenarios of combined cyber and physical attacks and describes ways to understand their likelihood based on ease of attack and seriousness of potential consequences.

1. Introduction

For years, there has been discussion about physical security in the maritime transportation system (MTS). That discussion has led to standards, regulations, etc.

In recent years, there has been an increasing interest in cyber security in the MTS (DiRenzo, Drumhiller, Roberts, 2017). This has led to the discussions about best practices for cyber security.

It seems clear that "conventional warfare" of the future will include a cyber component as well as a physical component. Indeed, publicly available military strategy from China, for example (Segal, 2017, The State Council Information Office of the People's Republic of China, 2015), indicates that the Chinese military expects to seize information dominance at the beginning of a conflict through cyber attacks.

Similarly, it is likely that future attacks on the MTS will be multi-modal, including both a cyber and a physical component (Tucci, 2017). As a simple example, hacking into security cameras at a port increases vulnerability to a physical intrusion. Thus, a cyber attack could be a precursor to a physical attack, and in fact the opposite could also be the case.

This paper resulted from the question of how the U.S. Coast Guard (USCG), or a vessel or facility operator, can identify and evaluate potential synergies between cyber and physical vulnerabilities to result in a holistic security assessment - including consequence management? We address this question by presenting scenarios of combined cyber and physical attacks, and discussing ways to understand their likelihood based on ease of attack and seriousness of potential consequences.

Our ideas result from the input of a variety of subject matter experts

(SMEs) from the U.S. Coast Guard, the U.S. Secret Service, the Transportation Security Administration, various U.S. ports, and a public utility commission. A list of SMEs is included as an Appendix.

2. A Simple Example: Fake News to Create a Distraction

We concentrate first on ports. The first set of scenarios are based on the ideas that "fake news" could be spread via social media. For example, multiple messages could say that something is happening at Pier F in the port. This would draw first responders to Pier F. (As one SME put it, an analogy is youth soccer: Everyone runs to the soccer ball.) The actual intent is to attack Pier L, which now may have less protection because first responders at the port mass at Pier F. Another version of this would be for an attacker to hack into a company's or agency's email system and generate an official-looking report about Pier F. Still a third version is to spread the news that a celebrity is at Pier F (numerous messages saying, e.g., that Justin Bieber is at Pier F). Here, the intention is not to draw first responders away from another location, but it is to draw a crowd at a given location and then to attack the crowd with a physical attack.

A port facility protection plan should prevent leaving one area unguarded as in the first two fake news scenarios. A response plan would also require understanding how defenders can mitigate a tsunami of false reports. Could they plan for ways to get out their own messages? Would those messages possibly have a fast enough impact based on a torrent of fake news messages?

There are physical versions of this idea of using cyber methods to create a distraction. For example, we learned of an example where Hezbollah attacked first responders in Israel by first setting off an IED in a car, drawing first responders to a muster point, and then attacking the muster point with a bigger bomb.

Another model is that an adversary could create a distraction in the water, drawing police boats and USCG vessels to the area, leaving another part of the port unprotected.

3. Cyber Attacks on Operating Systems in the Port

There are many conceivable ways that a cyber attack on an operating system in a port could result in making a following physical attack more likely to succeed. Some examples are:

- Shut the gates so people are trapped inside and first responders are trapped outside.
- Turn off the lights to make it easier for physical attackers.
- Turn off the alarms to make it easier for physical attackers to avoid detection.
- Disable the cameras to make it easier to avoid detection.
- Interrupt the power supply to create a distraction.
- Disable cyber-enabled traffic lights to create traffic jams so that emergency vehicles are unable to respond to a physical attack.
- Hack into emergency communication system and tell first responders to go to a different place.
- Spoof TWIC cards or other access control systems to let the "bad guys' in.

Many of these seem feasible. (We discuss them more next.) However, an adversary with this level of sophistication might find it is easier to do a more intrusive physical break-in as the preliminary attack prior to a more serious physical attack. This is a central point: When we consider, potential scenarios for combined cyber and physical attacks, the likelihood of a given scenario needs to be taken into consideration. More generally, one should consider threat, vulnerability, and consequence in determining the risk of a given attack scenario. Not surprisingly, the SMEs we talked to did not always agree as to likelihood or risk.

To get into more detail, we note that disabling cameras may have a high level of risk because they are often add-ons. The ability to hacking into the emergency communications system depends upon how it is configured. If is connected to the Internet, it is certainly possible. Jamming communications might be easier. One SME felt that port security would quickly determine that hacking into the emergency communications systems was indeed a hack and would limit first responders going to the wrong place. A Denial of Service Attack could turn off the lights or the alarms. A cyber attack on the power supply could have significant consequences since many terminal operations do not have backup generators.

At some operating ports, one system handles all gates. At others, there are individual gate controls. Which is less vulnerable? By sheer size, ports might not be so vulnerable to access control hacks; airports or schools or hospitals might be more vulnerable. Moreover, doors or gates locked by access control systems are supposed to have overrides for life safety, typically a mechanism to break the circuit. So this scenario might be less likely since the "bad guys" wouldn't buy much time and so the likelihood of their trying it might be small.

Do ports have plans to respond quickly to these various cyber scenarios that could be preliminary to a physical attack? The speed with which first responders could respond would depend upon the port's Facilities Security Plan. It might also depend on the MARSEC level.

4. Port Security can Create Vulnerabilities

Efforts to make our ports more secure

might in fact create unexpected vulnerabilities. Large sports and entertainment venues use walkthrough metal detectors or other systems to screen patrons. The long lines waiting to be screened create vulnerabilities. After the 2013 Boston Marathon attacks, sports stadiums sought to minimize vulnerabilities by creating an outer perimeter with initial screening.

Similarly, at a cruise ship terminal with many ships leaving at roughly the same time, lines form outside the building. Passengers are initially vetted to see if they have a valid ID and are at the right terminal. An attacker should not get past the screener. (Unless they bought a cheap ticket just to get inside.)

The 2017 attack at the Ariana Grande concert in the Manchester Arena showed that patrons leaving an arena could be vulnerable. What if they were "drawn out" in a group by hacking into the arena's emergency communication system or "message board"? This has raised the awareness in the venue security community about vulnerabilities of patrons leaving a venue.

In general, it is thought that debarking at cruise ship terminals does not have as many vulnerabilities as embarking. Passengers are released in groups to avoid standing in line at customs. There is good departing security. Operators think you are ok once you leave the dock. But what if a hacker could manipulate an alarm system to get them all to debark at the same time? There is still an under-appreciation of debarking vulnerabilities at ports.

Could a hacker manipulate an alarm system (e.g., fire alarm) and perhaps a communication system to get passengers to debark at the same time? That might depend upon whether the alarm system and communication system were online. Port fire alarm systems are not too sophisticated. They are designed to operate over a network and push a signal out to a monitoring agency. It might be a challenging hack to get into this system. Physically setting off the fire alarm might be more likely to succeed. Even if a "bad guy" could get the fire alarm going, would this create the desired problem? If a fire alarm goes off in a cruise ship port, there are many people trained to direct passengers where to go. Those people would more likely be used than an audible emergency message. So the scenario of additionally hacking into a communication system is not very likely to have the desired effect.

In some port systems, if a fire alarm goes off, certain doors open up. Thus a physical attack on the alarm system could create access to an attacker seeking to introduce malware into a port operations or cargo handling system. So, physical attacks can be the precursor to cyber attacks, not just vice versa, and one needs to be aware of this possibility.

5. Taking Advantage of Port Congestion

Port congestion is a big problem in all ports. Large container vessels add to the congestion problem. It used to be that several smaller vessels in port at the same time – using different terminals. Now there is one large one – requiring all of its unloading/loading at one terminal. The scheduling of trucks picking up or delivering containers is controlled by a cyber system. A simple denial of service attack could impact the ability to offload a large ship in a timely way. This would result in traffic jams in the port area. In turn, that could create the possibility of having a serious impact by throwing a bomb.

6. Autonomous Vehicles in Ports

Terror attacks using vehicles are on the rise, witness recent such attacks in Berlin, Nice, London, and New York. The lines of passengers lining up to embark on cruise ships could be vulnerable to this type of attack. But terrorists ended up dying in the process. What if they could control a vehicle remotely and not risk dying? Would that make this type of attack even more likely?

Car hacking in which "bad guys" remotely take control of your car to steal it or use it as a weapon is certainly already feasible. For instance, in 2013, Miller (Twitter) and Valasek (IOActive) demonstrated how to take control of a Toyota Prius and Ford Escape from a laptop. They were able to remotely control smart steering, braking, displays, acceleration, engines horns, lights, etc. (Greenberg, 2013). This becomes a serious issue as in-car technology becomes more sophisticated. Indeed, there are already thousands of semi-autonomous cars – modern cars are more like bundles of computers on wheels. And fully autonomous cars are coming.

Already, many ports are operating with autonomous vehicles. At the Long Beach container terminal, a gantry crane operator brings a container to an autonomous truck. A computer lowers the container to the truck, which takes it to a storage area or a non-autonomous truck. Autonomous trucks even monitor their battery life and drive themselves to charging station for a recharge – operated by a robot. The Hampton Roads container terminal is completely automated, robotic, and intermodal (rails, cars, trucks). Cranes are run from an office. All vehicles are autonomous. Could an autonomous truck be used as a weapon in a port scenario? It is technically possible. An adversary could use low-cost jammers to jam the GPS that makes the autonomous vehicle work. GPS jamming is possible with low cost jammers available over the Internet (though illegally). Many devices are battery-operated or can be plugged into a cigarette lighter and cost as little as $20.The hacking

might seem harder to do than hijacking a truck and driving it into the port to create havoc. Also, where autonomous trucks operate in a port, they are blocked from people, so would more likely damage infrastructure. This suggests that the risk of this scenario is not so high, both because it would be easier to do something different and because the consequences of the original scenario might not be that high, at least in terms of human life. However, automated vehicles in ports create other problems. Could a "bad guy" hack into the control system and arrange to put the "wrong" box on the wrong train, or take it to the storage facility and open it?

Unmanned aerial vehicles might be a much bigger risk to a port than unmanned trucks. Ports have a great deal of hazardous material readily attacked from the air (LNG, gasoline, etc.) Prof. Todd Humphreys of UT Austin has demonstrated how GPS signals of an unmanned aerial vehicle can be commandeered by an outside source (Cockrell School of Engineering, 2012). How do you mitigate against hackers taking over a drone and dropping it on hazardous material? You can't knock it out of the air because that itself could cause it to drop on hazardous material. Ports don't have authority to take over a drone and take it down.

A drone could also be a threat to a vessel entering or leaving a port. Could an attacker hack into a drone and have it land on the deck of a nearby cruise ship? You might cause some panic this way. A scenario with a large impact would be to load it with explosives and have it land on the deck and then create an explosion.

7. Hazardous Materials in Ports

As noted above, ports have or host a lot of hazardous materials. As a case in point, gigantic LNG ships enter directly into the city of Boston to dock at the LNG terminals in Boston Harbor. It is one of the few ports in the world (and only one in US) where this happens. Could a cyber attack on an LNG ship cause it to careen off course and create an explosion? This is not likely – there are tugs on it and the Coast Guard keeps other vessels away.

However, once the ship is in the terminal, if an adversary could access its industrial control systems, they could cause a serious problem. There are pumps, valves, etc. (operational technology – OT) run by software/ computers (IT systems). Hacking into those systems could conceivably lead to an explosion in light of the hazards from LNG. How likely is this scenario? At least one of our sources had this as his nightmare scenario.

Maybe this isn't so far-fetched. The Stuxnet is a malicious computer worm that targets industrial computer systems. It put a virus into a controller running centrifuges and damaged them – causing substantial damage to Iran's nuclear program (Zetter, 2014). Similarly, an adversary could hack into a sensor system, e.g., affecting tank level indicators, pressure sensors, temperature sensors, hazardous gas sensors. A leak or build-up of pressure or a fire might not be detected, thus possibly leading to an explosion. Recently, Naval Dome described how a hacker could penetrate numerous machinery control systems on a vessel. We discuss this in Section 10.

To add to the discussion of hacking into sensor systems, we note that sensor systems other than those used on a vessel could also be hacked. An explosion or fire started at some other port facility from a hack into a sensor system could serve as a distraction and make it easier to succeed with a physical attack. A bad actor could also hack into the system to set off a false alarm that could serve as a distraction. Could an adversary start a cyber attack by first physically starting some hazardous materials on fire or releasing noxious gases, creating a diversion? This might allow them to gain access to a facility and hack into it.

8. Cargo

Modern port operations, around the world, are heavily dependent on complex networked logistics management systems that track maritime cargo from overseas until it has reached a retailer. Yet, these systems are subject to cyber attacks that can cause significant problems.

The Port of Antwerp is one of the world's biggest. During 2011-2013: Hackers infiltrated computers connected to the Port of Antwerp, located specific containers, made off with their smuggled drugs and deleted the records. Attackers obtained remote access to the terminal systems; released containers to their own truckers without knowledge of the port or the shipping line. Access to port systems was used to delete information as to the existence of the container after the fact. The hackers began by emailing malware to the port authorities and/or shipping companies. After the infection was discovered and a firewall installed to prevent further infections, the criminals broke into the facility housing cargo-handling computers and fitted devices allowing wireless access to keystrokes and screen shots of computer screens. The first part of this was a cyber attack preceding a physical attack (stealing cargo). The second part was a physical attack (breaking in) preceding a cyber attack, which in turn preceded a physical attack (stealing cargo). (See Bell, 2013, CyberKeel, 2014, Pasternack, 2013, Wagstaff, 2014.)

There have been other examples of cyber attacks followed by physical attacks (stealing cargo). In 2012 it was revealed that crime syndicates had penetrated the cargo systems operated by the Australian Customs and Border protection. The

penetration of the systems allowed the criminals to check whether their shipping containers were regarded as suspicious by the police or customs authorities. The consequence was that containers with contraband were abandoned whenever such attention was identified by the criminals. Others could be handled without worrying about the police. (See CyberKeel, 2014.)

The Iranian shipping line IRISL suffered from a cyber attack in 2011. The attack damaged data related to information such as cargo number, rate, loading information, date, place, etc. The result was that it was impossible to know where containers were, even whether they had been loaded, and whether they were onboard ships or onshore. The data was eventually recovered, but there were major disruptions in operations, including cargo sent to wrong destinations and lost cargo. The results were severe financial losses. (See CyberKeel, 2014.)

9. Blocking the Port Entryway

Could an adversary block entry to a port from the water through a cyber attack? The chokepoint for a port is the channel. Blocking it could create a big problem. Consider for example the Kill van Kull in New York – if an adversary could cause a vessel to run aground there, this would create a huge problem. If an adversary could do this, they could create a great deal of economic damage if the port remained closed for a period of time.[1]
In a bad case, the port could remain closed for a year or more. (It took 20 months to get the grounded Costa Concordia cruise ship off the rocks in 2013 – Mackenzie, 2013. An adversary could also divert port resources to clearing the blockage, and possibly create an opening for a following physical attack e.g., through a bomb in the port. At the least, they might create huge traffic jams, not allowing emergency vehicles to enter to counter that physical attack.

Autonomous vessels are coming. Could an adversary hack into such a vessel as it approaches a port and cause it to ram into another vessel or a bridge? Or run it aground, thereby blocking the entryway to a port? Could they choose one loaded with LNG for maximum damage? One SME told us this was not likely. There are alarms and warnings that you would have to bypass. Would port authorities overcome mistrust of automated systems to allow an autonomous vessel to operate in congested or treacherous waterways? In San Francisco, for example, the eddy current can make your bow veer towards a bridge abutment and there is not much tolerance for variance from the intended path. Would the pilots union allow the vessel to enter the port without a pilot?

Another SME thought this scenario was feasible. One complex attack would be to spoof a ship's Automatic Identification System (AIS) to arrange it so awareness systems are not transmitting a problem. AIS tracks ships automatically by electronically linking data with other ships, AIS base stations, and satellites. This system enables ships to share positional data with other ships. It offers awareness about those operating within the MTS. An attacker could exploit weaknesses in AIS and falsify a vessel's identity or type, or its position, heading, and speed, as well as to hide problems. (See Mullin, 2014, Zora, Zora, and Kucan [2013.) Spoofing AIS and arranging no transmission could allow a "bad guy" to take over an autonomous vessel and run it hard aground. It is unlikely defenders could mitigate the impact of such an event if they saw it happening. You can't interdict very well on the water. There are few options except to ram the vessel running out of control – which could also cause an explosion.

Recently, Naval Dome, an Israeli company, showed that it was feasible to attack the ECDIS (Electronic Chart Display and Information System) of a vessel. They designed an attack to change the vessel's position during a "night-time passage through a narrow canal." Their attack left the ECDIS display looking completely normal while the actual situation was not and, if fully implemented, would have sent the vessel aground. The "position, heading, depth and speed" all looked different from what they really were. The attack took place through the captain's computer, "which is regularly connected to the internet through a satellite link, which is used for chart updates and regular logistic updates." (See AJOT, 2017.)

Baraniuk (2017) describes a cyber attack on the ECDIS system of a ship in an Asian port. Malware was introduced into the computers of a large 80,000 ton tanker when a crew member used a USB stick to print some paperwork. Later, a second crew member used a USB stick to update the ship's charts, and the ECDIS was infected. Luckily, this was caught and the main damage was delayed departure.

[1] Disruption of the MTS could cause billions of dollars in damage to the economy. During the month of January 2015, the ports on the West Coast of the United States were closed due to a labor stoppage and the impact on the economy was dramatic [Salmon, 2015]. Those economic impacts are sometimes calculated using computable general equilibrium methods or via simulation. Actual events and sim¬ulation studies have indicated losses of tens of billions of dollars from various broader impacts of port disruptions (see, e.g., Cohen 2002, Park 2008, Rose and Wei 2013, Werling 2014). Cyber disruptions could have similar outcomes. (For more on the latter, see Rose 2017.)

The hull stress monitoring system (HSMS) is designed to detect problems with stability and balance. If an attacker could cause an imbalance of cargo without the crew being aware, through an attack on the HSMS, it is possible that a vessel could be put under stress and eventually break up and sink. Pen Test Partners have demonstrated how this might happen. Many HSMS are PCs connected to a ship's network. Taking control of such a PC, a hacker could arrange to have containers loaded in such a way as to create imbalance without the crew's knowing about it. The hacker could take control of the load planning software that places heavier containers to place heavier containers at the top or all on one side. (See MarEx, 2017.) While this is all feasible, there would be difficulty in predicting where the ship might break up or sink. Thus, it might not be an effective way to arrange to block a tight shipping channel, making the risk of such an attack less likely – unless the goal was to simply demonstrate the ability to destroy a vessel and achieve the resulting economic damage.

An adversary might be able to block the port entryway without attacking a particular vessel. All ports operate at full capacity. Due to amount of incoming vessel traffic, the only way to schedule arrivals at a modern port is by computer. An adversary could attack the port traffic management system or the AIS on many of the incoming vessels. A few $500 portable devices placed in a few areas around the port could jam the AIS of incoming ships. Ships would anchor in place. Even if the authorities identified the jamming signal, it could be repeated the next day. The port would be closed. The adversary might even follow up by physically attacking one of the ships at anchor. Not everyone agrees that the taking out of multiple AIS systems scenario would be a big problem. There are tertiary systems to replace AIS, e.g., radar. Moreover, especially in a port where the weather is usually good, even line of sight would allow vessels to operate and enter the port.

An adversary might also stop traffic by setting a terminal on fire, or setting a moored ship on fire or causing an explosion at a berthed ship. Could an adversary accomplish this by hacking into the fire control system? Could they accomplish this by initiating the fire by taking over a drone (hacking into it) and fitting it with a taser?

10. Attacks on the Cyber-physical Systems on a Vessel

Today's vessels are highly dependent on cyber-physical systems. Vessels are less tightly regulated than facilities. On a vessel, just the number of control systems make it difficult to defend against an attack. In cyber security awareness, navigation systems and control systems and their vulnerabilities are gaining increasing attention.

For modern ships there is dependence on a proliferation of sophisticated technology – that is subject to cyber attack. This includes:

- ECDIS (Electronic Chart Display and Information System)
- AIS (Automatic Identification System)
- Radar/ARPA (Radio Direction and Ranging) (Automatic Radar Plotting Aid)
- Compass (Gyro, Fluxgate, GPS and others)
- Steering (Computerized Automatic Steering System)
- VDR (Voyage Data Recorder –"Black Box")
- GMDSS (Global Maritime Distress and Safety System)
- Numerous other advanced units and systems

ECDIS flaws might allow an attacker to access and modify files and charts on board or on shore. See the discussion above about Naval Dome's ECDIS attack. The result of modified chart data would be unreliable and potentially dangerously misleading navigation information. That could lead to a mishap resulting in environmental and financial damage. In January 2014, the NCC Group tried to penetrate an ECDIS product from a major manufacturer. Security weaknesses such as ability to read, download, replace or delete any file stored on the machine hosting ECDIS were found. Once such unauthorized access is obtained, an attacker could interact with the shipboard network and everything to which it is connected, causing chaos. Such an attack could be made through something as basic as insertion of a USB key or through download from the Internet. (See CyberKeel, 2014.) An adversary doesn't need physical access to cause damage; they can get in via cellphones or satellite.

In October 2013, Balduzzi, Wihoit, and Pasta [2013] demonstrated how easy it is to penetrate a ship's AIS. Recently a Coast Guard Academy team used commercially available software to hack into AIS and turn it off. Per Cyberkeel [2014], such a hack could allow an attacker to impersonate marine authorities to trick the vessel crew into disabling their AIS transmitter. This would render the vessel invisible to anyone but the attackers themselves. AIS spoofing has apparently happened recently. There were suspected cases of mass-spoofing of AIS in the Black Sea in June 2017, with more than 20 ships affected. The GPS were giving false locations, some inland and some at airports. (See Blake, 2017).

Naval Dome has demonstrated how an attack could penetrate a vessel's machinery control system. It targeted the ballast system and was able to affect the valves and pumps (and stop them from working) while the display did not show any problems. Other systems such as generators, air conditioning, or fuel systems could

also be controlled in this way. (See AJOT, 2017.)

Attacks on the hull stress monitoring system are also of potential concern, especially if combined with attacks on the load balancing system while loading cargo. See the discussion in Section 9.

11. Monitoring a Vessel from a Distance; Ransom-ware

There is increasing interest in being able to monitor the behavior of shipboard systems from elsewhere, e.g., company Headquarters. Now, engine manufacturers monitor their engines for reliability, but also to make sure they are not being abused - which would void a warranty. They might be watching sensors that give advance notice that something isn't working right, for example detecting vibrations before a bearing goes bad. Manufacturers might also take control of onboard computers to install software upgrades. The bottom line is that many outsiders have access to vessel systems. A bad actor could hack into your system from outside, especially if your shipboard systems are networked. For Headquarters or an engine manufacturer to monitor a vessel's systems, the vessel might send telemetry from the ship. As soon as they create the network connection, there could be a problem. One could try to completely separate a sensor network. But of course it is easier to put everything on the same network – thus causing potential problems. This opens the vessel up to ransom-ware attacks, to pay ransom to get some shipboard system working again. Monitoring from elsewhere also leads to a different combined attack scenario: Start with a physical attack on the remote monitoring facility that allows the adversary to take over the facility and send malicious code to your vessel.

Could a "bad actor" inject ransom-ware and actually stop a vessel? Something like this actually happened to a commercial freight operator. They had their administrative system separate from their machine control system; the attack impacted the former. An economic effect (the ransom) was the desired outcome.[2] But what if the desired outcome was physical: stop the vessel in its tracks, making it easier to board it with a physical attack?

12. Cruise Ships: Passenger Systems and Vessel Systems

Today's cruise ship passengers want communication and entertainment systems akin to what they are used to ashore. Cruise ship operators are increasingly aware of the interplay between these systems and the critical IT systems on the vessel. There is a "tug of war" between reliability (which passengers demand of their systems) and vulnerability. A knowledgeable actor could take advantage of the vulnerabilities in the former to attack the latter. Today's cruise ship operators are fire-walling the servers for the passengers and those for the ship's operation, control, and hotel functions. There could be several hundred of the latter. Disrupting hotel services (water, power, AC) could make life unacceptable for passengers – a physical attack of sorts on passengers and a definite economic attack on the cruise ship industry. The industry thinks it understands how a "bad guy" might do this. Of most concern was that an attack like this could come through the passenger email system. But that has been largely dismissed because firewalls have been set up. There remains a vulnerability through authorized services that handle things remotely, e.g., desalinators and other equipment with lots of computer controls.

13. Hacking into a Cruise Ship's Navigation System

A 2012 demonstration by a UT Austin team showed how a potential adversary could remotely take control of a vessel by manipulating its GPS. The yacht "White Rose of Drax" was successfully spoofed while sailing on the Mediterranean. The team's counterfeit signals slowly overpowered the authentic GPS signals until they

[2] Maersk Lines is the world's largest container shipping company and moves 20% of the world's freight. In June 2017, a cyber attack on Maersk made everyone in the MTS sit up and take notice and gives a small idea of the impact of ransomware. The NotPetya virus was involved in ransomware attacks on Maersk and various other companies. Operations at Maersk terminals in four countries were affected, there were delays and disruptions for weeks, and the cost was estimated at $200M-$300M. (Osborne, 2018). A July 2018 cyber attack on Cosco Shipping Lines that caused failure in its networks in the United States, Canada, Panama, Argentina, Brazil, Peru, Chili, and Uruguay, was not as successful as the Maersk attack. Presumably Cosco had learned from what happened to Maersk and had isolated its internal networks, thus minimizing damage from the attack. [See Mongelluzzo, 2018.] This example raises the importance of information sharing in cyber defense. In sectors other than maritime, there is robust exchange of information about new types of attacks, new types of defenses, etc. The maritime sector has lagged behind. See Egan, et al, (2017) for a discussion of possible reasons, and possible approaches to change things. A key issue here is what kinds of incentives to give to companies to share information about cyber attacks with competitors and the government, when revealing such information could cause them significant financial loss. What economic and other incentives can we design to make such information sharing more likely?

ultimately obtained control of the ship's navigation system. "The ship actually turned and we could all feel it, but the chart display and the crew saw only a straight line." (Bhatti and Humphreys, 2014, Zaragoza, 2014). It is important to note that the GPS and navigation systems impacted were essentially the same as those used throughout commercial maritime operations and the Marine Transportation System, generally. "White Rose of Drax" was not a "soft target." However, a realistic analysis of the threat underscores the need for both proximity and persistent presence required for this attack to work. It can't be done remotely.

In February 2017, hackers reportedly took control of the navigation systems of a container vessel en route from Cyprus to Djibouti for 10 hours. "Suddenly the captain could not manoeuvre. … The IT system of the vessel was completely hacked." The attack was carried out by "pirates" who gained full control of the vessel's navigation system intending to steer it to an area where they could board and take over. (See Blake, 2017.) Certainly either of these examples demonstrates the possibility of hacking into the navigation system of a cruise ship.

Consider the scenario where a bad actor hacks into the navigation system on a cruise ship and causes it to change direction imperceptibly, eventually running it aground. This could be the precursor for a physical attack on the ship. Is this scenario feasible? Several of our SMEs described a failed GPS off of Cape Cod leading to the grounding of the Royal Majesty, heading from Bermuda to Boston in mid 1995. It resulted from failing to reconnect the navigation system to the GPS after maintenance. (See Blackett, 2004.) Jamming a ship's navigation system takes almost no sophistication. Spoofing it takes more.

One SME pointed out that if a bad actor spoofed a ship's GPS so that there are small changes in course, it is possible the crew would not notice. Especially at night if there were no visual cues. (There were such cues for the Royal Majesty.) The bad actor would need intimate knowledge of where the vessel is and reasonably close access. They would need to transmit false data. Each time they told it it was off course to the left (though not true), it would compensate by moving to the right. However, another SME pointed out that with modern ECDIS, the radar overlay would show your GPS is off. Another SME said that a physical attack is unlikely to be very successful since first responders would be there quickly.

Another SME pointed out that it would be a challenge for the bad actor to predict where the vessel would hit and therefore prepare for a physical attack. However, they could move the vessel to go into a shipping lane they want it to go into - perhaps making the physical attack easier. Another SME pointed out that an attacker could alter charts, hiding what shoal waters exist, leading to grounding of the vessel in a desired area. Just being able to run a cruise ship aground would have a major psychological impact. The result could be a major economic blow to the cruise ship industry. So even without human casualties, the would be a major effect of the cyber attack of grounding the ship.

14. Attacking Cruise Ship Passengers by Having them Move

Consider an attack on a cruise ship analogous to those in a port, where some hack on a ship's system leads to people gathering in large groups, creating vulnerability. (See Section 2.) Could a "bad guy" hack into the fire alarm system on a cruise ship, leading passengers to gather at mustering boat stations as a prelude to a physical attack there? This could happen through a planted explosive or attack by group arriving by boat or a suicide bomber on board cruise ship. Is this a plausible scenario? It seems feasible to hack into a fire alarm system on a ship, at least in some cases. But wouldn't it be easier to let an inside actor attack a large group of passengers already in one place – e.g., dining room? Or wouldn't it be easier for a group of attackers to come alongside by boat and just start shooting at miscellaneous passengers? One SME doubted this kind of combined attack would work because security on cruise ships is so good.

Note that to maximize impact, an attacker would not have to follow the fake fire alarm with a physical attack. They could simply fake a fire alarm, announce they were responsible and say they could do it again. This could create psychological impact and potential economic damage to the cruise industry. Doing this multiple times would create an even bigger impact.

An attacker could also avoid the challenge of hacking into the fire alarm system on the vessel by starting a real fire to activate the fire alarm. However, this would require physical presence, whereas the precipitating cyber attack to set off the fire alarm could be done from a distance.

Could a fire alarm arising from a hack or a physical act be just a distraction for a cyber attack – loading something on a server to use later? Conceivably, according to an SME, but not likely because servers would be locked down and because fire drills don't take very long. However, another SME felt that attackers could move crew where they want them and away from the location of a desired cyber attack, which could be to any of a number of control systems on the vessel.

15. Ferries

Many of the cyber attacks described for cruise ships are also relevant for ferries. The combined attacks

we have described might have another component, since passenger screening on ferries is less stringent than on cruise ships and vehicle screening is inconsistent. This allows for the possibility of a cyber attack followed by a physical attack through a passenger or a vehicle.

16. Cargo at Sea: Pirates

Pirates have been reported to have hacked into a cargo management system and identified where on a vessel valuable cargo is located. This enabled them to make a very fast and efficient raid on a vessel, going right to the container of interest. (See Hand, 2016.) Is this feasible?

One of our SMEs felt that it was feasible to hack into the cargo system and identify containers of interest and their location, but wondered how this would help the pirates since it is only the topmost containers they could access.

Another of our SMEs pointed out that the USCG had gotten quite good at getting into containers upon boarding a ship. Still another SME pointed out that the adversary could influence the loading of containers so that those of interest were placed to be accessible.

17. Autonomous Vessels

Our SMEs all felt that autonomous vessels were coming, soon. Such vessels will be programmed to decide where to go; will be tracked and monitored using diagnostics from Headquarters; will put out a problem message if they are unable to solve a problem, resulting in Headquarters sending instructions on where to go for repair. Do we trust the technological solutions so such vessels can go alone on the seas? Could a hacker take over the Headquarters computer and instruct the vessel to go to a place where it could be boarded by attackers?

The owners of an autonomous vessel are saving on crew costs but accepting some risk. One SME told us that shipboard systems and shipboard industrial control systems would be much harder to patch or have their software updated than many other systems. These systems might not be updated in real time, and hence become vulnerable to ransom-ware.

An attacker could jam or spoof the GPS or do a more sophisticated attack on the control system of the internal diagnostics of such a vessel. Could this affect heat or pressure or gas sensors, leading to an explosion, as in the example of Sec. 7 and in the discussion in Section 10 of an attack on the machinery control systems? This could cause economic damage, and possibly loss of life as well. If the goal of the attacker is psychological impact, they wouldn't do it in the middle of the ocean, where there is no media to film things. However, near a port, the vessel might not be entirely autonomous.

18. Closing Comments

Ultimately, the weak link in defense against combined cyber-physical attacks is still the human being. A successful attacker tries to influence behavior, leading to bad decisions. He or she would aim to introduce doubt, for example through false aids to navigation showing up on an electronic chart, spoofing a vessel track that may not correlate with radar, and creating a chain of things initiated by influencing the thinking of the bridge operator.

Our discussion has been limited to a single pair of events, one cyber, one physical. But there could be multiple events, or cascading events. More work is needed to develop scenarios for those. For example, an adversary could attack a cruise ship in a port and announce their intention to attack other cruise ships in other ports. What would the Coast Guard do? Would it close down those other ports, creating a vulnerability with large crowds waiting to embark? While it is not an MTS example, the following example of cascading events in an attack on the power grid, developed by the Cambridge Centre for Risk Studies and Lloyd's of London (Freedman, 2016), illustrates the point. Imagine hackers gaining access to the US electric power grid without security being alerted. They could do this through remote access systems, network monitoring systems, or personal devices of key personnel. Then the attackers lie low until some time in the future, when they would disable safety systems, allowing them to affect the circuit breakers on multiple generators and damaging some of their bearings. As a result, many generators burn and are partially destroyed, and operators shut down other generators to investigate. A large population across many states is left without power. This affects street lights, water systems, transit systems, phone systems, ATMs, etc. It takes weeks to restore power and the economic cost is enormous. To add to this, in the interim, the attacker gains access to multiple other systems that depend upon power to protect access, allowing for further cyber attacks on water systems, transit systems, banking systems, etc. One should be able to envisage similar cascading effects/attacks on the MTS.

This paper has been limited in scope. Examples of other areas to investigate include combined attacks on locks, drawbridges, barges, oil rigs, inter-modal landside connections, etc.

Fundamentally, there does not seem to be anything special one would do to prevent a cyber attack intended as a precursor to a physical attack that one wouldn't do to prevent any cyber attack.

References

AJOT, 2017. Cyber penetration tests underscore maritime industry's nightmare security scenario. American Journal of Transportation , December 21, 2017. https://www.ajot.com/news/cyber-penetration-tests-underscore-maritime-industrys-nightmare-security-sc, accessed Dec. 26, 2017.

Balduzzi, M., Wihoit, K., Pasta, A., 2013. Hey Captain, where's your ship? Attacking vessel tracking systems for fun and profit, 11th Annual HITB Security Conference in Asia, October 2013. http://conference.hitb.org/hitbsecconf2013kul/materials/D1T1%20-%20Marco%20Balduzzi,%20Kyle%20Wilhoit%20Alessandro%20Pasta%20-%20Attacking%20Vessel%20Tracking%20Systems%20for%20Fun%20and%20Profit.pdf, accessed Feb. 21, 2015.

Baraniuk, C., 2017. How hackers are targeting the shipping industry. BBC News. https://www.bbc.com/news/technology-40685821, August 18, 2017, accessed Aug. 6, 2018.

Bell, S., 2013. Cyber-attacks and underground activities in Port of Antwerp. Bull Guard, Oct. 21, 2013. http://www.bullguard. com/blog/2013/10/cyber-attacks-and-underground-activities-in-port-of-antwerp.html, accessed Feb. 21, 2015.

Bhatti, J., and Humphreys, T.E. 2014. Covert control of surface vessels via counterfeit surface GPS signals. Unpublished. https://pdfs.semanticscholar.org/6f20/450b32b71f2454e63292acb632d3619ee8ef.pdf, accessed Dec. 12, 2017.

Blackett, C., 2004. Analysis of the Royal Majesty grounding using SOL 3rd Bieleschweig Workshop on Systems Engineering, 12-2-2004. http://www.rvs.uni-bielefeld.de/Bieleschweig/third/Blackett-B3-2004.pdf, accessed Dec. 13, 2017.

Blake, T., 2017. Hackers took 'full control' of container ship's navigation systems for 10 hours. ASKET Ltd, Maritime Security News and Updates, Nov. 26, 2017. https://www.asket.co.uk/single-post/2017/11/26/Hackers-took-full-control-of-container-ships-navigation-systems-for-10-hours-AsketOperations-AsketBroker-ELouisv-IHS4SafetyAtSea-TanyaBlake-cybersecurity-piracy-shipping, accessed May 14, 2019.

Cockrell School of Engineering, 2012. Todd Humphreys' research team demonstrates first successful spoofing of UAV. The University of Texas at Austin Aerospace and Engineering and Engineering Mechanics News. June 12, 2012. http://www.ae.utexas.edu/news/504-todd-humphreys-research-team-demonstrates-first-successful-uav-spoofing, accessed Dec. 28, 2017.

Cohen, S. S. 2002. Economic Impacts of a West Coast Dock Shutdown. Unpublished report prepared for the Pacific Maritime Association, Berkeley Roundtable on the International Economy, University of California at Berkeley, Berkeley, CA: University of California at Berkeley.

CyberKeel, 2014. Maritime Cyber-Risks: Virtual Pirates at Large on the Cyber Seas. White Paper, CyberKeel, Copenhagen. October 15, 2014.

DiRenzo, J. III, Drumhiller, N., Roberts, F.S. (Eds.), 2017. Issues in Maritime Cyber Security. PSO-Westphalia Press.

DiRenzo, J. III, Goward, D.A., Roberts, F.S., 2015. The little-known challenge of maritime cyber security. Proceedings of the 6th International Conference on Information, Intelligence, Systems and Applications (IISA), IEEE, 2015, pp. 1-5. DOI: 10.1109/IISA.2015.7388071

Egan, D., Hering, D., Kantor, P., Nelson, C., Roberts, F., 2017. Information Sharing for Maritime Cyber Risk Management. In DiRenzo, J. III, Drumhiller, N., Roberts, F.S. (Eds.). Issues in Maritime Cyber Security. PSO-Westphalia Press, 2017, 271-302.

Freedman, A., 2016. Cyber grid attack: A cascading impact. Risk & Insurance, April 2016 issue. http://riskandinsurance.com/cyber-grid-attack-cascading-impact/, accessed Dec. 14, 2017.

Greenberg, A. 2013. Hackers reveal nasty new car attacks – with me behind the wheel. Forbes, Aug. 12, 2013. https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/#18a55198228c, accessed Dec. 11, 2017.

Hand, M., 2016. Cyber-attack allows pirates to target cargo to steal. Seatrade Maritime News, July 7, 2016. http://www.seatrade-maritime.com/news/americas/cyber-attack-allows-pirates-to-take-a-roman-holiday.html, accessed Dec. 13, 2017.
Mackenzie, J., 2013. Wrecked cruise ship Costa Concordia raised off Italian rocks. Reuters, Sept. 16, 2013. https://www.reuters.com/article/us-italy-ship/wrecked-cruise-ship-costa-concordia-raised-off-italian-rocks-idUSBRE98F02T20130917, accessed Dec. 13, 2017.
MarEx, 2017. Hackers could sink a bulk carrier. The Maritime Executive, Dec. 20, 2017. https://www.maritime-executive.com/article/hackers-could-sink-a-bulk-carrier#gs.ZogtZZo , accessed Aug. 6, 2018.
Mongelluzzo, B., 2018. Cosco's pre-cyber attack efforts protected network. JOC.com, July 30 2018. https://www.joc.com/maritime-news/container-lines/cosco/cosco%E2%80%99s-pre-cyber-attack-efforts-protected-network_20180730.html, accessed Aug. 6, 2018.

Mullin, S., 2014. Cyber resilience in the maritime and energy sectors. Templar Executives, May 1, 2014, http://www. templarexecs.com/cyberresilience/, accessed Feb. 21, 2015.

Osborne, C., 2018. NonPetya ransomware forced Maersk to reinstall 4000 servers, 45000 PCs. Zero Day, Jan. 26, 2018. https://www.zdnet.com/article/maersk-forced-to-reinstall-4000-servers-45000-pcs-due-to-notpetya-attack/, accessed Aug. 6, 2018.

Park, J-Y. 2008. The economic impacts of dirty bomb attacks on the Los Angeles and Long Beach ports: Applying the supply-driven NIE¬MO (National Interstate Economic Model)." Journal of Homeland Securi¬ty and Emergency Management 5 (1): Article 21.

Pasternack, A., 2013. To move drugs, traffickers are hacking shipping containers. Motherboard, Oct. 21, 2013.

https://motherboard.vice.com/en_us/article/bmjgk8/how-traffickers-hack-shipping-containers-to-move-drugs, accessed Dec. 13, 2017.

Rose, A. (2017). Economic Consequence Analysis of Maritime Cyber Threats. In DiRenzo, J. III, Drumhiller, N., Roberts, F.S. (Eds.). Issues in Maritime Cyber Security. PSO-Westphalia Press, 2017, 321-356.

Rose, A., Wei, D. (2013). Estimating the economic consequences of a port shutdown: The special role of resilience. Economic Systems Reseach 25 (2), 212-232.

Salmon, K. "West Coast Port Congestion Could Cost Retailers $36.9 Billion in the Next 24 Months," Business Wire, Feb. 7, 2015, http://www.businesswire.com/news/home/20150207005007/en/West-Coast-Port-Congestion-Cost-Retailers-36.9#.VPiNIsbA7c8, accessed March 5, 2015.

Segal, A. 2017. How China is preparing for Cyberwar. Christian Science Monitor, March 20, 2017. https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar, accessed Dec. 10, 2017.

The State Council Information Office of the People's Republic of China 2015. China's military strategy. China Daily, 5-26-15. http://www.chinadaily.com.cn/china/2015-05/26/content_20820628.htm. Accessed 12-10-17.

Tucci, A. 2017. Cyber risk management: Preparing for new operational risks. Port Technology Edition 2017, Summer 2017.

Wagstaff, J., 2014. All at sea: Global shipping fleet exposed to hacking threat. Reuters, April 23, 2014. http://www.reuters.com/article/2014/04/23/tech-cybersecurity-shipping-idUSL3N0N402020140423, accessed Feb. 21, 2015.

Werling, J. 2014. The National Impact of a West Coast Port Stoppage. Inforum Report Commissioned by the National Association of Manufacturers and the National Retail Federation, https://www.nam.org/Data-and-Reports/Reports/The-National-Impact-of-a-West-Coast-Port-Stoppage-(Full-Report).pdf, accessed May 14, 2019.

Zaragoza, S. 2014. Spoofing a superyacht at sea. Know, University of Texas at Austin, May 5, 2014.

Zetter, K., 2014. An unprecedented look at Stuxnet, the world's first digital weapon. Wired, Nov. 3, 2014. https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/ , accessed Dec. 13, 2017.

Zorz, Z., Zorz, M., Kucan, B., 2013. Digital ship pirates: Researchers crack vessel tracking system. Net Help Security, October 16, 2013, http://www.net-security.org/secworld.php?id=15781, accessed Feb. 21, 2015.

BIOGRAPHY

FRED ROBERTS is a Distinguished Professor of Mathematics at Rutgers University in New Jersey, USA, and Director of the CCICADA Center, a US Department of Homeland Security University Center of Excellence. For 16 years he directed DIMACS, a US National Science Foundation Science and Technology Center with academic and industrial partners and 350 affiliated scientists.

Roberts has served as co-chair of the New Jersey Universities Homeland Security Research Consortium, on the Department of Health and Human Services Secretary's epidemiology modeling group, the New Jersey Governor's Health Emergency Preparedness Advisory Council and the New Jersey Domestic Security Preparedness Task Force Planning Group. He has been Research Director of the University-US Coast Guard research initiative on Maritime Cyber Security.

Roberts has authored four books (some of which have been translated into Russian and Chinese), over 190 scientific articles, and edited 23 books, including his book Issues in Maritime Cyber Security published in 2017. His research interests include large venue security, resource allocation, container inspection, security metrics, behavioral responses to disasters, maritime cyber security, and homeland security aspects of global environmental change.

Professor Roberts has received the Commemorative Medal of the Union of Czech
Mathematicians and Physicists, the Distinguished Service Award of the Association of Computing Machinery Special Interest Group on Algorithms and Computation Theory, the National Science Foundation Science and Technology Centers Pioneer Award, and was awarded the title Docteur Honoris Causa by the University of Paris-Dauphine.

Appendix: List of Subject Matter Experts Consulted

CAPT Michael Dickey, USCG
Mark Dubina, Port of Tampa Bay
Casey Hehr, Port of Long Beach (USCG – ret)
CAPT David Moskoff, SUNY Maritime
VADM Rob Parker, USCG-ret
Randy Parsons, Port of Long Beach
Daniel Searforce, Pennsylvania Public Utilities Commission
Drew Schneider, Port of Long Beach
CAPT Andrew Tucci, USCG
CDR Nick Wong, USCG
Michael Young, TSA and Secret Service – ret

Acknowledgements: The authors thank Linda Ness for helpful discussions. They thank the U.S. Department of Homeland Security, Office of University Programs, for partial support under grant number 2009-ST-061-CCI002-08 to Rutgers University, and Fred Roberts thanks the U.S. National Science Foundation for partial support under grant number DMS-1737857 to Rutgers University. The authors thank the subject matter experts listed in the Appendix; much of this paper results from the ideas generously shared by these people.

NMIOTC Course "17000"
Train-The-Trainers Technical Instructors Course

From 14th to 25th January 2019, the Train-the-Trainers Technical Instructors Course was conducted at NMIOTC premises, in cooperation with the Hellenic Navy Training Centre ''PALASKAS''.
The objective of the course was to provide the basic technical skills, advanced teaching methods and presentation skills, required to teach technical subjects in an international training audience, while maintaining the high qualification level of the NMIOTC's instructors in the context of the ACT Quality Assurance Process.
In total 14 staff officers from Bahrain, Estonia, Malta, Poland, Romania and Greece, participated in the course.

NMIOTC Lessons Learned (LL) AND Best Practices (BP) "WORKSHOP"

NMIOTC organized and conducted the Maritime Interdiction Operations (MIO) Lessons Learned (LL) Lessons Identified (LI) and Best Practices (BP) Process Workshop in the eve of Operation Sea Guardian Focused Operations in-brief at its premises on Thursday the 7th of Feb 2019.
The aim of the workshop was to analyze VBSS and MIO operations which were executed recently form a Hellenic Coast Guard SOF team to a vessel involved in illicit trafficking as well as various MIO ops executed from Hellenic Navy assets and SOF/UDT teams in an effort to support NATO's LL and BP process.
The LL & BP Workshop was facilitated by the Quality Assurance Management (QAM) team of NMIOTC with the involvement of Allied Maritime Command (MARCOM), the Commander and staff from the Task Group of Operation Sea Guardian, and representatives from various Armed Forces, Law Enforcement authorities, US NSA and NMIOTC's international staff.
The outcomes of the Workshop, such as Lessons Identified, remedial actions etc, will enhance the internal QAM process of training deliverables in NMIOTC and through Joint Analysis &Lessons Learned Centre (JALLC) will support the Alliance's future operations.

NMIOTC Course "6000" – WMD in MIO

From 11th to 15th of February 2019, the NMIOTC Course "6000", Weapons of Mass Destruction in Maritime Interdiction Operations (WMD in MIO), was conducted at NMIOTC premises.
In total nineteen (19) trainees coming from six (6) countries (Denmark, Egypt, Georgia, Greece, Pakistan and United Arab Emirates) attended the course. Three (3) Subject Matter Experts from Czech Republic and Greece were invited to support the course as augmenters, in addition to the Centre's Instructors and Lecturers

Developing Course 20000
"Protection of Critical Maritime Infrastructure (CMI)"

In order to obtain proper and accurate conclusions regarding the developing Course 20000 "Protection of Critical Maritime Infrastructure (CMI)", NMIOTC conducted trials using as training platform of the Ocean Rig Management Inc. (OCR) drilling ships from 26 Feb - 02 Mar 18, by deploying a Mobile Education and Training Team (METT) in Pireus, Greece,
"Train the Trainers" training has been organized among Norway Special Operations Command (NORSOCOM) and NMIOTC from 15th to 23rd Jan 19, in NMIOTC premises, for drawing proper and accurate conclusions regarding the development of the Course and enhance NMIOTC sea trainers with the topics which are directly related with the development of Course 20000.

Libyan Navy & CG VBSS Operations Informative Course (28 Feb – 15 Mar 19)

From 28th February to 15th March 2019, NMIOTC provided the VBSS Operations Informative Course in favour of EUNAVFOR MED Operation SOPHIA. The duration of this Course was twelve (12) working days and the target audience included military personnel from Libyan(LBY) Navy and Coast Guard.

The Course aimed to enhance the Capacity building of Libyan Navy and Coast Guard by providing the theoretical framework on how to plan a VBSS Operation while taking into consideration legal and gender aspects of respective operations. Upon completion the trainees are able to participate in the planning of MIO and execute proper tasks as a member of a Visit, Board, Search and Seizure Team (VBSS-T).

In total 24 trainees from Libyan Navy and Coast Guard participated and successfully graduated from the course. Instructors/ augmenters from UNCHR, RAVA Foundation, NMIOTC,
Chania's Military Court and ENFM were involved to the training process.

EDA – FRONTEX Joint Pilot Training on the Coordination of Law Enforcement and Navy Actions in Maritime Border Security

From 25th March to 05th Apr 2019, European Defence Agency (EDA), FRONTEX and NMIOTC jointly organized a tailored training for military and law enforcement personnel, This focused on Migration, Search and Rescue and Crime Scene investigation as well as Legal Issuesin Maritime Operations.

The objective was to enable participating personnel to improve their knowledge and skills in the above mentioned subjects, to enhance their cooperation and coordination by implementing standard procedures, based on best practices and recognized international standards.

In total 24 trainees from EU countries (Bulgaria, Denmark, Germany, Greece, Italy, Lithuania, Malta, Poland, Romania and Spain attended the course. Twenty one (21) Subject Matter Experts from Italy, Lithuania, Spain, Poland, Germany and Greece were invited to support the course as augmenters/instructors.

MULTINATIONAL EXERCISE «NOBLE DINA 2019»

During the in-port phase of the exercise "NOBLE DINA 2019", from 4th to 7th April, NMIOTC delivered theoretical and practical training on Maritime Interdiction Operations (MIO), to the trainees from participating units of Greece and Israel.

3rd CONFERENCE ON CYBER SECURITY IN MARITIME DOMAIN

From 10th to 11th April 2019, the 3rd Conference on "Cyber Security in Maritime Domain" was held at NMIOTC, attended by 147 participants from 24 Allied and Partner nations, International Organizations, the international academic community, representatives from the marine and communication industry and several strategic think tanks.

The aim was to build synergies between public and private sector in general, individual researchers, navy staffs, members of associations, academia, shipping companies, standardization bodies, international organizations and governmental agencies regarding Cyber Security in the maritime domain and Cyber Defence operations. NMIOTC envisaged tackling Cyber Security issues in the maritime domain in a holistic, comprehensive and effective way.

NMIOTC's participation to the CJOS COE Maritime Security Regimes Roundtable 2019

From 30th April to 1st May 2019, NMIOTC participated in the CJOS COE Maritime Security Regimes Roundtable 2019 in Norfolk VA, USA. The center contributed to the event by providing one of the panels, focused on the Cyber Security in Maritime Domain with the theme "Cyber Defense as a form of Hybrid Threat in MSO". NMIOTC's panel comprised of NMIOTC Commandant , Commodore Stelios Kostalas GRC (N) as a chairman, and Lt Cdr Dimitrios Megas GRC (N) - NMIOTC Staff, Dr Alberto Domingo ACT, Mr Christos Vidakis Deloitte, Professor Maria Papadaki- Plymouth University as speakers.

NMIOTC's panel objective was to highlight the cyber threat rising in the Maritime Domain and discuss how cyber capabilities are a critical enabler of success across all missions, ensuring that these capabilities are leveraged by commanders and decision-makers from tactical, operational and strategic level. Finally, NMIOTC had the opportunity to present to all Maritime community participants the outcomes of the 3rd NMIOTC Conference on Cyber Security in Maritime Domain which took place at its premises from 10th to 11th of April 2019.

Course «21000»
(Medical Combat Care In Maritime Operations)

Resident Course 21000 "Medical Combat Care in Maritime Operations" was conducted at NMIOTC's premises from the 13th to the 24th of May 2019.

The goal of this course was to transfer knowledge and enhance trainees' skills so as to provide combat medical care from the point of injury in the mission/theatre until the final transfer to the closest Medical Treatment Facility.

Twenty nine (29) participants from six (6) Countries attended the course (Greece, Ireland, Italy, Malta, Netherlands, Qatar and USA). Training was delivered from Subject Matter Experts (SME's) certified as National Association of Emergency Medical Technicians (NAEMT) instructors and other augmenters specialized in Stress Management, telemedicine and HAZMAT. In addition, an assigned Medical Director was closely monitoring all medical interventions performed throughout the Course in absolute coherence with NAEMT's policies, and regulations.

In April 2019 the NMIOTC was successfully reevaluated by ACT' Quality Assurance Team of Experts and be re-awarded with Unconditional Accreditation for another six years.

NORTH ATLANTIC TREATY ORGANIZATION
ORGANISATION DU TRAITÉ DE L'ATLANTIQUE NORD
HEADQUARTERS, SUPREME ALLIED COMMANDER TRANSFORMATION
7857 BLANDY ROAD, SUITE 100
NORFOLK, VIRGINIA, 23551-2490

ENCLOSURE TO 1
ACT/JFD/HCEIT/TT+1429/Ser:NU0171
DATED: 6 JUN 19

Quality Assurance Accreditation Certificate

The core processes and procedures of the NATO Maritime Interdiction Operational Training Centre (NMIOTC) were reviewed and identified as being aligned with NA TO Quality Standards. Therefore the Institution qualifies for

UNCONDITIONAL ACCREDITATION

Certificate No: ACT/JFD/HCEIT/TT+1429/Ser:NU

Effective: 31 May 2019 Expires: 31 May 2025

NMIOTC was found to have:

a. sound internal procedures for the assurance of quality;

b. procedures that are applied effectively at each level to ensure the quality of education and training;

c. effective and regular processes of reviewing the curriculum and implementing required changes and enhancements;

d. accurate, complete and reliable information about its curriculum.

FOR THE SUPREME ALLIED COMMANDER TRANSFORMATION:

Stefano Vito Salamida
Major General, ITA AF
Deputy Chief of Staff Joint Force Development

Course «19000»
(Cyber Security Aspects In Maritime Operations)

Resident Course 19000 “Cyber Security Aspects In Maritime Operations” was conducted from 20th to 24th of May 2019 at NMIOTC premises. Seventeen trainees (17) from seven (7) nations attended the Course (Belgium, Bulgaria, Croatia, Denmark, France, Greece and USA).

Course objective was to provide a comprehensive knowledge to facilitate the understanding of the maritime cyber aspects, designed for operational planners and staff officers from tactical and operational level, without sufficient cyber operational background.

10th NMIOTC ANNUAL CONFERENCE 2019

The 10th NMIOTC Annual Conference took place from 4th to 6th of June 2019 at NMIOTC premises. Titled ”Countering Hybrid Threats: “An Emerging Maritime Security Challenge”, it was attended by 114 participants from 25 Allied and Partner nations, International Organizations, the international academic community, representatives from the shipping and IT industry and several strategic think tanks.

The aim of the Conference was to discuss issues related to maritime security operations and forward proposals and solutions to current and future security challenges and emerging from the Maritime domain.

NATO Partnerships 360 Symposium

NATO Partnerships 360 Symposium was held in the NMIOTC premises from 11th to 13th June 2019. As a contemporary and innovative venture co-hosted by NATO's Allied Command Transformation and NATO International Staff Political Affairs and Security Policy Division, it engaged the partnership network and community in a "one NATO" spirit of political-military cooperation, bringing together civilian and military representatives from 45 Allied and all partner nations to stimulate free exchange of ideas. Projecting Stability, awareness-sharing and understanding of new technologies in the face of hybrid challenges, were some of the topics to be addressed in this "symposium" of friends.

NATO Submarine Staff Officers Conference (SSOC)

The NATO Submarine Staff Officers Conference (SSOC) was organized by Hellenic Submarine Command (COMHELSUB) and hosted at NMIOTC premises from 18th to 21st of June 2019. SSOC is an annual working-level forum coordinated by COMSUBNATO, in order to improve Alliance's submarine interoperability through achievement of standardization and promotion of mutual understanding.

At the conference participated thirty one (31) attendees from (12) twelve nations.

DRAFTING, PRODUCTION AND MAINTENANCE OF NATO STANDARDS COURSE

From 24th to 28th of June 2018, the 4th Iteration of Drafting, Production and Maintenance of NATO Standards Course was conducted at NMIOTC premises, with the cooperation of Warsaw Military University of Technology (MUT), HNDGS and NATO Standarddization Office (NSO). The course provided comprehensive knowledge to facilitate understanding of the procedures for development, production and maintenance of NATO standardization documents.
In total, six (6) lecturers and twenty nine (29) trainees coming from eleven (11) countries attended the course.

SUBMARINE ESCAPE AND RESCUE WG 2019 (SMERWG 19)

The Submarine Escape and Rescue Working Group 2019 (SMERWG 19) organized by Hellenic Navy and the Hellenic Submarine Command (COMHELSUB), was hosted at NMIOTC premises from Monday 24th to Friday 28th June 2019.
The NATO SMERWG encourages the development and implementation of Military Standardisation processes within the global Submarine Escape, Rescue and Abandonment community.
One hundred and forty two (142) participants from twenty six (26) Countries attended the Working Group

Imbros Gorge Crossing

In April, NMIOTC personnel and their families crossed the Gorge of Imbros. It is the second most popular gorge for walkers in Crete after the gorge of Samaria and is located in the province of Sfakia.

7k Fun Run

In June NMIOTC organized the “7 km Memory Run” with the addition of the 3km power walking, in the memory of the late Lieutenant Colonel Pantelis Karastergiou GRC (A) MD.
In total, 43 participants from NMIOTC, Souda Naval Base, 115th C. Wing and the Naval Hospital attended the event.

Training Platfroms End of Season Cleaning Activities

Twice a year all NMIOTC personnel participate in the revival and cleaning of the centre's training platforms ARIS and ALKYON, in order to prepare them for training activities, followed by BBQ happy hour..

Visit of the Ambassador of the Republic of Poland in Greece,
H.E. Anna Barbarzak, February 7, 2019

Visit of the Staff Director of the
US Senate Foreign Relations Committe, Chris Socha,
February 21, 2019

Visit of Force Commander EUNAVFOR Operation Atalanta, Rear Admiral Ricardo A. Hernández López, February 28, 2019

Visit of the Rectoral Authorities of Technical University of Crete, February 28, 2019

Celebration of Czech Republic, Hungary and Republic of Poland's 20 Years since their Joining in NATO, March 14, 2019

Visit of HEL SOCOM, Major General Georgios Tsitsikostas, May 8, 2019

NMIOTC COM's visit to "Nikola Vaptsarov" Naval Academy in Varna, Bulgaria, May 20, 2019

46th NATO VLF MSK User Group Conference, May 21-22, 2019

Train the Trainers Course on Critical Maritime Infrastructure Protection, January 14-25, 2019

NMIOTC Course 3000 - Boarding Team Practical Issues, February 25 March 8, 2019

Training of Belgian SOF Team,
March 18-29, 2019

EDA - FRONTEX Training,
March 25 - April 5, 2019

Training of FS Marne,
April 2, 2019

Training of German Forces for Boarding Deployment Team,
April 8-19, 2019

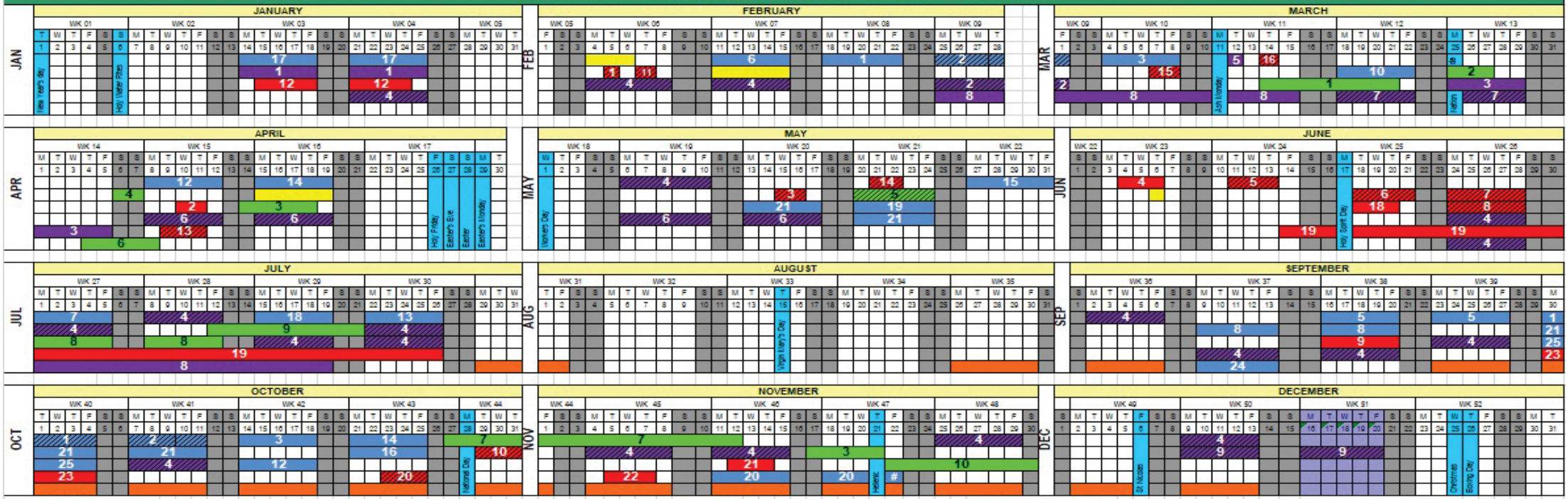
NMIOTC Course 4000,
"Maritime-Improvised Explosive Device Disposal" (M-IEDD),
April 15 -19, 2019

NMIOTC Biometrics Exercise,
May 20-24, 2019

NMIOTC Course 15000
Migrant Handling Team Issues in Maritime Interdiction Operations in Support of International Efforts to Manage the Migrant and Refuge Crisis at Sea, May 27-31, 2019

Drafting, Production and Maintenance of NATO Standards Course, (New NMIOTC, Course 25000)
June 24-28, 2019

NMIOTC Program of Work 2019 (NPOW 2019)



COURSES (ETOC ID.)

1. Course 1000 - Command Team MIO Issues (MOP-MO-51201)
2. Course 2000 - Boarding Team Theoritical Issues (MOP-MO-51203)
3. Course 3000 - Boarding Team Practical Issues (MOP-MO-41205)
4. Course 4000 - MIO Final Tactical Exercise (MOP-MO-41207)
5. Course 5000 - Maritime Operational Terminology Course (MOP-MO-11208)
6. Course 6000 - Weapons of Mass Destruction in MIO (MOP-MO-31209)
7. Course 7000 - MIO in support of Counter Piracy Ops (MOP-MO-41210)
8. Course 8000 - C-IED Considerations in Maritime Force Protection (IED-ED-31679)
9. Course 9000 - Legal Issues in MIO (LGL-LE-31613)
10. Course 10000 - MIO in Support of Countering Illicit Trafficking at Sea (MOP-MO-32012)
11. Course 11000 - AVPD Course (MOP-MO-32011)
12. Course 12000 - C-IED in Maritime Interdiction Operations (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-3215)
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 (Pilot)
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-22373)
19. Course 19000 - Cyber Security Aspects in Maritime Operations (COP-CD-22104)
20. Course 20000 - Protection of Critical Maritime Infrastructure [C(M)I] (Pilot)
21. Course 21000 - Medical Combat Care in Maritime Operations (MED-MS-34411)
23. Course 23000 - WIT Supplement in Maritime Operations (IED-ED-35437) (Pilot)
24. Radiological Threat in Maritime Ops (Pilot)
25. Course 25000 - Drafting, Production and Maintenance of NATO Standards Course

ACTIVITIES

1. NAB (NMIOTC)
2. Cyber Security Conference
3. NCB (HNGS)
4. NMIOTC Annual Conference
5. NATO Partnerships 360 Symposium
6. Submarine Staff Officers Conference
7. ATP-71 WS
8. Submarine Escape and Rescue WG
9. Countering Hybrid Threats Seminar
10. ACO Security Conference 19
11. OSG FOCOPS In Brief & LLWS
12. CMI TTT Training
13. QA on Site Visit
14. VLF MSK Users Group
15. Bio TIWS
16. Czech Rep-Hungary-Poland 20th Year Ceremony
17. CDX-N (Apr 19)
18. Human Security WS
19. Libyans Communication Course
20. Demonstration of NATO NSCI-294
21. Environmental Protection Course
22. Littoral OpTech EASTMED WS
23. 5th International Senior Course of the Hellenic National Defense College

EXERCISES / METTs

1. ARIADNE 19
2. METT in PHOENIX EXPRESS 19
3. METT in KUWAIT - ICI Regional Centre
4. METT in SEA SHIELD 19
5. LIVEX for the Project Biometrics DAT POW
6. METT in NOBLE DINA 19
7. METT in IMX 19
8. METT in SEA BREEZE 19
9. METT in BREEZE 19
10. NIRIIS 19
11. ADRION 19

TAILORED TRAININGS

1. GHA BT
2. AUT BT
3. EDA FRONTEX Training
4. GRC SOF
5. AZE BT
6. DEU BT
7. BEL SF
8. LBY VBSS Training
9. POL BT

► **Updated 24 September 2019**

Training Courses | Tailored Trainings | NATO Events | Exercise / MTTs | Conference - Meeting | Unit Training | Official Holidays | Available Period for Training | Evaluation of Courses / Maintenance

NMIOTC
Souda Bay 732 00 Chania
Crete, GREECE

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

Webpage: www.nmiotc.nato.int

Hellenic Army Printing Office