Issue 12
1st Issue 2016
ISSN: 2242-439X

NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE

nmiotc

Maritime Interdiction Operations Journal

NATO
Maritime Interdiction Operational
Training Centre

1st Conference on Cyber Security

CYBER SECURITY IN THE MARITIME DOMAIN

04 - 05 OCTOBER 2016

CONTENTS

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Commodore G. Tsogkas GRC (N)
Commandant NMIOTC

Executive Director
Captain C. Campana ITA (N)
Director of Training Support

Editor
Lt Commander N. Tiantoukas GRC (N)
Head of Transformation

Layout Production
CPO E. Miskou GRC (N)
Journal Assistant Editor

NMIOTC
Commandants Editorial 12th edition

During the last two years from Whales to Warsaw Summit, concrete decisions were reached for the adaptation of the Alliance. The maritime domain holds a significant part of this adaptation effort. The way though from Whales to Warsaw is paved by new security challenges. Conditions are set in order to cope with potential emerging challenges to our collective security proactively. The environment has fundamentally changed as regards Alliance's Eastern and Southern flanks security. At the same time, USA is shifting its interest to the Pacific, and NATO members are requested to take over increased responsibilities in and around Europe. This burden, regardless how heavy it could be, it creates opportunities for collaboration especially in the maritime domain. NATO's Alliance Maritime Strategy, along with Partners' involvement and broad collaboration in the areas of training, information exchange and others such as energy security and illicit trafficking, would empower all stakeholders to be prepared to face these challenges in a timely manner and at further out distances.

NATO's adaptation calls for enhanced opportunities for training. It is anticipated that the Warsaw Summit outcomes would call for enhanced training opportunities with security provider partners. This is exactly why NMIOTC is more relevant than ever. In its capacity as a NETF, awarded by ACT with a Quality Assurance Accreditation, focused on the maritime domain, offers education and training opportunities to Allies and Partners within their framework of cooperation with NATO. Its operational capacity has been recognized by those who have been following its evolution since its establishment. NMIOTC stands ready to better support NATO's partners following relevant decisions, in addition to existing programs and synergies.

Emerging security challenges, such as Critical Infrastructure Protection, Countering Proliferation of Weapons of Mass destruction, C-IED in the Maritime domain, illicit activities and organized crime at sea, interdiction at range and cyber defense in the maritime domain, has been timely identified and are tackled in a comprehensive manner by both NMIOTC's training and transformation departments. Having said that and referring to this journal, I

wish to draw your attention to the fact that it presents articles focused on current and future challenges to maritime security. In particular;

In the lead article, Dr. Marina Skordeli on "Energy Security in the Maritime Environment Challenges and Opportunities emerging in the Eastern Mediterranean" articulates the particular importance that energy security in the maritime environment of the Eastern Mediterranean region has for the Euro-Atlantic community. On the same spot Stephen L. Caldwell within his article'' Trends in Global Energy Economics, and Their Implications for Maritime Energy Infrastructure Security and Related Interdiction Training" analyzes trends in energy economics and their impact on the security of maritime energy infrastructure. David Incertis within his article "Risks and Interdependencies in the LNG Supply Chain" refers to the maritime part of the LNG (Liquefied Natural Gas) supply chain, identifying its main links, their interdependencies and related risks which could hamper the normal flow of this very energy source. Dr George Gougoulidis within his article "Energy-saving Measures for Naval Operations", examines the feasibility and application of various operational and technical measures aiming out energy saving for maritime vessels.

The remaining part of the Journal deals with the maritime sector's vulnerability to cyber-attacks. Mr Robert Hayes article "Understanding &Mitigating Cyber Threats in the Maritime Domain'' describes how organizations can develop an effective strategic approach to cyber-security, and discuss how examples of global best practice from other industry sectors can help the maritime sector. Finally Lt Cdr Nikolaos Tiantioukas GRC (N) and Lt Cdr Dimitrios Megas GRC (N) at their article present the content and the mentality of our Centre in its efforts to provide effective and efficient training to counter cyber threat in the maritime environment through cyber security awareness. Last but not least Lt Cdr Ioannis Argiriou GRC (CG) presents NMIOTC efforts regarding countering Illicit trafficking at sea.

Finally, taking this opportunity, I would like to announce with great pleasure, the 7th Annual NMIOTC Conference which will be held at our premises (Souda Bay – Crete) from 7th to 9th June 2016, with topic "Challenges to Maritime Security Derived from Transnational Organized Crime at Sea" and the 1st Conference on Cyber Security in the maritime domain, which will also take place at our premises, from 4th to 5th October 2016.

Georgios Tsogkas
Commodore GRC (N)
Commadant NMIOTC

Energy Security in the Maritime Environment Challenges and Opportunities emerging in the Eastern Mediterranean

by Dr Marina Skordeli
Director of the Jean Monnet European Centre of Excellence, National and Kapodistrian University of Athens, Greece, jmcenter-athens@pspa.uoa.gr

Abstract

In recent years, technological advances have drawn attention on the extraction of energy from the sea, while the emergence of enhanced risks in the maritime environment is increasingly raising the issue of securing the extraction as well as the transfer of energy via maritime routes. Within this context, the Euro-Atlantic community should pay special attention on the Eastern Mediterranean, due to the immense geopolitical importance of the region and the particular challenges it

is facing. A traditionally volatile environment in the Eastern Mediterranean, as was defined in the past by both conventional and asymmetric threats, has now been further aggravated by new developments. The maritime dimension of the Eastern Mediterranean, in particular, is its basic feature, which involves special risks that need to be better analyzed and addressed. Nevertheless, a collective approach toward risks can also bring new opportunities to the fore.

Keywords

Eastern Mediterranean; energy; maritime security; NATO; European Union.

1. Introduction

This paper will explore the particular importance that energy security in the maritime environment of the Eastern Mediterranean region has for the Euro-Atlantic community. It will present shortly the respective NATO and EU policies on maritime and energy security. Subsequently, it will analyze the geopolitical importance of the Eastern Mediterranean and it will examine the risks and challenges emanating from this region in the maritime environment, as well as how they could threaten vital Euro-Atlantic interests related to energy security. Finally, it will explore the opportunities arising for a collective approach toward these challenges with a view to safeguarding energy supply and security.

2. The Euro-Atlantic Approach toward Maritime and Energy Security

In recent years, a collective approach towards risks at sea is becoming more systematized both by NATO and the EU.

The identification of the numerous EU interests and policies related to the sea, as codified in its Integrated Maritime Policy (Commission of the European Communities, 2007), pointed to the need to explore the military aspect of protecting these interests. The collective surveillance and management of maritime areas was set as a first step for the EU (ibid; European Council 2008). The European Parliament's study The Maritime Dimension of CSDP (European Parliament, 2013) raised the need to strengthen the maritime dimension of the Common Security and Defence Policy (CSDP) and develop more synergies between CSDP and the Integrated Maritime Policy. Once more, this development marked a growing awareness of the interconnection between maritime security and increasing global economic interests. All these culminated in the recent Maritime Security Strategy of the EU, adopted in June 2014 (European Commission 2014). NATO, for its part, adopted the Alliance Maritime Strategy (NATO 2011), which identifies four roles for NATO's maritime forces: deterrence and collective defence, crisis management, cooperative security and aritime security.

Maritime security and energy security are closely interrelated in the sense that a safe maritime environment and safe lanes of communication ensure the security of energy extraction from the sea and shipments via the sea. Energy security in the maritime environment includes the protection of the vessels themselves (e.g. tankers), of ports, of energy related infrastructure near ports (e.g. pipelines, oil refineries, oil storage depots), of off-shore oil and gas rigs and of Energy related assets are particularly vulnerable, especially when they extend beyond borders and attacks on them by hostile states, terrorists or hacktivists can have repercussions across regions. Political instability or conflict, in areas where these assets are being developed, is a main source of concern.

As regards Europe's energy security policies in particular, the EU Maritime Security Strategy stresses that energy security largely depends on maritime transport and infrastructures. According to the document, the strategic maritime security interests of the EU and its Member States include the preservation of the freedom of navigation, the protection of the global EU supply chain and of maritime trade, the right of innocent and transit passage of ships and the security of their crew and passengers. The protection of the EU's economic interests, in particular, include the safeguarding of maritime energy resources, the sustainable exploitation of natural and marine resources in the different maritime zones and the high seas, the delimitation of maritime zones, which presents a potential for growth and jobs, the protection of off-shore installations (e.g. gas or oil platforms), of port infrastructures (e.g. LNG facilities), of energy supply by the sea and of underwater pipelines. Maritime security threats to these interests, as identified by the Strategy, include threats or use of force against Member States' rights and jurisdiction over their maritime zones, threats to the security of European citizens and to economic interests at sea.

As regards NATO's role in energy security, the 2010 Strategic Concept (NATO 2010) calls for a capacity to

contribute to energy security, including by the protection of critical energy infrastructure and transit areas and lines, cooperation with partners, and consultations among Allies on the basis of strategic assessments and contingency planning. NATO seeks to increase its competence in supporting the protection of critical energy infrastructure, mainly through training and exercises. Protecting energy infrastructure is considered primarily a national responsibility, hence NATO's contribution focuses on areas where it can add value, notably the exchange of best practices with partner countries and with other international institutions and the private sector. With its maritime presence, through Operations Active Endeavour and Ocean Shield, NATO is also making an indirect contribution to energy security.

3. Geopolitical Importance of the Eastern Mediterranean

The Eastern Mediterranean is an area of major geopolitical and geostrategic importance. In economic terms, the location of the Eastern Mediterranean makes it a crucial transit point for trade in general and for vital energy resources directed to Europe and the United States in particular. This transit aspect of the Eastern Mediterranean has a strong maritime dimension. In political and security terms, for the past decades, the Eastern Mediterranean has been characterized by a complex security context made up of all sorts of conventional risks as well as what we call asymmetric threats. On top of those, in the past few years, we have been witnessing the emergence of a couple of new developments that could ultimately lead to a rebalancing of powers in the region and threaten its stability even further: the Arab Spring and the recent offshore energy findings. As a result, the risk factor at sea has been augmented in this region, thus jeopardizing the transit use of the wider area.

More specifically, the economic and energy security importance of the Eastern Mediterranean is strongly connected with its value as a key transit route. The Eastern Mediterranean, together with the Red Sea, plays a crucial role for international and, especially, European shipping by facilitating easy access between Western markets, on the one hand, and those of the Far East, the Middle East and the Black Sea, on the other. Consequently, the Mediterranean is one of the most used maritime corridors globally, as a significant part of the world shipping activity flows through it.

What enhances the region's importance dramatically is that a remarkable percentage of the energy resources traded internationally, almost 1/3, flows through the Mediterranean, whether via ships or through pipelines. Energy resources coming from the Persian Gulf and Russia pass mainly through this region. Oil is being transferred from the Persian Gulf primarily to Europe, but also to the US, through the Suez Canal. Russia is attempting to transfer its energy resources through southern corridors, in order to avoid what it perceives as hostile neighbors, such as Ukraine. The flow of natural gas and oil from the Caucasus and Central Asia via this region is also expected to increase. The number of pipelines already existing in the Eastern Mediterranean, but also those expected to be constructed there is adding to its geopolitical importance. Especially in currently crises-ridden areas, pending on developments, such pipelines could end up at Turkish, Syrian or Israeli shores, in the future. For example, with the normalization of the situation in Iraq, much of the oil there will most likely be transported to the Eastern Mediterranean through pipelines ending in its shores. Another parameter adding to the importance of this region is its own oil and gas reserves. The EU already covers a great part of its energy demand from sources in the Middle East and North Africa and European states seek to rely more on the Mediterranean states, in order to avoid dependence on Russia. The recent offshore energy findings in the Eastern Mediterranean could add significantly to its importance. As a consequence, the EU and NATO are now increasingly exploring the potential future role of the Mediterranean for transatlantic energy security. Recently, the Italian Presidency of the EU and the Commission announced the promotion of a Mediterranean gas hub, taking into consideration that the region is a strategic gas supplier to the EU and to its Mediterranean neighbours, it has important gas reserves and it is located in the midst of the world's busiest waterways for global shipping.

The EU has also expanded its renewable energy plans towards the south. Producing electricity from renewable sources in countries of the Southern Mediterranean is indeed a viable option. Submarine connections for electric power transmission have been proposed and such a grid could transmit to Europe significant shares of electricity produced from renewable sources in the future.

While the region's importance for

Euro-Atlantic energy security is being increasingly enhanced, in political and security terms, the Eastern Mediterranean has long been known for a list of conventional and asymmetric threats that could potentially affect vital interests of the EU and the US, in addition to their energy security. The gravity of these threats made many scholars, as well as numerous EU and NATO policy documents, characterise the Mediterranean as the new security front for the West after the end of the Cold War. Conventional threats in the Eastern Mediterranean take the form of a significant number of rivalries, regional crises and high intensity conflicts (e.g. the Arab-Israeli wars), as well as what until recently was characterised as rogue states (Syria, Libya) and dangerous non-state actors (e.g. Hezbollah). Stability in this region has also been threatened by asymmetric threats, such as terrorism and the use of Weapons of Mass Destruction.

Today, the security environment in the Eastern Mediterranean is being further aggravated. Political transformations in Egypt and Libya, the on-going turmoil in Syria and frozen relations between Turkey and Israel are reshaping longstanding balances and correlations, causing uncertainty and instability. With the emergence of the so-called Islamic State (ISIS), terrorism emanating from this region takes a new form, the dimensions of which cannot be assessed in full, yet. The possibility of the loss of state control over coastal areas and of the creation of lawless maritime zones, as a result of state collapse in the Mediterranean, could have an immediate impact on maritime security. In case that non-state actors are able to take hold of these coastal and maritime areas, severe risks to maritime traffic and energy flows could be posed. Hence, Europe and the US demonstrate a renewed attention toward this region, since such issues can threaten the security of their citizens and their vital interests.

We can conclude that stability in the Eastern Mediterranean is of particular importance for the Euro-Atlantic and global economic interests in general, since it allows for the flow of energy resources from areas in the periphery of Europe, such as Russia, the Middle East, Caucasus and Central Asia, but also from the region itself and, therefore, it allows for stability of the world economy. Thus, it must be ensured, in order to safeguard uninhibited and cost-effective shipping and the smooth operation of energy infrastructure.

4. Challenges to Energy Security in the Maritime Environment of the Eastern Mediterranean

The maritime dimension of the Mediterranean is its special feature that involves special risks. These risks could be associated both with conventional as well as with asymmetric security concerns.

Starting with asymmetric threats, preventing the entry of terrorists into the territorial waters of Western states, as well as terrorist attacks at sea and from the sea, is a major European and American concern. This is not a new threat. To date, there have been incidents of terrorist attacks on American or European warships, tankers or passenger ships. Such incidents demonstrate that maritime terrorism is a fact and that it is one of the most serious security threats. These have included attempts to damage tankers or disrupt loading operations in or near overseas ports, such as the attack of a small ship with explosives on the French tanker Limburg off the coast of Yemen, in October 2002.

As regards the Mediterranean, the disclosure of a number of attempted terrorist attacks on ships leads to the conclusion that such scenarios are becoming increasingly possible for the Eastern Mediterranean. Organizations, such as Hezbollah, the Jemaah Islamiyah, the Popular Front for the Liberation of Palestine, have long tried to develop capabilities, in order to undertake similar action.

Cargo ships crossing the Mediterranean could either be placed under the control of terrorists or suffer from attacks on their journey. Energy infrastructure at sea, such as oil and gas rigs, could be damaged or hijacked. Terrorists could, also, use the sea to infiltrate and attack land-based targets. Pipelines, refineries, pumping stations have been among terrorists' targets in recent years. In the Mediterranean, possible attacks on tankers, terminals or pipelines flowing there would have a significant impact on a global scale. The same is true for attacks at crossing points to and from the Mediterranean. The morphology of the Mediterranean, which requires passage through straits, such as the Suez Canal, the Bosporus and Gibraltar, makes ships particularly vulnerable. Such scenarios include the risk of a potential environmental terrorism, affecting the environment and, therefore, tourism, which is one of the biggest sources of income in the region. These scenarios become even more nightmarish, if there was an attack with a ship trapped with a weapon of

mass destruction. While previous attacks have used ships loaded with explosives, one could also imagine an attack using aircraft.

The consequences from energy-related maritime terrorism in the Mediterranean can include human casualties, a blow on the economy and an environmental impact. As regards the implications for the global economy in particular, these could be huge. Apart from jeopardizing the safe flow of oil and gas, implications could include rising oil prices, disruption of trade, the use of more time-consuming detours that would increase the cost of transportation, crowded passage points and ports, more expensive insurance premiums, environmental disasters and a blow on tourism. The straits, in particular, could be blocked for several days, depending on the size of the damage caused and controls or safety measures taken, and therefore crossing them would slow down, with again financial implications. The same goes for hits on ports and oil terminals.

A very alarming scenario is posed by the possibility of ISIS securing territory on Libya's Mediterranean coast. ISIS has recently been making inroads along the coast of Libya taking control of the port city of Derna and nearby Sirte, just a few hundred miles across the water from mainland Europe. Greater ISIS access to the Mediterranean would be deeply troubling to the region and a large strategic advance for the terrorist group. Such a development could increase ISIS's potential for attacks in Italy, Greece and elsewhere in Europe. With the use of small boats, ISIS could launch terrorist attacks in the Mediterranean that could expose it to hijacking, kidnappings and damage of vital energy infrastructure and vessels.

Piracy is another dimension of maritime risks and some acts of piracy have targeted oil shipments. The vast majority of pirate attacks against energy vessels occur against oil tankers. Pirates have also demonstrated the ability to attack LNG carriers and offshore drilling platforms successfully. There have been a few notable cases where tankers have been hijacked and the crews held for ransom. It should, also, be noted that many of the modern times pirates are terrorists coming from Islamic extremist groups. International efforts to freeze financial resources of terrorist organizations have led such groups to piracy as an alternative means for their financement. Today, piracy is being addressed by the international community in the Gulf of Aden, around the Somali coast and in the Indian Ocean. However, piracy is being spread worldwide. It appears already in the Red Sea and it could be extended to the Mediterranean. European officials have recently been alarmed by the possibility of ISIS also bringing Somali-style piracy to the Mediterranean. While ISIS is gaining control of ports and vessels in Libya, it could launch pirate attacks in the the Mediterranean.

Political instability in the region can also cause the disruption of energy flows. Conflicts or hostile action can impede the freedom of navigation or they can cause damage on infrastructure. Recent instability in Egypt, for example, has caused concern, since the country has been struggling to keep the peace in the area around the Suez Canal and the Sinai Peninsula. A recent rocket attack on the Cosco Asia, a giant container ship, was not the first time that terrorists tried to target ships passing through the Suez Canal. Closure of the Suez Canal would have significant financial implications, one example of which would be the addition a time-consuming and more costly detour around the Cape of Good Hope.

Finally, technological advances now allow new opportunities to emerge related to the exploitation of various maritime resources. The sea can offer almost one third of the oil and natural gas worldwide consumption. It is estimated that 40% of the oil and 60% of the gas currently consumed in Europe are drilled offshore. Gradually the sea also provides more renewable energy resources.

The ability of coastal states to protect their territorial integrity and ensure their sovereignty on their maritime zones is, therefore, expected to become increasingly important in the future. The anticipated growth of human activity in the seas and the need to produce energy from the sea will contribute to this. This can cause conflicts at sea between state, but also non-state, actors, because of competition for these scarce resources. As a consequence, the majority of states today extends or wishes to extend their territorial waters to 12 n.m. and their Exclusive Economic Zone to 200 n.m., which creates vast maritime surfaces for surveillance and protection and disputes with neighbouring countries on the delimitation of these zones.

One such great challenge is posed by the energy factor in recent developments in the Eastern Mediterranean. The discovery of gas implies that the region will remain an important energy provider for Europe in the foreseeable future and that it can also provide indigenous resources (in the case of

Cyprus). The new energy resources of the region overall could complement the Southern Corridor in the medium term. This challenge will only be reinforced by existing plans to construct large-scale solar projects in the Southern Mediterranean, as well as by possible future plans on new forms of renewable energy from the sea, such as wave energy, floating photovoltaic panels and biofuels produced from algae.

The risk implications of the offshore energy findings in the region add a significant new security dimension in this maritime environment. Disputes of the riparian states over maritime zones and possible asymmetric threats against energy assets in the region reinforce fears. Turkey, Israel, Cyprus, Greece, Lebanon, the Palestinians have already entered the fray and Egypt, Libya and Syria could follow. Moreover, drilling platforms, expected to be built at sea, and other related installations or transfer means are potential targets. Recently, Israel called on the EU to support the East Med pipeline project that would connect the natural gas fields in Israel and Cyprus to the EU via Greece. An LNG terminal at the coastal area of Vassilikos in Cyprus is a complementary project of extreme importance that is still on the table. These energy assets could be highly vulnerable in case of a terrorist attack or during an armed conflict. A possible attack on the rigs, for example, could include missiles launched from tens of kilometres away, proximity attacks by frogmen, a collision with an approaching boat or the intentional crashing of manned or unmanned aircrafts. While the drilling companies are responsible for security within the rigs and they hire private security companies for that, private security guards might be able to prevent rigs from being taken over, but are unlikely to help them withstand an outright attack. A more remote threat scenario is posed by the possible future transfer of energy from renewable sources via undersea cables, which are much less vulnerable to attacks. Nevertheless, this possibility has also been referred to. For the purpose of protecting such installations off-shore and along the coast, Israel recently launched a plan of adding new warships and submarines to it's naval fleet and of deploying hundreds of soldiers in the area, in order to protect above and beneath the water. In addition, Israel Air Force "Shoval" drones will patrol the area and intelligence-gathering and radar equipment will be installed on the platforms. Also, intelligence efforts have been refocused toward threats to the maritime facilities. The threat is quite real, since, given the situation in the region, advanced weaponry fired from Lebanon, the Gaza Strip or the Sinai Peninsula could threaten offshore facilities. For example, Hezbollah has threatened to protect the maritime assets of Lebanon warning Israel not to try to steal Lebanon's resources. The organisation is thought to have an arsenal of thousands of rockets, midget submarines, exploding boats and armed private planes, which could potentially reach targets in the Eastern Mediterranean.

Both the conventional and asymmetric challenges described above draw a rather complex and alarming picture as regards energy security in the maritime environment of the Eastern Mediterranean. The importance of the region for the economic and energy-related interests of the Euro-Atlantic community makes it imperative that these challenges be properly addressed.

5. Energy Security in the Maritime Environment of the Eastern Mediterranean as an Opportunity

The fact that the seas are associated with critical economic interests that require protection by military means is not new. All major trading powers have always protected their interests with powerful Navy. What is new is the collective approach and cooperation among partners in this field that now acquires a central role in international strategic planning. NATO and the European Union are in a process of developing a particular strategy on maritime security. They have also prioritized energy security within this context and in their overall policies.

Modern challenges in the maritime environment are particularly demanding for one country to face alone. The threats are common and the interests that need to be safeguarded are mutual. Moreover, this is a costly undertaking, especially at this time of financial strain. It will, therefore, take a greater part of the financial burden to be undertaken jointly. For all these reasons, collective approaches are deemed NATO and the EU should focus on three main areas, namely the operational, the relevant infrastructure and maritime diplomacy. The overall aim would be to prevent threats, such as terrorism, piracy, proliferation, and to ensure a safe environment for the extraction and transport of energy.

Maritime operations in the region are important. NATO's Operation Active Endeavour is considered of utmost

importance for monitoring maritime communications in the Mediterranean. The operation has proved valuable for the safe transportation of energy resources, but also for securing economic activity in the Mediterranean in general.

Infrastructure, such as the NATO Maritime Interdiction Operational Training Centre (NMIOTC), plays an important role in enhancing maritime security by providing expertise in boarding techniques, by contributing to counterterrorism missions in the Mediterranean and by offering the relevant training.

Maritime diplomacy and multilateral defense cooperation in the Eastern Mediterranean should bridge interests and threat assessments between Euro-Atlantic institutions and the countries of the region and it would cultivate trust with Euro-Atlantic partners.

By ensuring collectively a safe maritime environment for energy transfer and production in the Eastern Mediterranean and by cultivating a trusting and cooperative environment with Euro-Atlantic partners in the region, NATO and the EU could tap into the multiple opportunities that the area can provide as regards energy security.

6. Conclusions

Energy security in the maritime environment is one area that NATO and the EU are increasingly including in their strategic planning, threat assesments and policy making. The Eastern Mediterranean in particular is now emerging as a region, which requires special attention in this regard. The geopolitical importance of the Eastern Mediterranean, a key maritime route for the transfer of energy resources, is now enhanced by its possible selection for the transit of future energy resources from the periphery of Europe, by the increasing use of gas and oil from the countries of North Africa and the Middle East, as well as by its own energy reserves. At the same time, the Eastern Mediterranean has been the scene of longstanding security challenges, while in recent years many more have emerged. These challenges have a strong maritime component and they could threaten energy security in the maritime environment. Due to the importance of the region for Euro-Atlantic energy security, a robust collective approach to the security challenges emanating from the Eastern Mediterranean is required, so that opportunities arising from this area can be better exploited.

Marina Skordeli

Dr Marina Skordeli is the Director of the Jean Monnet European Centre of Excellence of the University of Athens. In 2004-2009, she served as Foreign Policy Advisor to the Prime Minister of Greece, Kostas Karamanlis. In 2002-2004, she held the position of Political Advisor on European security and enlargement at the European People's Party, in Brussels. She holds a PhD on "The CSDP and security in the Eastern Mediterranean". She has been teaching, lecturing and publishing in Greece and abroad on European defence, security in the Eastern Mediterranean, maritime security and Greek foreign and defence policy.

Illicit Trafficking at Sea Training opportunities at NMIOTC

by Ioannis Argyriou
Lieutenant Commander GRC (CG)
Instructor at NATO Maritime Interdiction Operational Training Center (NMIOTC)

Shipping is an important factor for the world trade as well as for the universal economy, social cohesion and prosperity of the people. Its safe conduction, however, raises issues of maritime security, which troubles the international community to a great extent. In order to take all the necessary measures to ensure the safe transportation of people and goods in the marine environment, we have to be aware of a wide spectrum of illegal actions that are committed at sea, such as piracy, armed robbery, human trafficking, drug trafficking and the illegal transport of weapons and dangerous substances/materials that can be used by terrorist organizations. The legal evaluation and proper response to such actions depends highly on the maritime area where these are committed.

An imperative prerequisite for the elimination or restriction of illegal acts at sea is to enhance the political and economic stability throughout the world. Within this context the global community in cooperation with international organizations (e.g. the International Maritime Organization - IMO) are undertaking initiatives to eliminate illegal acts through regional capacity building or multinational allied law enforcement operations. However, apart from international initiatives or allied operations in international waters, a key factor for controlling and hindering illegal acts at sea is the role and responsibilities of coastal states in the region of their sovereignty.

To that aim, the Maritime Interdiction Operational Training Center (NMIOTC), an accredited NATO training center located in Crete-Greece, has proven a very successful tool. In this Center, with its high value training infrastructure and certified educational expertise and procedures, a series of trainings are conducted as well as training and developing bonds for future collaboration among personnel from very different states. Theoretical and practical training provided respond to a wide spectrum of maritime operation issues, while the conduction of joint practical exercises help to evaluate the effectiveness of procedures and any improvements required thereof. To enable learners to act in a realistic environment, the practical training takes place on fully equipped

mock ships as well as perfectly up-to-date simulators. All current trainings are focused on issues of criminal acts investigation in the maritime environment, providing a wide range of knowledge from intracurricular fields, with the participation of officers from US/DEA, the Hellenic Police, the Interpol, the US National Security Agency/Naval Criminal Investigation Service located in Chania and the Naval Hospital of Crete as subject matter experts.

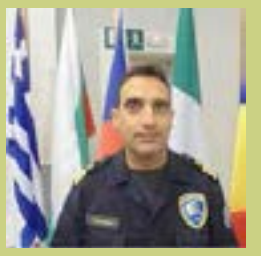
One of the trainings which is going to be conducted this year is the "Illicit trafficking at Sea". The particular course covers extensively the need for training on the suggested subjects and aims to provide quality, sustainable, and effective training for government and state officials and practitioners who are engaged in policy development, law enforcement, intelligence and interdiction operations aimed at countering illicit trafficking. Such trafficking may involve the illegal trade in drugs, small arms and light weapons (SALW) as well as the smuggling of human beings and/or human organs. The objectives of these trainings is to improve the knowledge and skills of trainees on human trafficking, drug trafficking, firearms trafficking, Crime Scene Investigation and Evidence Collection, Illicit trafficking related organized crimes, biometrics, legal issues on Illicit trafficking and interrogation Tactics. Moreover practical training is provided on mock up ships on the subjects on crew control as well as on the techniques of searching of area.

The trafficking of human beings is viewed by the international community as a major concern and has been described as amounting to modern day slavery. A large number of men, women and children are victims of human trafficking for different reasons (sexual, forced labor and other forms of exploitation). Moreover, drug trafficking is another pervasive form of illicit trafficking that remains highly profitable and extremely difficult to control, despite increasing efforts by the international community to contain and then reduce it. The mission of the traffickers is to get the drugs from the suppliers to the consumer as efficiently as possible without being detected. In addition the illicit trafficking of firearms occurs in all parts of the globe but is concentrated in areas afflicted by armed conflict, violence and organized crime, where the demand for weapons is often highest. All of the above issues related with transnational organized crime. Transnational organized crime (TOC) poses a significant and growing threat to national and international security, with dire implications for public safety, public health, democratic institutions, and economic stability across the globe.

Global criminal activities are transforming the international system, changing the rules, creating new players and reconfiguring power in international politics and economics. States and international organizations have largely failed to anticipate the evolution of transnational organized crime into a strategic threat to governments, civil societies and economies.

Summarizing we can say that various forms of illegal activities can take place in the marine environment. The international community has taken steps to reduce these phenomena by conducting naval allied operations. However, while the presence of coalition forces may have reduced phenomena of illicit trafficking, it has not entirely eliminated them. The coastal states play an important role in this effort. Within this context, the NMIOTC is taking initiatives intended to enable the coastal states to train their staff so as to perform their duties more efficiently. Additionally, one of the main objective of these course is the exchange of views among the staff of these countries in order to achieve better and more efficient cooperation between them towards the common cause of enhancing maritime security.

Ioannis Argyriou



Lieutenant Commander GRC (CG)
Instructor at NATO Maritime Interdiction Operational Training Center (NMIOTC)
In 2001, he joined the Hellenic Naval Academy (Coast Guard Officers' Cadet School) and in 2002 he was sworn in as Ensign of the Hellenic Coast Guard. During his career in the Hellenic Coast Guard he has served in a number of local Port Authorities. In March 2014 he was appointed a National Briefing Officer and liaison by FRONTEX on issues of illegal immigrants. Since April 2014 he has been serving at NATO Maritime Interdiction Operational Training Center (NMIOTC) as an instructor and an officer of primary responsibility for the conduction of training events by the International Maritime Organisation (IMO) and East Africa Standby Force (EASF). Moreover he coordinates the training for various groups from NATO state members and other affiliated countries.
E-mail: argirioui@nmiotc.nato.int - johnarg00@yahoo.gr Mobile: (0030) 6974014100

TRENDS IN GLOBAL ENERGY ECONOMICS, AND THEIR IMPLICATIONS FOR MARITIME ENERGY INFRASTRUCTURE SECURITY AND RELATED INTERDICTION TRAINING.

byStephen L. Caldwell
Member, US National Maritime Security
Advisory Committee

ENERGY INFRASTRUCTURE AND SECURITY

Abstract

This paper discusses trends in energy economics and their impact on the security of maritime energy infrastructure. After revisiting selected terrorist and pirate attacks on tankers and offshore facilities, the paper summarizes programs to protect such infrastructure. The paper then discusses more recent trends such as the rise (and subsequent fall) of piracy off the Horn of Africa. More recently in other parts of the world pirates and other criminal networks have specifically targeted energy infrastructure. Other developments, such as sanctions against pariah countries provide additional challenges in monitoring and interdicting tankers through international waters. The paper also weaves in recent economic trends in energy markets—such as the fall in energy prices, the American Energy Renaissance and the rise of Liquefied Natural Gas as both a commodity and vessel fuel. The paper concludes with the implications of these trends for maritime interdiction and training

Key Words

Maritime; security; energy; offshore; piracy.

Introduction

As an alliance that stretches across many oceans and seas—the Atlantic, Baltic, and parts of the Mediterranean—the North Atlantic Treaty Organization (NATO) has the maritime security mission of protecting its sea lanes of communication. And as an alliance that produces and imports much of its oil and gas within and across the maritime domain, NATO must pay particular attention to the maritime security of energy commodities. Recognizing this, NATO's Strategic Concept emphasizes the importance of emerging threats that include counter-terrorism and energy security. The Strategic Concept also emphasizes an enhanced awareness of border and port security. Related to this, NATO has a designated organization—the NATO Maritime Interdiction Operational Training Centre (NMIOTC)—with the mission to train member forces for maritime interdiction. This paper, developed for the June 2015 NMIOTC 6th Annual Conference, examines several trends in energy economics, both long-term and short-term, and discusses their implications for the NMIOTC program of training.

Continued Threats to Maritime Energy

One of the long term trends in energy markets is continued security threats to maritime energy infrastructure—both vessels and facilities. Reports of the U.S. Government Accountability Office (GAO) have documented that for more than 10 years, terrorist have exploited the vulnerabilities of energy tanker vessels. In general, tankers are vulnerable to attack due to their predictable schedules and routes, and long voyages in open seas and politically unstable waters. As an example of predictable routes, tankers also sail through well-known choke points such as straits and canals. During these voyages, tankers are vulnerable to a number of types of attacks, including suicide attacks, armed assaults, and stand-off missile attacks. Terrorist have exploited these vulnerabilities, attacking the MS Limburg in 2002, and more recently, the MV Star in 2011.

In addition to terrorists, pirates have also exploited tanker vessel vulnerabilities. Somali-based piracy off the Horn of Africa rose rapidly in 2008, peaked in 2011, but has fallen to almost zero in recent years. According to GAO, the recent decline in attacks was due to broad efforts to protect vessels including industry best management practices, private security companies, and naval escorts—such as NATO's "Operation Ocean Shield." However, even during the peak in piracy off the Horn of Africa, the impact on energy tankers was limited because many of them were not the "slow and low" prey that the pirates preferred. One early exception was the tanker Sirius Star which was slow and low, and reported to have stopped when approached by the pirates. But even in that case, the ransom of $3 million paid to pirates to release the tanker was far below the value of the oil cargo. This is a far different situation than the more recent pirate attacks in the Gulf of Guinea and Southeast Asia, which will be discussed later in this paper.

GAO documented several steps that have been taken to protect tankers. In response to the terrorist and pirate threats, several protective measures have been taken at the national and international level. In the United States, as in other nations, there are regulations and operations to protect tankers visiting their ports. These activities, generally led by the U.S. Coast Guard (USCG) ensure that tankers—regardless of flag—meet national and international requirements to have security officers and security plans in place. USCG and other federal agencies run security checks on the crews of inbound energy tankers. Within U.S. ports, USCG and state and local harbor police may escort tankers in and

out of port, based on risk, location and the availability of resources. In addition, based on a risk matrix, USCG and other federal, state, and local partner agencies may board and inspect high-risk energy tankers arriving at U.S. ports. At the international level, the International Maritime Organization (IMO) adopted global standards for maritime security (the International Ship and Port Facility Security Code or "ISPS" code). Also on the international front, USCG also visits and assesses the security at foreign ports that are departure points for vessels (including tankers) coming to the United States. Finally, and as mentioned earlier, U.S. and allied navies patrol high-risk international waters, such as piracy-prone waters off the Horn of Africa.

Energy facilities, both in port and offshore, also have vulnerabilities that have been exploited by terrorists. GAO's report on offshore facilities noted they are particularly vulnerable due to their location in open waters, far away from military or law enforcement response assets. The locations of these facilities is common knowledge because of their concentration in well-known areas such as the Gulf of Mexico and the North Sea. Officials at some facilities are concerned that small vessels carrying fishermen or divers frequently violate safety zones around them and, in some cases, try to attach their small vessels to the facilities. Terrorist have targeted and attacked such facilities, including two offshore of Iraq in 2004. In that case, terrorist using a speed boat with explosives attacked the Al-Basrah and Khwar Al'Amaya oil terminals, killing three U.S. sailors. In addition to the human cost, the loss of two days of operations cost almost $40 million in lost revenue. Further, the explosion and sinking of the Deepwater Horizon oil rig in the Gulf of Mexico (which was admittedly not a terrorist attack) showed that a major incident on an offshore facility could cause economic and environmental consequences in the billions of dollars. As late as 2011, US intelligence reported that Al Qaeda was still interested in targeting maritime energy infrastructure in western countries (e.g., NATO members). More recently, terrorist groups such as MEND in the Niger Delta have attacked onshore and offshore energy facilities as part of their political agenda.

Similar to tanker vessels, several steps have been taken to protect facilities. Of some 4,000 offshore energy facilities in the Gulf of Mexico, GAO found that about 50 meet the threshold for USCG security regulations. These 50 offshore facilities—as with waterside terminals—must have security officers and plans in place. The USCG approves such plans, and inspects the facilities once per year to ensure compliance with their security plans. For waterside terminals, and to a lesser extent offshore facilities, USCG and state and local harbor police conduct patrols based on risk, location and the availability of resources. For the offshore facilities, USCG also established an Area Maritime Security Committee for the Gulf of Mexico, to help identify vulnerabilities, share information, and develop response and recovery plans. Finally, US agencies have held major exercises, such as the National Law Enforcement exercise in 2009 (also known as "NLE 2009") to test the US response to a terrorist attack on, among other things, offshore facilities in the Gulf of Mexico. One threat to both tankers and facilities is the so-called "small vessel threat" from anonymous and agile smaller boats that could evade detection and use explosives to attack energy infrastructure or other maritime targets. To address this threat, the U.S. Department of Homeland Security developed and is working to implement its Small Vessel Security Strategy.

These past and ongoing threats to maritime energy infrastructure do not necessarily indicate that any changes are needed in NMIOTC interdiction training. While the threats to tankers and facilities remain, protective measures—such as those against small vessel attacks—have been in place by the United States and other NATO members for several years. The challenge in past years and continuing into the present is that military and law enforcement agencies have limited resources to ensure the security of tankers and facilities against an unknown threat that could strike in any place at any time. Also, the lack of actionable intelligence or a credible threat to domestic US ports—a situation that is several years old—makes it more difficult to justify more resources for maritime security programs. But the limits on resources to train or conduct protective operations is a separate issue than whether the current tactical training needs to be changed. Given the long standing nature of these threats, NMIOTC has already developed and delivered tactical training for these standard terrorist and piracy scenarios—and should continue to do so. But the continued existence of these threats does not indicate that any major change is needed in NMIOTC training.

ENERGY INFRASTRUCTURE AND SECURITY

Increasing Use of Technology

Another long term trend in energy economics is the continued transition to new technology, sometimes in ways that create additional security challenges. For several years, industry has worked to become more economically efficient by using more sophisticated technologies to find, recover, store and distribute energy. Offshore production continues to use new technology to move to deeper water (e.g., beyond 10,000 feet) and operate in more harsh environments (e.g., the Arctic). The development of hydraulic fracturing (or "fracking") of shale deposits has led to significant recovery of oil and gas in previously unproductive regions. The more sophisticated facilities, and the desire to increase efficiency of operations, has led to more networked facilities with remote access control. As an example, DNV GL recently announced its plans for "Solitude" an unmanned floating LNG concept for remote offshore areas. And with the continued trend toward complex technologies, the related regulatory regimes have also become more complex for national governments.

A key part of the transition to new technology has been the use of automation in ways that create cyber vulnerabilities. GAO found there has been a continued increase in the use of Industrial Control Systems, which are automated systems used to control industrial processes such as manufacturing, product handling, production and distribution. Specifically, these systems are used to operate motors, pumps, valves, signals, lighting, access controls, and to facilitate the movement of goods throughout maritime terminals using conveyor belts or pipelines. These systems are now frequently networked to business operations systems, and remote control centers, thus creating potential cyber vulnerabilities for hackers and criminals to exploit.

Cyber security weaknesses in the maritime industry, including the energy sector, are now widely recognized. Several recent studies in the United States (by the Brookings Institution, and GAO), Europe (By the European Network and Information Security Agency), and Australia (by the Office of the Inspector for Transport Security) looked at maritime cyber security issues. The Australia study specifically focused on offshore energy resources, and made specific recommendations related to cyber security. The several reports, while differing in their scope and methodology, collectively raised five areas of concern and related recommendations. These similar concerns were (1) maritime operations are growing more automated and interconnected, (2) stakeholder awareness of cyber threats and their cyber hygiene has been weak, (3) cyber vulnerabilities exist, with potentially harmful consequences to ports, (4) risk assessments to date have generally focused on physical security and not cyber security, and (5) threat information sharing is ad hoc and needs to be improved.

The long term technology trends and their implications for security—especially cyber security—will require continued monitoring and decisions by NATO and NMIOTC. Overall, NMIOTC should monitor the development of any technologies that may impact the maritime interdiction mission. One thing to monitor might be the development of more sophisticated Mobile Offshore Drilling Units. It is not hard to think of a scenario where NATO maritime forces may have to board such a vessel. Cyber technologies also should be monitored, but raise more fundamental questions about their relationship to the missions under discussion. While the cyber threat is real, to what extent is cyber security a maritime interdiction issue? For example, is there a role for offensive cyber operations to interdict vessels that are suspected of being hijacked or carrying contraband? Cyber security also raises questions about the roles of industry versus government to secure cyberspace. Currently there is an ongoing debate within NATO countries and NATO itself about who in their respective governments or militaries should take the lead for defensive and/or offensive cyber operations. NATO needs to plan out its role, and then determine whether NMIOTC also plays a part in that role. If NATO does designate cyber security as a role for NMIOTC, then appropriate technical tactics and training would need to be developed. And such cyber training would need to be integrated into the existing training program at NMIOC as appropriate.

Falling Energy Prices

Moving from long-term energy trends to more recent trends, the prices of energy have fallen dramatically in the last year. From June 2014 to June 2015, the market price of benchmark North Sea Brent oil fell from $115 to $50 per barrel, and looks to continue falling. Some observers, such as energy analyst G. Allen Brooks, most observ-

ers, trace the reason to a November 2014 decision by Saudi Arabia not to cut its oil production, thus keeping global supply high. Brooks speculates that Saudi Arabia did so to preserve their long term market share, to punish other OPEC members violating production quotas, and to force out non-OPEC countries with higher production costs—such as Canada tar sand energy production. Another reason for the decrease in prices was a glut of supply rising from the American Energy Renaissance fracking operations in shale deposits (see more discussion of this Renaissance in the next section of this paper). Beyond the reasons for the decline, does the decline foretell a sharp drop in maritime energy development? According to Brooks, offshore development in shallow waters probably hold little hope for meaningful oil output growth because they have already been highly explored and developed, leaving few new areas of opportunity. However, despite the drop in oil prices, deepwater development and output will remain growth markets through 2025. An analysis by Norwegian consultancy Rystad Energy states that, despite the current negative sentiment, there will be positive offshore energy growth rates by 2017.

The implications of lower prices for NMIOTC training remain uncertain, so the trend does not necessarily warrant any changes to the curriculum. This is because it is hard to predict the mid or long term impact on maritime security issues. Low prices could have many potential impacts such as
(1) reducing offshore activities and thus creating fewer maritime targets, (2) forcing maritime energy firms to cut costs, reducing security spending and thus increasing vulnerabilities, and (3) making it less attractive for pirates or criminals to hijack tankers and sell the oil on black markets. Another more sinister impact might be unintended consequences such a reducing stability in current energy producing countries. Alternatively, instability in such countries (e.g., Libya) might impact production, and thus global prices. And dramatic price swings in any global market could swing back in the other direction, making this trend a transitory blip. In any case, none of these theoretical impacts are certain enough to suggest specific changes to NMIOTC's training program.

The American Energy Renaissance

Another recent trend in energy economics is the so-called American "Energy Renaissance." According to the U.S. Department of Energy's Quadrennial Energy Review, the United States has recently achieved unprecedented energy production growth, and is now the world's largest producer of oil and gas. The review also notes that U.S. petroleum consumption is flat and coal consumption is declining. These factors, combined with new clean energy technologies and improved fuel efficiency, means U.S. "energy security" is stronger than it has been for more than half a century. According to the Quadrennial Energy Review, "the focus of US energy policy discussions have shifted from worries about rising oil imports and high gasoline prices to debates about how much and what kinds of US energy commodities should be exported." And that department's Annual Energy Outlook 2015 predicts that, under certain assumptions, the United States will be a net exporter of gas by 2017, and net exporter of oil by 2020.

According to the Commandant of the USCG, the American Energy Renaissance is causing tremendous change in the U.S. Maritime Transportation System. As the United States expands exports of energy, many former import terminals in ports will become export terminals. In addition, the Quadrennial Energy Review notes that fracking has reversed midstream distribution from "south-to-north" to "north to south" through multiple transportation modes, including the maritime mode. That is, instead of energy being imported into Gulf of Mexico states refineries, then the refined product being shipped into the central states consumers… now the energy is recovered in the central states and shipped to Gulf of Mexico state refineries. To facilitate this reverse flow, the United States is using the Mississippi Basin and the Intercoastal Waterway—which have more miles of navigable inland waterways than the rest of the world combined. Oil and gas from fracking are now being moved in large quantities in tank barges on the "Marine Highway" of the Maritime Transportation System. More than 4,500 tank barges transport liquid fuels and coal nationwide. Between 2010 and 2013, there has been a 300 percent increase in crude oil deliveries by barge.

The implications of the American Energy Renaissance for NATO maritime interdiction training will require some thought and decisions by NMIOTC. In general, the maritime security requirements of energy tankers and terminal facilities in port and coastal areas is

similar whether importing or exporting energy. So appropriate NMIOTC tactical training is likely in place already for such scenarios. However, for the United States and other NATO members producing oil and gas in their interior areas, and transporting it in rivers and other waterways, the threats and vulnerabilities are different from ports and coastal seas. This raises the question of whether this is a broad issue facing several NATO countries, or more of a niche threat facing the United States and few others. There is also the question of whether protecting internal waterways is the mission of law enforcement authorities or the military. But if this is an issue that NATO decides to take up, and it decides that it is a core military maritime interdiction function, then NMIOTC should examine whether new tactical training is needed for scenarios involving threats to energy transport in narrow rivers, channels, and locks. Figure 1 below shows an energy tanker in the narrow Houston Ship Channel.

Figure 1. Energy Tanker in the Narrow Houston Ship Channel
(Source: the author)

Expanded Use of LNG as a Commodity and Fuel

The increase of Liquefied Natural Gas (LNG) as a commodity and fuel is another recent trend in global energy economics. Largely as a result of the American Energy Renaissance, the use of LNG as a general energy source has expanded significantly. Natural gas is attractive as an energy source because it burns "cleaner" than other sources such as oil and coal. Also natural gas shrinks in volume to 1/600th when liquefied into LNG (by cooling to -260 degrees F) making it much easier to transport. In the United States, natural gas is abundant and cheap since production from fracking is significantly higher. Because of this, the use of gas to generate electricity in United States is projected to grow from 16% of all energy sources, (2000) to 31% (in 2040). The U.S. industrial sector as a whole has taken advantage of this situation by converting to gas. Now the United States is positioned to become a major exporter of LNG, just 10 years after accelerating its import capacity. As an example of this reversal of fortune, in May 2015, the U.S. Department of Energy authorized the export of LNG from Cove Point, Maryland, a long-time LNG import terminal.

The same qualities that make LNG attractive as a general energy source, also make it attractive as a fuel for vessels. Specifically, availability, costs and cleanliness are making LNG attractive as a vessel fuel, particularly as some regions (e.g., the State of California) require vessels to use cleaner fuels. Some U.S. companies like Crowley and TOTE are moving ahead smartly, and have ordered several purpose-built LNG-fueled vessels. Crowley is expanding its business for LNG as both a commodity and fuel in the Caribbean, and is conveying LNG in container-size quantities. At the international level, IMO is moving ahead with safety and crew training guidelines for LNG-fueled vessels (and other "low flashpoint fuels"). At the U.S. level, USCG is moving ahead with policy letters for LNG-fueled vessels, LNG bunkering facilities, and with design standards for U.S. barges intending to carry LNG in bulk (e.g., non-self-propelled barges for LNG bunkering). Despite its positive qualities, there

are some security issues with LNG in ports and vessels. LNG is considered a safer "low flashpoint fuel" and LNG vapors mixed with air are not explosive in an unconfined environment. However, GAO had noted that an incident involving an LNG tanker or terminal could have significant negative public safety consequences. In some very specific scenarios, an attack or incident could result in a very hot-burning fire. Also, LNG vapors mixed with air in the right ratio in a confined environment could be explosive. Despite the general consensus that LNG is safe, and that the industry has a good safety record, some in the public have strong fears regarding LNG and the conditions in which it might cause a fire or explosion. Because of these fears, some of which are very local, security measures for maritime LNG assets vary across the United States. In Lake Charles, Louisiana (a rural area with an LNG terminal), there are relatively few extra security measures in place. In contrast, in Boston, Massachusetts (an urban area with an LNG terminal), there are extraordinary security measures in place. These include having 6 vessels escort the tankers into and out of the port, shutting down the airport runway when the tankers pass by, and closing a major bridge when the tankers pass under. Figure 2 below shows the USCG escorting an LNG tanker in Boston Harbor.

NMIOTC should continue to monitor development of LNG markets and technologies, especially as they relate to vessel design for LNG-fueled vessels. In general, the security requirements of LNG tankers and facilities is similar whether importing or exporting LNG. However, LNG as a fuel raises new issues about its explosiveness in confined spaces such as below deck on vessels. NMIOTC could follow the developments and designs of vessels using LNG as fuel, and determine whether they require new training or not. In doing so, NMIOTC could research questions on the potential impact of using weapons in a confined space (like below deck) on an LNG-fueled vessel. For example, on such a vessel, could a below deck shootout during an opposed boarding lead to any LNG leaks in a confined space which could result in a fire or explosion?

Figure 2. USCG escorting an LNG Tanker in Boston Harbor (source GAO-08-141)

Growing Energy Black Markets

The final trend discussed in this paper is growing energy "black markets," particularly those involving energy tankers. In recent years, piracy and other maritime crime have given rise to growing black markets for stolen oil. GAO found that, unlike piracy off the Horn of Africa—with its business model focused on vessels & crew for ransom—the piracy elsewhere such as the Gulf of Guinea has a business model focused on stealing energy commodities. This has been an ongoing problem in the Gulf of Guinea, perhaps best documented through a series of Chatham House conferences and reports on Nigeria. Chatham House researchers found that attacks on tankers were well-choreographed, conducted with knowledge on how to operate tankers, and done with precision based on prior intelligence about tanker schedules and routes. They also found that corruption and fraud are rampant in Nigeria's oil sector, concluding that the country's crude oil was being stolen on an "industrial scale."

Piracy and maritime crime against oil tankers is also a growing issue in Southeast Asia. In fact, piracy is up in SEA by 23% in the last year (up to 183 incidents in 2014). Similar to their counterparts in the Gulf of Guinea, part of the pirates' business model in

Asia focuses on stealing energy cargoes. The problem was recently highlighted by the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against ships in Asia (ReCAAP) in its Annual Report and two Special Reports on Incidents of Siphoning of Fuel/Oil at Sea in Asia. The reports note that of the 13 incidents categorized as "very significant" in 2014, all involved siphoning of ship fuel or oil. The majority of incidents occur at night in remote locations, which allow the pirates to "buy time" while they bring another ship alongside to siphon the oil, then then escape the scene of the crime. In three of the 3 incidents, the pirates had repainted and renamed the tankers to mask their true identities. ReCAAP assessed that at least 3 organized criminal syndicates were involved in these incidents. The reports attributed the surge in oil siphoning to high market prices, high taxes on fuel/oil, and demand in black markets.

In addition to pirates and other criminals, black-listed nation states and non-state actors are also using energy black markets. The United Nations Security Council adopted several resolutions imposing sanctions on North Korea and Iran which impact maritime energy shipping. The most recent resolutions were UNSCR 2087 on North Korea, and 2049 on Iran. However, both North Korean and Iranian shipping lines have sometimes worked successfully to mask their illegal shipping to get around sanctions. To further the effectiveness of such sanctions on Iran—formerly a major exporter of oil—the European Union has ceased all purchases of Iranian oil and gas. The U.S. Congressional Research Service has noted that the U.S. government has also adopted a number of its own Executive Orders and laws related to sanctions against Iran, some that impact maritime energy shipping. For example, laws PL-104-172 and PL-112-239 provide for sanctions on firms that deal with Iran's energy and shipping sectors. More recently, Congress has considered additional legislation that generally shut Iran out of oil export markets. Beyond such "pariah" nation states, there are reports that non-state actors (other than traditional pirates or criminal syndicates) are also using tankers to sell illegal oil on black markets. These actors include rebels in Libya and Syria (including "Islamic State" rebels"). The proceeds from such sales are likely re-invested into weapons and other contraband to support their political aims to overthrow established governments.

Whoever steals oil and fuel and sells it on the black market, and wherever it occurs, there are legal issues to consider in conducting maritime interdiction operations. One issue involves the location of the hijacking or other criminal activity (e.g., whether in international or territorial waters). Another involves the ownership and flag of the vessel and the stolen energy commodity. Yet another involves the level of evidence needed to determine the oil origin and ownership, and the chain of custody for that evidence to ensure a successful prosecution. A further issue involves the legal authority (or permissions for their own or other governments) granted to the law enforcement or military force conducting the interdiction. Finally, in some cases there are legal issues surrounding the complicity of corrupt authorities somewhere along the supply chain.

The rise in maritime incidents involving black markets have several implications for NMIOTC training. While many of these incidents are far from NATO's traditional area of operations, the attacks in the Gulf of Guinea affect oil production and transportation that was intended for NATO countries. Companies that have been targeted include Nigerian joint ventures with European oil companies. NMIOTC could develop various stolen oil scenarios and explore what appropriate legal procedures to include in its training. NMIOTC could also partner with non-NATO partner countries in areas prone to black markets, and help train their maritime law enforcement and military forces. In addition, NATO and NMIOTC could review the Chatham House report Nigerian Criminal Crude: International Options to Combat the Export of Stolen Oil for additional steps to be taken. Sample recommendations from Chatham House include better intelligence on the volumes of stolen oil, patterns of movements of stolen oil, the money trail for black market traders, and an analysis of related political and security risks.

Conclusions

NATO has made maritime energy security a high priority for the alliance. And NMIOTC has a proven track record of providing maritime interdiction operational training to naval and other maritime forces of both member and non-member nations. In that context, NMIOTC needs to monitor trends in maritime energy security and, where appropriate, make adjustments to their

tactical training. Some of the trends noted in this paper do not warrant any adjustments, while other trends suggest possible changes. For the long-standing trend of security threats to maritime tankers and facilities, NMIOTC should continue training for standard terrorism and piracy scenarios. For the long-standing trend of increasing technology complexity, NMIOTC should monitor new technology developments in general. For the subset of advanced Industrial Control Systems, and the cyber security vulnerabilities they bring, NATO and NMIOTC must determine their appropriate role. If a determination is made that NMIOTC does have role in cyber security, it should develop technical training and integrate that with its other training programs.

As for the development of inland oil and gas sources (through fracking or other means), and their transportation via inland waters, NMIOTC should consider tactical training for river, channel and lock scenarios. For the trend toward more LNG as a commodity and fuel, NMIOTC should follow developments and designs for LNG-fueled vessels. It should also study the impacts of using weapons below deck on such vessels. Finally, regarding the rise of energy black markets, NMIOTC should determine the legal basis for interdicting tankers with illegal energy commodities under various scenarios. Based on that determination, it might also want to add training on rules of evidence on the sources of such illegal commodities, as well as consider training non-NATO partners in areas prone to criminal black market activity.

Selected References

Brooks, G. Allen, article in The Maritime Executive, (March/April 2015), Will Offshore Exploration Fall Victim to Low Prices? Fort Lauderdale, FL, USA, Volume 19, Edition 2

Regional Cooperation Agreement on Combating Piracy and Armed Robbery against ships in Asia (ReCAAP), (2015), Annual Report on Piracy and Armed Robbery Against Ships in Asia, 1st January – 31st December 2014, Singapore

U.S. Department of Energy (DOE), (April 2015), Quadrennial Energy Review: Energy Transmission, Storage, and Distribution Infrastructure, Washington, DC, USA

U.S. Government Accountability Office (GAO) (August 2011), Maritime Security: Progress Made, but Further Actions Needed to Secure the Maritime Energy Supply, GAO-11-883T, Washington, DC, USA

U.S. GAO (March 2007), Maritime Security: Public Safety Consequences of a Terrorist Attack on a Tanker Carrying Liquefied Natural Gas Need Clarification, GAO-07-316, Washington, DC, USA

U.S. GAO (June 2014), Maritime Security: Ongoing U.S. Counterpiracy Efforts Would Benefit From Agency Assessments, GAO-14-422, Washington, DC, USA

Stephen L. Caldwell

is a member of the US National Maritime Security Advisory Committee. Before that, he was the Director for Maritime and Supply Chain Security Issues, U.S. Government Accountability Office, Washington DC, where he led GAO's studies on maritime security, and provided Congress with reports and testimony, including some specifically on maritime energy issues. He is a graduate of the University of California at Berkeley, and the U.S. Naval War College.

Risks and Interdependencies in the LNG Supply Chain

by David Incertis
Rafael Company
Project Manager, Safety & Security Dept., FEPORTS, Spain,
dincertis@feports-cv.org

Abstract

The LNG maritime transport system can be considered as a "floating" pipeline distribution and storage system in which a costly infrastructure for the liquefaction, regasification and storage of natural gas is involved. This system also involves critical information infrastructures related to important document and information flows which are determining for the right performance of this system. The high optimization of this mode of transport also implies the presence of risks

which come from the interdependencies among the different supply chain links, including physical sub-systems, persons and information and the special features of the LNG projects. As a critical infrastructure system involving sensitive sectors such as transportation and energy, these risks can be approached from the point of view of the capacity of the system, the supply availability and even geopolitical risk factors among others. This article describes the maritime part of the LNG supply chain, identifying its main links, their interdependencies and related risks which could affect the normal development of the busi-ness.

Keywords

LNG; transport; supply chain; risks; interdependencies.

1. Introduction

The most important natural gas (SC) chain is by LNG (Liquefied Natural Gas) tankers crossing the seas from the production to the distribution areas. LNG transport is an industrial energy transport system, meaning that it is designed as part of a specific industrial development (Hokstad et al., 2012). Each LNG transport system is unique and complex, but shares common aspects with others. One of these aspects is the presence of risks and hazards which come up from the interdependencies among the different SC links, including physical sub-systems, persons and information and the special features of the LNG projects and the properties of the gas. This article presents a categorization of these hazards and threats, covering physical and information threats, especially for those with regards illicit acts which could cause a serious brake of the gas supply, and a proposition for modeling the interdependencies between the main links of the SC. The article also describes a methodology for risk assessment (RA) of supply chains applied to the case of the LNG transport. The purpose of this methodology is to create a model to be integrated in a computer tool for assessing risks (and their interdependencies) of critical information infrastructures in several SCs involving maritime transport. This methodology for RA of SCs is being developed by the project MEDUSA (2014), co-funded by the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme of the European Union".

2. LNG Transport Hazards

Hazards in the LNG transport system can be considered from three perspectives:

1) The first one is due to the properties of LNG. Haz-ards related to its physical and chemical properties include flammability after vaporization into a gaseous state, freezing and asphyxia. Accidents in LNG trans-portation may occur especially during the compression or vaporization phases.

2) Derived of its properties, other kind of hazards which can be referred to as threats involve using the LNG flammability with terrorist purposes: For instance, a LNG tanker (usually containing more than one hundred thousand cubic meters of LNG) represents a potential hazard of explosion that can be caused by a deliberated attack. To stress that LNG does not explode or burn while in liquid state.

3) In third place, natural gas has become one of the most necessary energy sources in developed countries. An interruption in the supply of LNG, no matter if it is due to an accidental or provoked cause, may lead to a serious shortage in the gas stock of certain populated areas. It is especially critical in the winter season, when the energy demand shoots up, and sometimes there are unpredicted cold waves in a row which could compromise the energy requirements of entire regional areas. This is what makes the LNG transport system a critical system from the point of view of Critical Infrastructures Protection, even beyond the explosive nature of the natural gas.

3. The LNG Supply Chain Model

3.1 The LNG Supply Chain

The LNG SC can be represented in Fig. 1. This study focuses just in the maritime part of the LNG SC going from the liquefaction plant (port of origin) up to the receiving terminal and storage/distribution (port of destination

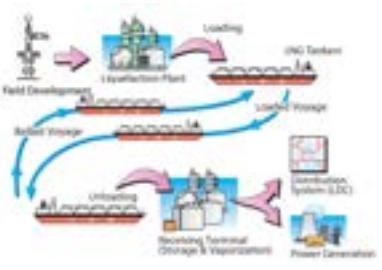


Fig 1. LNG Supply Chain (Source: IHRDC)

The LNG value chain consists of five elements:

1. Finding and producing gas
2. Gas treatment and liquefaction
3. Transport as a liquid
4. Receipt in terminals for storage and regasification
5. Distribution and consumption by power producers, industrial users, and households.

3.2 Supply Chain Actors

In the model proposed for describing the LNG SC, it has been considered two flows: physical flow and "cyber" flow (documents/information flow) including the main links or actors of Table 1 (just in the maritime part of the chain):

The uniqueness of each LNG project, plus the symbiotic relationship that traditionally exists between the various LNG value chain elements, results in a complicated process. Each project presents unique challenges that may take from 2 to 20 years to resolve. Due to this uniqueness for each LNG supply project, a series of simplifications and assumptions has been taken for the study use cases. Among them:

• Supply contracts phases (producer-customer / producer-carrier) have been omitted since they are based in long term delivery plans.

• The local agent at the import port deals directly with the ship owner /ship agent

• Document/information flows are actually bi-directional and parallel. A uni-directional and serial sequence is proposed in order to simplify the physical/ document flows.

• Cargo manifest is delivered, fees and taxes are paid and port services are requested via Port Community System (PSC) managed by the Port Authority. In the model proposed, an insurance contract covers the seller up to the port of loading and other insurance contract covers the buyer for the laden voyage and port of unloading / regasification.

Link/actor	Flow Model
Liquefaction plant	Physical
Seller/carrier/shipper	Cyber
Local Agent	Cyber
Ship agent	Cyber
Insurance company	Cyber
Loading port	Physical
Shipowner/ ship agent	Cyber
Sea Transportation	Physical
Port Services	Cyber
Unloading port	Physical
Customs	Cyber
Port Authority	Cyber
Buyer/importer	Cyber
Regasification	Physical
Storage	Physical
Distribution	Physical
Bank	Cyber

Table 1. LNG Supply Chain Links

4. Supply Chain Risk Assessment Methodology

4.1 Design Criteria

The main design criteria of the Medusa SC RA methodology are:

• Holistic view of the Supply Chain: Medusa aims to provide a holistic SC view in order to identify global SC threats, such as the cascading threats within the SC. These may not always be easy to identify from an organization-centric perspective.

• Collaborative: Medusa aims to promote collabora-tion between all business partners involved in the SC, by taking into consideration the views of all the partners.

• Compliance with standards: Medusa will be compliant with a range of existing standards such as ISO 28000, ISPS Code, ISO 27001, etc. In par-ticular, the goal of Medusa is to fully comply with (and also extend) the ISO28001 standard for SC risk assessment, as a means of increasing its adoption and achieving technological longevity.

4.2 Objective of the SC RA Methodology

The goal of the SC Risk Assessment Methodology is to:

1) Assess the overall risk of the examined SC Ser-vice.

• Input: Information provided by all the business partners involved in the SC.

• Output: For each business partner, the meth-odology will output a SC Service security policy, describing the minimum security controls that need to be implemented by the business partner.

2 Assess the risk of cascading effects, for various threat scenarios, by using the results of the risk as-sessment.

4.3 Steps of the SC RA Methodology

The proposed Supply Chain Risk Assessment Methodology involves the following steps (which are fully de-scribed in the SC RA Methodology proposed in the project Medusa):

Step 0: Scope of the SC Risk Assessment - Initially, the business partners (or the risk assessor that initiates the risk assessment in consensus with the business part-ners) shall define the scope of the SC Service (SCS) under examination and define the goal, the scope, and the outcome of the SCS. The risk assessor may create use-cases to clarify the business processes of the SCS, clarify its business role and functions within it.

Step 1: Analysis of the Supply Chain Service (SCS) - In this step, the SCS under examination, as defined in Step 0, will be decomposed. The actors of this step are the business partners, or the risk assessor that initiates the assessment in consensus with the business partners.

Step 2: SC-Threat Scenario Identification - In this step the threat scenarios against the SCS will be identified and assessed. A critical step to-wards threat identifica-tion and assessment is the use of a well-defined threat categorization. Threat identification will be derived from the model produced in Step 1.

Step 3: Assess the expected likelihood for all Threat Scenarios - In this Step, the expected likelihood for each possible Threat Scenario for the SCS under examination will be estimated. The likelihood of each TS will take into consideration two values: a threat value, reflecting the probability of occurrence, and a vulnerability value, reflecting the current level of protection against a particular Threat Scenario.

Step 4: Assess the consequence of each Threat Scenario for each business partner. - In this Step, each business partner participating in the SCS will be assessed for its expected consequence if a Threat Scenario were realized. A consequence refers to “to the loss of life, damage to property or economic disruption, including disruption to transport systems that can reasonably be expected as a result of an attack on an organization in the supply chain or by the use of the supply chain as a weapon” [ISO28001]. In MEDUSA methodology first a consequence classification, based on ISO28001 is defined. Then it is defined how consequence is assessed for each business partner.

Step 5: Assess the risk for each examined Threat Sce-nario. - In this Step, the final outcome of the SC Risk Assessment is produced, mainly the expected security risk for the SCS under examination for each possible Threat Scenario. Risk values are calculated and threats are ranked according to their risk values.

Step 6: Assess the risk of cascading threats for all Threat Scenarios. - In this Step, the risk assessor will make use of all the risk parameters computed in the previous steps, in order to evaluate the effect of potential cascading threats, for each examined threat scenario. As in Step 5, in this case it will be assessed the risk of cascading dependency chains within the SCS-Graph and then ranked the Threat Scenarios according to the cascading dependency risk values. This ranking will provide input for the prioritization of the required security controls. The risk assessment of cascading threats is based on the methodology proposed in (Kotzanikolaou et al, 2013).

Step 7: Selection of appropriate security controls - In this Step, the risk assessment values are checked against a risk threshold, in order to examine the need for additional security controls by the business partners.

5. Use cases for LNG supply chain

Use cases are based on Scenarios related to securi-ty/safety contingencies that may occur in the three main parts of the considered SC: loading port, navigable fairway and unloading port. These will take into account both physical and cyber use cases. There is a broad casuistic in the materialization of threats so just 4 scenarios have been described in the study as a representation of many others. Scenarios considered are:

Scenario 1: Berth unavailability and

stop of operations due to coordinated bombing of docks, bridges and other important infrastructure at the loading port while loading a LNG tanker.

Scenario 2: LNG tanker is hijacked by pirates during its voyage producing a long delay in the supply, compromising the LNG stock at the destination in the middle of several cold waves which have increased the demand.

Scenario 3: A delay occurs during the vaporization process phase at the unloading port due to damage to critical infrastructure in vaporization/ storage terminal area.

Scenario 4: A hacker enters in the PCS in order to steal bank accounting information and other sensitive information from the importer.

Scenarios considered cover several aspects of physical and cyber security and different types of threats which mainly can cause a temporary delay or unavailability in the LNG supply.
The scenarios proposed can be studied from the per-spective of specific threat scenarios (TS) and threat scenario categories (TC) that affect to each part of the SC and which are defined in the SC Risk Assessment Methodology developed under the project MEDUSA. For the LNG transport system model, threats and threat categories considered have been (Table 2):

Liquefaction plant	TC-1: Infrastructure Threats TC-2: Information & ICT Threats TC-3: Personnel Security & Safety Threats TS4-1: Intrude and/or take con-trol of an asset TS4-3: Cargo Integrity TS4-4: Unauthorized use
Loading in LNG tankers	TC-1: Infrastructure Threats
	TC-2: Information & ICT Threats
	TC-3: Personnel Security & Safety Threats
	TC-4: Goods and Conveyance Se-curity Threats
Unloading	TC-1: Infrastructure Threats
	TC-3: Personnel Security & Safety Threats
	TC-4: Goods and Conveyance Security Threats
Regasification (vaporization)	TC-1: Infrastructure Threats
	TC-2: Information & ICT Threats
	TC-3: Personnel Security & Safety Threats
	TS4-1: Intrude and/or take control of an asset
	TS4-3: Cargo Integrity
	TS4-4: Unauthorized use

Storage	TC-1: Infrastructure Threats
	TC-2: Information & ICT Threats
	TC-3: Personnel Security & Safety Threats
	TS4-1: Intrude and/or take control of an asset
	TS4-3: Cargo Integrity
	TS4-4: Unauthorized use

Distribution	TC-1: Infrastructure Threats
	TC-2: Information & ICT Threats
	TC-3: Personnel Security & Safety Threats
	TS4-1: Intrude and/or take control of an asset
	TS4-3: Cargo Integrity
	TS4-4: Unauthorized use
	TS4-5: Goods and Conveyance misuse

Seller/ Carrier/Shipper	TS1-1: Destroy critical SC Infrastructure
	TS1-2: Unauthorized access to SC Infrastructures
	TC-3: Personnel Security & Safety Threats
	TS4-4: Unauthorized use

Exportation formalities through local agent	TS3-1: People under attack
	TC-2: Information & ICT Threats
	TC-4: Goods and Conveyance Security Threats

Bill of lading and cargo manifest to ship agent	TC-2: Information & ICT Threats TC-4: Goods and Conveyance Security Threats
Insurance contract for loading	TC-2: Information & ICT Threats
Importation formalities through local agent	TS3-1: People under attack TC-2: Information & ICT Threats TC-4: Goods and Conveyance Security Threats
Request of port services through PCS	TC-2: Information & ICT Threats TC-4: Goods and Conveyance Security Threats
Cargo Manifest to customs through PCS	TC-2: Information & ICT Threats TC-4: Goods and Conveyance Security Threats
Tax /Fees payment to authorities through PSC	TC-2: Information & ICT Threats TC-4: Goods and Conveyance Security Threats
Bill of lading to buyer/ importer	TC-2: Information & ICT Threats
Bill of lading to buyer/ importer	TC-2: Information & ICT Threats
Buyer pays seller	TC-2: Information & ICT Threats

Table 2. Threats considered in LNG transport model

However this categorization and specification of threat scenarios is still under revision an enhancement, while MEDUSA project is still in progress, in order to cover a wide set of possibilities.

6. Modeling Interdependencies

6.1 Dependency Analysis

According to the LNG supply chain model described, the interaction of the involved entities could be through physical or non-physical flows (document/ information/ transaction flows). Theses interactions can be classified into four main types of interdependencies as follows:

- Access to cyber-systems: The access could be to a database, to operational systems, networks, etc. (identifier: 1)
- Interaction with cyber-systems: The interaction could be by sharing information, the offer of common services, etc. (identifier: 2)
- Access to physical facilities: These facilities are build-ings, terminals, etc. (identifier: 3)
- Usage of physical facilities: The use could be for warehousing, offering a service, for hosting an installation, etc. (identifier: 4)

Interdependencies among key entities can be modeled in Table 3. The direction of the dependency is as fol-lows: Entities in the first row depends on the entities in the first column according to the type of dependency shown in the corresponding cell (1, 2, 3 or 4).

Where:

A = Gas trading Company/ shipper/ importer
B = Gas producer/ liquefaction plant
C = Ship agent/ owner
D = Public Administrations

E = Port Authority / port services
F = Customs Authority
G = Regasification /Distr. Company
H = Local Agent
I = Insurance Company

	A	B	C	D	E	F	G	H	I	J
A		1	1	2		2	2	2	2	2
B	1 2		2 3 4	2	2 3 4	2 3		2		
C	2	1		2 3	2	2	1 2	2	2	
D	2	1 2	2				1	2		
E		1 2 3 4	1 2 3 4	2 3 4		2 3	1	2		
F		2	2	1 2	2		2	2		
G	1 2 3 4	2	1	2	2 3 4	2 3		2		
H	2		2	2	2	2	2		2	2
I	2		2				2	2		
J	2				2		2	2		

Table 3. Dependencies between LNG SC entities

J = Banks

The next step of the methodology consists of translating these interdependencies, based on qualitative criteria into a mathematical model. For doing this, first a Supply Chain Graph is proposed, like in the example of Fig. 2: Then, the elements which will be integrat-ed n the RA Methodology are defined:

- Node $\varkappa i \in \mathbb{N}$.. It represents a business partner participating in a supply chain.
- Directed edge $\varkappa i \rightarrow \varkappa j. \in \mathcal{E}$. It represents a service provided by $\varkappa i$ to $\varkappa j$ in order to sup-port the provisioning of the supply chain services.

Each node $\varkappa i$ has a weight ωi which repre-sents the business impact of a node for the provisioning of the SC Service (High = 1, Medium = 0,5, Low = 0,25).

The type of dependency (D) showed in Table 3 is defined between business part-ners $\varkappa i$ and $\varkappa j$: $D(\varkappa i, \varkappa j)$ = 1, 2, 3 or 4 de-pending on the type of interdependency defined in section 6.1.

Finally, it is defined the Order of Depend-ency: $order(\varkappa i, \varkappa j)$: the order of a business partner $\varkappa j$, in relation to another business partner $\varkappa i$, is defined as number of steps required for $\varkappa i$, to reach $\varkappa j$, using the path of the smallest length (shortest path).

All these parameters will constitute the basis for the RA methodology which will be integrated in a computer tool for as-sessing risks of the supply chain considering cascading effects.

6.2 Use case

Taking for instance the proposed Scenario 1: "Berth unavailability and stop of operations due to coordinated bombing of docks, bridges and other important infrastructure at the loading port while loading a LNG tanker"; it would have to be analyzed first by identifying the part of the supply chain in which the threat applies and the nodes $\varkappa i$ that are involved in. In this case the threat applies in the loading port, at the beginning of the maritime sup-ply chain. Normally the loading port has the liquefaction plant so the first node can be set in the entity "gas produc-er/liquefaction plant" (entity B of Table 3): $\varkappa 0$ = Liquefaction Plant

Following the dependency in the services received or provided by the node $\varkappa 0$ the rest of nodes are identified and numbered according to the order of dependency:

$\omega 3 = 0,5$
$\omega 4 = 0,25$
$\omega 5 = 0,5$
$\omega 6 = 0,25$
$\omega j = \ldots$

than one type of dependency can be established between two nodes. Considering n different nodes and d types of dependencies, the maximum number of interdependencies possible

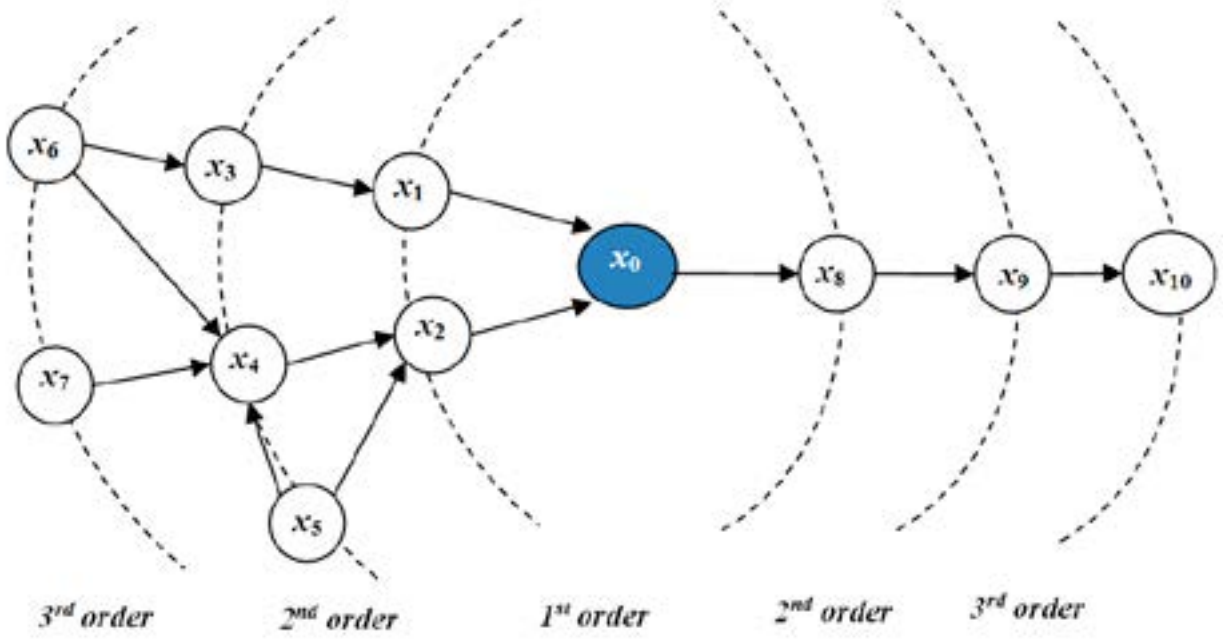


Fig 2. Example of Supply Chain Graph (MEDUSA)

$\varkappa 0$ = Liquefaction Plant
$\varkappa 1$ = Ship agent / owner
$\varkappa 2$ = Port Authority / Port services
$\varkappa 3$ = Trading company / importer
$\varkappa 4$ = Local Agent
$\varkappa 5$ = Customs
$\varkappa 6$ = Public Administrations
$\varkappa j = \ldots$

And a weight is assigned to each node:
$\omega 0 = 1$
$\omega 1 = 1$
$\omega 2 = 1$

The type of Dependency between each node is then established:
$D(\varkappa 0, \varkappa 1) = 1$
$D(\varkappa 1, \varkappa 2) = 1, 2, 3, 4$
$D(\varkappa 2, \varkappa 3) = \varnothing$
$D(\varkappa 3, \varkappa 4) = 2$
…
$D(\varkappa 1, \varkappa 0) = 2, 3, 4$
$D(\varkappa 2, \varkappa 1) = 2$
$D(\varkappa 2, \varkappa 0) = 2, 3, 4$
…
In this case there are no dependencies considered between $\varkappa 2$ (port authority) and $\varkappa 3$ (Importer) as well as more

between nodes will be $I = (n2 - n) \times d$. In the LNG supply chain model, 10 nodes are considered and 4 types of interdependencies so 400 would be the maximum number of interdependencies possible between nodes, however some nodes have no interdependencies be-tween each other or they have less than 4. In the LNG supply chain case, 87 interdependencies have been identified.
Once nodes, weights and dependencies are established, the SC RA methodology has to be applied in order to

obtain risk values for threat scenarios and also for cascading effects. Depending on the risk thresholds established and the presence of controls, the computer tool, making use of the methodology will check the risk assessment values in order to examine the need for additional security controls by the business partners.

7. Conclusions

For the moment, threat scenarios for the LNG supply chain are accurately being defined and categorized. The methodolo-gy proposed under the project MEDUSA for assessing risks in supply chains taking into account the involvement of many nodes and the presence of interdependencies using first a graphic approach seems very adequate for the purpose. Main difficulties will come from the accurate description of threat scenarios since modeling supply chains is complex due the high amount of nodes, interdependencies and different configurations (depending on geographical factors, kind of contracts and business partners involved, etc). On the other hand it is also need the validation of the model of the LNG supply chain by as many stakeholders as possi-ble in order to get the most realistic model to work with. At the end the LNG industry may count on a tool that, using effective algorithms for capturing multi-order de-pendencies between supply chain's enti-ties and other actors and also by using predictive mechanisms to assess the im-pact of security incidents, will identify the critical path of the interdependencies across the supply chain, visualize critical risk levels and probabilities and propose security controls to minimize or avoid such risks.

8. Acknowledgements

We want to thank the MEDUSA project team from the University of Piraeus Re-search Center, the Austrian Institute of Technology, Singular Logic and University of Cyprus for their very valuable contribution to the development of the methodology to assess risks in supply chains.

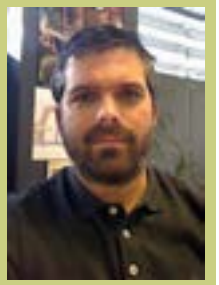
References

• Hokstad, P, Utnem I.B, Vatn, J (2012). "Risk and Interdependencies in Critical Infrastructures" Springer, p 175.

•Kotzanikolau , P, Theoharidou, M, Gritzalis, D (2011), "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Springer, pp 104-115.

David Incertis

Chemical Engineer qualified in environmental systems and Master in Occupational Risks Prevention, qualified in Industrial Safety. Ten years managing EU projects in the fields of maritime Safety and Security, Maritime Environmental Protection, Oil Pollution, Port Cyber-security, etc. Currently performing business development/capacity building proposals in the fields of maritime environment and port safety and security. Development of emergency and contingency plans for ports, design and development of training courses for the port/maritime sector.



Cyber Security within Maritime Domain

by Lt Commander N. Tiantoukas GRC (N)
and
Lt Commander D. Megas GRC (N)

The main principles of war remain unchanged as have been defined from the great theoreticians of war like Sun Tzu and Clausewitz. Both the scholars gave great importance to the protection of own forces and according to the principle "You can be sure of succeeding in your attacks if you only attack places which are undefended and you can ensure the safety of your defense if you only hold positions that cannot be attacked".

What changes though from time to time are the available capabilities tools for defense and challenge. Nowadays more than ever before the technological evolutions are so fast that change the battle environment in all domains from rapidly and constantly. The ability of forces to adapt to the use of these capabilities is crucial for the successful outcome of every operation.

Another consideration was perceived by both the great theoreticians of war and the Alliance; It is that of the importance of the information dominance. What changes the operational environment today is the digitalization of both naval units and Operational centers of all levels. On one hand we have tremendously advanced capabilities in terms of C4I, but on the other, a cyber threat could be fatal for a naval unit and for the coherence of the forces as well. Even though the vulnerability of naval forces to a cyber attack has been tackled at theoretical level, there has been some examples that prove that the threat nowadays is eminent and the tools and techniques to execute such an attack are widely available and at very low cost. Thus the possibility of a hacker with a cheap Commercial off-the-Shelf (COTS) equipments to challenge a maritime capability should be considered accordingly.

Maritime Domain could to be the new hacker's playground. The world's oceans are increasingly busy maritime highways. Almost 90 per cent of all international trade in raw material and manufactured goods travels by sea, and tankers carry more than half of the world's fuel energy sources. Maritime industry may be the oldest and the smartest in the market, but reports issued by the United States Accountability Office (GAO) and the European Network and Information Security Agency (ENISA) confirm that this very industry is extremely vulnerable to cybersecurity risks.

Cyber threats in the maritime industry are characterized by lack of security awareness or accountability while the increased use of new, sophisticated communications technologies raises the threat level at a non acceptable level. With the potential of sensitive data leaks via numerous maritime systems like ECDIS, AIS, and GPS, it is important that commonly accepted cyber security procedures are in place and operators should know how to identify a potential security threat and should be trained to respond to a cyber attack is in progress. Noteworthy incidents that prove the existence and the high impact of the threat are the following:

a. Researchers from the University of Texas in the United States demonstrated in July 2013 that it is possible to change a vessel's course by interfering its GPS, signal causing the onboard navigation systems to falsely interpret vessel's position and heading.

b. A hacker caused a floating oil-platform located off the coast of Africa to tilt to one side, thus forcing it to temporarily shut down.

c. Inspections on rigs and ships discoverd computers and control systems riddled with viruses. In one case it cost 19 days to recover a drilling rig en route from South Korea to Brazil of malware which had brought the vessel's systems to a standstill.

d. Hackers infiltrated cyber systems in Antwerp port to locate specific containers loaded with illegal drugs and remove them from the port undetected.

e. Somali pirates employed hackers to infiltrate a shipping company's cyber systems to identify vessels passing through the Gulf of Aden with valuable cargos and minimal onboard security provisions, which led to at least one hijacked vessel.

The above mentioned clearly illustrate that the cyber threat to the maritime domain is eminent and preparation failures may set the conditions for the adversaries to take over a naval unit or to hamper a naval operation. By recognizing the importance of Cyber security in the maritime Domain is not enough. Provision for effective efficient and affordable solutions should be considered. In this regard NMIOTC with the support of academia, will organize 4-5 of October 2016 a conference which aims to analyze the latest trends in cyber security threats in the maritime environment and to assist in drafting guidance on how to counter this potentially catastrophic 21st century security phenomenon.

Following that, and having gathered several stakeholders namely the Plymouth University (Maritime Cyber Threats Research Group) and NATO ACO Cyber branch an initial course on cyber security in the Maritime Security in order to strengthen the weakest link in cyber security, the human factor,will be launched later this winter. The main objectives of the course will be:

a. To provide deep knowledge of the threats and to increase of personnel awareness.

b. To make everyone accountable potential risks.

c. To identify the cyber vulnerabilities within the maritime domain.

d. To consider the consequences of exploited maritime cyber security vulnerabilities.

e. To adopt a centrally managed and coordinated training and certification approach.

f. Eliminate emotional factors i.e fear of honesty and increase the consequences of dishonesty for those that are users and administrators of IT devices.

There is no doubt that Cyber conflicts within the Maritime Environment are here for good. It is emerging challenge which dictates firm decisions and actions. Nations themselves and the Alliance collectively should master the domain and the ultimate fields of "Cyber Seas". Or as stated centuries ago by Sun Tzu "If you know the enemy and know yourself, you do not need to fear the results of hundred battles. If you know yourself but not the enemy, for every victory you may gain you will suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle".

Lt Cdr Nikolaos Tiantioukas GRC (N)
is the Head of NMIOTC's Transformation Section. He is an experience Navy Officer with long Transformation background. He poses a Masters Degree in Computer Engineering and has worked for several years as Head of IT Department.

Lt Cdr Dimitrios Megas GRC (N)
is a Staff Officer of NMIOTC's Transformation Section. He has served as Weapons Officer and Director of Weapons Department,Above Water Warfare Officer onboard Frigates and Fast Attack Crafts. He holds a Master of Science in Computer Science from Naval Post Graduate School and he is certified as Information Systems Security (INFOSEC) Professional, System Administrator,CNSS, Information Systems Security Officer (ISSO).

Understanding & Mitigating Cyber Threats in the Maritime Domain. Lessons Learned From Other Sectors.

by Robert Hayes
Senior Director, Microsoft Global Cyber Security & Data Protection Group
robert.hayes@microsoft.com

Abstract

Cyber-attacks against public and private sector organizations continue to increase at an unprecedented pace, with vulnerabilities in software & hardware being exploited by adversaries ranging from hacktivist groups, through organized crime & terrorist organizations, to nation states. The maritime sector with a high dependence on embedded systems, and complex supply chains, is particularly vulnerable to cyber-attacks, and those attacks could have particularly severe effects in a marine environment. However, emerging technologies offer real step-change opportunities for organizations to become more effective & efficient, and some organiza-tions are now managing to develop a strategic approach which balances the potential opportunities against the risks, within an agreed organizational risk model. This paper will describe how organizations can develop an effective strategic approach to cyber-security, and discuss how examples of global best practice from other industry sectors can help the maritime sector.

Keywords

Cyber-attack; cyber-security; risk; strategy; emerging-technology.

1. Introduction

Organizations in many sectors are seeking to exploit emerging technologies such as cloud hosted services and the internet of things to transform

the way they do business, and interact with customers and stakeholders.
However, few organizations have adequately considered how they balance the potential benefits of these new technologies with the potential security risks that they can also present if not managed and integrated.
These risks are potentially severe in a maritime environment, yet much of the risk mitigation is similar to that employed in other domains.
This paper will discuss the business change processes that are necessary to safely embrace these new technologies; describe the characteristics of organizations which have managed this change; and present some priority actions which will help organizations to protect, detect and respond to cyber-attack.

2. Leveraging emerging technologies

Emerging technologies offer organizations significant potential effectiveness gains, enhanced resilience, & efficiency savings.
The ability to link together data from a multitude of sensors, and to undertake intuitive big-data analytics on this dataset, in combination with open source & existing organizational data, enables organizations to gain new insights into their operational environment, and enhance dynamic decision making.
In addition, being able to deliver real-time user-driven context specific processed data to diverse user devices, provides field based users with the ability to make rapid decisions without having to wait for the data they require to be processed and delivered from elsewhere in their organization.
The ability to present this contextually rich data through off the shelf augmented reality devices provides the ability for a user to visualize complex data whilst dealing with a real-world problem.
This data can then be shared securely with partners and end users.
In business the maritime domain is no different to other domains – organizations that are able to innovate and safely leverage emerging technologies will survive; organizations that do not will wither and die. The key word here is “safely”.

3. Cyber context

It is difficult to find a daily news bulletin without some reference to a successful cyber-attack against an individual, enterprise or government. The scale, scope, complexity, and sophistication of cyber-attacks contin-ues to increase with new attack vectors being uncovered on an almost daily basis.
Worryingly, many organizations are realizing too late that their infrastructure was not designed with an appropriate level of cyber-security, and that it is far more diffi-cult to retrospectively engineer security into an organizations infrastructure than to design it in from the start.
Most large scale attacks succeed because organizations continue to rely on perimeter security to keep attackers out, and when this fails, for example from an insider attack, there is often little to stop an attacker moving laterally across organizational systems, compromising each in turn, until the whole enterprise has been compromised.
Whilst traditional hackers often made very visible changes to websites, attackers seeking to steal data will try to avoid discovery, so accumulated data losses can be acute. In Microsoft’s experience, the average time an attacker will be present and active in an organizations infrastructure before detection is over 200 days.
The initial attack vector mostly relies on some type of user interaction; clicking a link in a phishing email; opening an email attachment; or inserting a device or media into a computer or piece of machinery. Despite increased awareness these attacks still succeed, and are becoming more sophisticated, for example by vectoring the initial point of attack at an individual in a second organization which is part of the primary organizations supply chain, and having connectivity into the primary organizations systems.
Supply chain integrity is also important, as organizations have discovered both software and hardware to have been corrupted with malware on delivery, or after remote upgrading. This is a particular issue in the maritime sector.

4. Costing cyber-attacks

There have been a number of studies aiming to produce definitive costs of a successful cyber-attack. These studies have produced significantly differing results, but recent data from Aon Corporation who are a leading global provider of risk management, insurance and reinsurance brokerage is illustrative. It asserts that 5% of business-related privacy and security breaches result in more than $20 million in direct costs and damages. Those costs include legal expenses and legal settlements, business interruption costs, investigating and remediating problems, as well as possibly paying for crisis communications and other specialized services.
In addition, too few organizations ad-

equately consider the reputational damage of a successful cyber-attack, or the consequent loss of business. A recent KPMG survey revealed that 79% of the 133 institutional investors surveyed would be discouraged from financially backing a business that has been subjected to a cyber-attack.

5 The maritime context

The maritime sector is particularly vulnerable to cyber-attack, and the consequences of a successful cyber-attack in the maritime domain would be especially acute. A number of factors contribute to this situation.

The maritime sector relies on complex embedded systems, often running mission critical safety equipment. Many of these systems were designed with limited security on the assumption that they would never be connected to networks or other machines, and so could not be compromised. Instances such as the Stuxnet attack on Iranian nuclear processing centrifuges have shown that these assumptions were flawed, and that embedded systems can be compromised and manipulated, often without any warning signs.

The maritime sector relies on a complex hardware & software supply chain, and because of the difficulty in providing physical first line support, many of the core mission critical systems are supported and patched remotely, often by third party organizations. Understanding and mapping the dependencies and risks resulting from this situation is something few organizations have done, let alone produce a plan to mitigate the identified risks.

Finally, managing the cyber-security of a complex envi-ronment requires a combination of skilled personnel on site, and at system architecture level, working together as one team. This is obviously difficult to achieve in a maritime environment.

6. If an attack succeeds, who will judge your organization & what will you be judged on

Should an attack succeed your organization will be judged by regulators, markets, customers & the media on the following criteria:

- How long it took to detect a breach
- The level of access to systems obtained by the attacker
- The quality of control, monitoring & cyber hygiene measures in place & supported by policy
- The effectiveness of the response plan
- The time taken to resume key services
- The effectiveness & speed of the post breach communication

Having a template in place covering these points that can be populated when needed is a simple but effective tactic, but one that few organizations have adopted.

7. Lessons learned, adopting a strategic approach to cyber-security

The maritime sector is not alone in wrestling with the issue of how to safely exploit emerging technologies whilst focusing on cyber-attacks. Other sectors, which featured earlier on the attackers' radar, have been deal-ing with this issue for several years and have experience & learning that can be leveraged and exploited.

Many governments run confidential information ex-change forums which are designed to facilitate exactly this type of communication, and feedback from organizations who participate is extremely positive. A recurring problem is that organizations only think about joining this type of forum after, not before, they have been attacked!

This situation is compounded by the fact that few organizations have an executive team or Board which possesses skills in the cyber-security area, so the issue is often delegated to the IT department to deal with. This approach misses the fundamental point that achieving a strategic approach to cyber-security, whatever the domain, is a balance between business imperatives, cost, and security. This balance cannot be successfully achieved without senior perspectives from the operations, finance, and infrastructure components of the organization. No matter how good an IT department is, they will not be able to reflect these three perspectives.

A growing number of organizations are recruiting non-executive directors with cyber skills to augment and enhance corporate decision making, and to help ask the right questions of the organizational internal stakeholders such as the IT department. This can also help to ensure that organizational policies are coherent with the cyber-security strategy; for example having an established policy covering when an organization can remotely access an employee's computer or device makes life much easier when an insider threat is detected.

Experience has clearly shown that organizations which regularly review cyber-threat & response planning at Board level are subject to fewer successful attacks, and respond more effectively when attacked.

8. Characteristics of successful organizations

From Microsoft's experience, there are a number of common characteristics which differentiate organizations that are most effective in preventing & responding to cyber-attack:

• A culture of "Assume Breach". This simply means that the base assumption is that there has been a successful attack, but it has yet to be discovered. All systems and plans are measured and tested against this principle.

To achieve this state organizations require dynamic & comprehensive situational awareness. This is a combination of entity (users, devices, and resources) behavior analysis (usually referred as User Behavior Analytics) and real-time detection of the attacker's Tactics, Techniques and Procedures.

This information will drive an assessment process which will have cognizance of normal patterns of behavior, and identify outlier behavior which needs further investigation.

This assessment process will feed into operational decision making & ultimately inform strategy.

• The organization understands and has documented its risk tolerance against key business imperatives. In simple terms this means that the organization has identified its high value assets where minimal risk is acceptable, and other assets or services where greater risk tolerance exists, it is these areas where innovation can achieve the most.

• The organization has at least attempted to map & understand its supply chain & has plans to mitigate any associated risks & dependencies. The definition of supply chain here is broader than most organizations consider in the cyber context. It will include attacks on power or utilities which could disrupt operations, as well as mitigating the risk of compromised hardware and software.

It will also need to consider the risk of attacks vec-tored through third parties, and ask questions about those third parties own cyber security. The Aon study identified that only one in three organisations vendor supply chain contracts contain any security provision.

• The organization has a coherent & rehearsed dynamic response plan for a range of cyber related scenarios. These will include attacks aiming to steal data, disrupt operations, or cause reputational damage.

• Cyber-security is treated as a cross-organizational priority and is enshrined in policy, training, and process.

• Cyber-security is owned & reviewed at Board level

9. Cyber-security as a business enabler to win market share

A number of organizations in different sectors are now looking at cyber-security as a business enabler & discriminator.

It is clear that an increasing number of governments and enterprises will only consider organizations as part of their supply chain if the organization can provide evidence of positive cyber security.

There is also a realization that consumers are becoming less tolerant of organizations which fail to prevent successful attacks (particularly if their basic cyber hygiene is poor) and will move to a competitor seen as being safer.

A growing number of organizations are now actively marketing that their security is sector leading, or in some cases directly better than a named competitor.

10. Cyber economics

The laws of economics apply to cyber-attacks and many organizations, including Microsoft now actively seek to increase the costs of attackers, to the point where they will seek another target.

This can be described in the following formula where:

(G) Gains per use
(T) Opportunities to use
(CV) Cost to acquire a vulnerability
(CW) Cost to weaponize

Attacker ROI = (G x T) – (CV + CW)

Organizations can materially affect the "opportunities to use", and "gains per use" aspects of the formula by undertaking the priority actions detailed in the following section.

There are also roles for governments and industry in working to increase the costs of vulnerability acquisition and costs of developing weaponized vulnerabilities.

11. Priority actions

The United States Computer Emergency Readiness Team recently asserted that as many as 85 percent of targeted attacks are preventable.

In Microsoft's experience there are a number of simple & inexpensive priority actions which organizations can take to significantly reduce their vulnerability profile:

• Reduce the number of accounts with privileged or administrator access to the absolute minimum,

re-quire different administrator credentials for each system, and use multi-factor authentication for all administrator accounts.

- Patch all systems promptly, and keep software as close as possible to the currently released version.
- Use application whitelisting to control which applications can be run on the organizations network.
- Control access to the organizations network by devices & use gateway checks to ensure that devices connecting are healthy and from an author-ized user.
- Regularly audit & analyze log files to look for outlier behavior.

In addition, there are priority actions which will enable an organization to quickly & effectively respond to a successful attack:

- Using corporate email with an attacker in your network could alert them to the discovery of their at-tack, and prompt a change in their behavior from data theft to data destruction to cover their tracks with severe consequences for the organization concerned.

Organizations should have a secondary communi-cation system in place which can be used during an attack. Companies such as Microsoft can provide a cloud based system which can rapidly be provisioned to provide voice and data services away from the corporate network.

- Map and understand your supply chain and key vendors with 24/7 contact details. The time to worry about who hosts a corporate web-site is not when that site is under attack.
- Understand who will support your organization through the tactical & strategic phases (they are very different) of recovering from an attack, and have those relationships, and any necessary con-tractual agreements, in place.

12. Conclusion - Bringing this back to the maritime sector

The consequences of a successful cyber-attack on a maritime target could be severe due to unique challenges of the sector.

Organizations operating in the maritime sector should therefore be treating the issue as a higher priority than other sectors, and have in place mature and robust plans for preventing, detecting, and responding to cyber-attack.

With up to 85 percent of targeted attacks being preventable, organizations in the maritime sector which fail to take the well documented steps to mitigate the risk of attack, or fail to plan for responding to a successful attack, can expect to find themselves harshly judged.

Robert Hayes

is Senior Director, Strategy & Partnerships in Microsoft's Enterprise Cybersecurity Group and leads Microsoft's global team of Chief Cybersecurity Officers.
Among others he served in British Intelligence as Head of the UK National Technical Assistance Centre and advises the UK Ministry of Defence on cyber security matters and holds the rank of Major (V) in the Engineer and Logistics Staff Corps of the British Army Royal Engineers.
Robert holds a B.Sc. in Psychology, is a Fellow of the British Computer Society and a Freeman of The City of London.

Energy-saving Measures for Naval Operations

by LtCdr *G. Gougoulidis, PhD*
Hellenic Navy
gougougr@mit.edu

Abstract

2013 was a landmark year for the shipping industry since the implementation of a series of new IMO measures, such as EEDI, SEEMP, etc., took place. These measures were implemented in the light of an environmentally responsible international shipping policy and refer to most types of merchant ships. Along with the environmental benefits, cost reduction is a collateral benefit in most cases.

On the other hand, there are navies, such as the US Navy, that have long been researching ways to increase energy efficiency. Although naval ships are not directly affected by the 2013 regulations, they have strong reasons to be concerned with energy efficiency. An important reason is energy security, which is related to the operational availability during crisis periods. In this context, advanced navies have been studying various methods to reduce energy consumption for decades.

The recent economic crisis and the new environmental regulations led to the emergence of several systems and products assisting in moving towards this direction. In this paper, the feasibility and application of various operational and technical measures for naval vessels are examined. Examples of certain navies are presented, predominantly from the US Navy, which has extensive experience in the field of energy efficiency, as well as the Royal Navy, and finally, the Hellenic Navy. These navies have been working on programs such as the Great Green

Fleet, or the Green Ship Challenge, which will be briefly described.

Keywords

Energy security; energy efficiency; optimization; hydro-dynamics; alternative fuels.

1. The Energy Security – Energy Efficiency Connection

The issue of energy security is a term more pertinent to navies than shipping companies. The term energy security is not limited to the actual defense of the energy sources, such as the oil storage facilities, but rather expands to securing that the naval fleet will be able to operate in times of crisis (both economic and geopolitical), as well as maintain a high degree of readiness. This means that a naval fleet should seek energy independence in order to decrease its exposure and vulnerability to foreign fuel availability, price volatility, or legislative issues.

For navies, things are more complicated than for ship-ping companies since the former case involves a national, public organization, while the latter case a private company. Hence, while for a shipping company it is easy to ensure that its ships will continue to operate even during a crisis period, provided that it has the financial resources to buy fuel, for a navy, financial resources are not the only affecting parameter since the procurement of fuel may be hindered by international embargos or other alliances.

In this sense, the degree of fuel storage capacity and availability defines the extent of a navy's operational capabilities. However, these capabilities can be en-hanced by another parameter which was to a large extent disregarded until recently: energy efficiency. Using less energy, or burning less fuel, directly increases the endurance of a vessel and, hence, the combat time available. Recently, it has become apparent that the issue of energy efficiency is of ultimate importance not just for the protection of the environment and the reduction of operating expenses, but also for enhancing the energy security levels of a navy. It is obvious that an energy efficiency policy will not ensure energy independence, but it will offer flexibility in strategic planning by decreasing foreign dependency.

2. The Energy Efficiency Challenge

Apart from this energy security issue, another significant difference between navies and shipping companies is the types of ships they operate. The majority of shipping companies operate specific types of ships (i.e., bulk carriers, containerships, etc.) However, this is not the case when it comes to navies. A naval fleet is quite a diversified group of vessels that includes all different kinds of ships. From fast combatants, like frigates, to slow ships, like mine hunters; from large ships, such as aircraft carriers, to small ships, like tug boats. Thus, as is evident, there is a high degree of non-homogeneity, making the adoption of a common energy efficiency policy a complex case.

At the same time, there is a plethora of energy efficiency methods that can be adopted. Each method has certain advantages and disadvantages. The decision on the method to be adopted is a function of several parame-ters, among which are the type and size of the ship, the route, and the operational profile. As a result, there are certain restrictions limiting the number of available, worthy solutions. However, there is a number of universal solutions that can be easily applied to various types of ships, as will be subsequently discussed.

To make things easier, IMO proposes guidance on best practices for fuel efficiency (IMO, 2012), measures that include both operational and technical solutions. More specifically, IMO proposes the following measures: improved voyage planning, weather routing, just in time, speed optimization, optimized shaft power, optimum trim, optimum ballast, optimum propeller and propeller inflow considerations, optimum use of rudder and heading control systems (autopilots), hull maintenance, propulsion system, propulsion system maintenance, waste heat recovery, improved fleet management, improved cargo handling, energy management, and fuel type. Although these measures are not binding, they can be a good starting point for analysis. In the following paragraphs, the available energy-saving solutions for navies based on an operational-technical categorization will be analyzed. Before proceeding with the analysis, a brief description of major energy efficiency naval programs will be presented.

3. Naval Energy Efficiency Programs

Navies, such as the US Navy and the Royal Navy, have certain programs that experiment with a variety of meth-ods and systems, both technical and operational. Bailey and Hardy (2014) describe the Green Ship Challenge, a program implemented by the Royal Navy in order to attain the goal of reducing, by 2020, fossil fuel consumption by 18%, compared to a 2010 baseline. The measures considered in order to achieve this goal

are divided into three main categories: technology, alternatives to fossil fuels, and behavioral measures. Potential technological measures analyzed are hydrodynamic (bulbous bow above sonar, optimized shaft brackets, vaned propeller boss, new propellers, twisted rudders) and platform systems improvements (waste heat recovery, heat pumps and HVAC improvement, prime mover efficiency and Type 23 Power Generation and Machinery Control and Surveillance System Update).

In the same framework, the US Navy announced in 2009 five energy goals, one of which was to demonstrate and then deploy a Great Green Fleet. This fleet will use alternative sources of energy, including nuclear power, and will utilize a series of energy-saving measures. The first demonstration of the Great Green Fleet took place in 2012, during the Pacific (RIMPAC) exercise, while deployment is scheduled for 2016. Except for the alternative fuels used during the demonstration, other energy-efficiency technologies that were tested according to the Great Green Fleet Fact Sheet (n.d.) included: solid state lighting, gas turbine on-line water wash, shipboard energy dashboard, smart voyage planning decision aid, and stern flaps.

Other than the Great Green Fleet project, the US Navy has been working on a number of different technologies and methods to increase the energy efficiency of its non-nuclear ships. According to Doerry, McCoy, and Martin (2010) these efforts are summarized in the following groups: improved prime mover efficiency (gas turbines, combustion trim loop for conventional steam ships, hybrid electric drive), reduced propulsion power demand (stern flaps, bulbous bows, hull and propeller coatings, propeller redesign, improved directional stability), reduced mission systems and ship systems power demand (advanced solid state lighting, improved HVAC efficiency), and modifying concept of operation (smart voyage planning, iENCON program).

4. Operational Measures

There is a variety of operational measures available, many of which are related to the planning of the voyage. Weather routing, speed optimization, just-in-time, and turnaround time in port are all parts of a well-designed voyage which is optimized, either for time, fuel consumption, or cost. All these measures can be easily applied to merchant vessels, which have to call certain ports on specified dates and times; however, this is not exactly the case for naval combatants. Their missions are not scheduled itineraries, and their speed can vary significantly, in opposition with merchant ships, which travel at roughly constant speeds.

However, for routine voyages, or when transiting during peace, voyage planning is a tool that can be used to increase efficiency. It is a low-risk solution that does not require expensive equipment and the main task is done by software that receives data from the installed ship systems or other navigational aids. Navies have an additional advantage since they can make use of their own Meteorology or Oceanography Commands and equipment to collect information, such as satellites, meteorological stations, etc.

Optimized trim is another measure that can be applied to every kind of vessel and there is a variety of software in the market for this purpose. However, naval combatants do not have large disposable loads, and they do not spend time in a ballast condition as do merchant ships. For this reason, the trim margins can be minimal and the savings through such a method insignificant. The exception to this rule can be certain types of auxiliary ships, such as oilers or landing ships, on which the loading condition can vary significantly.

A more profitable method is what is called cold ironing. Cold ironing refers to the provision of shore side electrical power to a ship at berth while its auxiliary engines are shut down. Although this is not standard for merchant vessels, for naval ships this is a typical practice when on base. Except for electric power, other facilities, such air conditioning, can be provided to the ships, reducing fuel costs as well as maintenance costs due to the reduced hours of operating the engines and machinery.

Another energy-saving method that can be applied mainly when the ships are on base is the hull and pro-peller maintenance. By maintenance, preserving a smooth surface condition is meant. Hull and propeller roughness due to fouling is a major cause of increased fuel consumption and thus, energy. Naval combatants, although capable of speeds exceeding 30 kt, spend most of their time at cruise speeds below 15 kt. These speeds correspond to low Froude numbers where the primary part of resistance comes from friction.

Thus, the monitoring and control of fouling can yield significant savings without any significant investment. Schultza et al (2011) present the results of a US Navy study which examined 320 DDG-51 inspection reports from 1/1/2004 to 31/12/2006. The calculated resistance penalty due to hull fouling amounted to US $56 million per year, and about US $1 billion over 15 years.

Navies are well aware of the importance of the fouling issue and have taken certain measures to monitor and correct the problem. Such an example is the Royal Navy's Optimizing Fleet Fuel Usage (OFFU) program. For the purpose of the program, torque meters have been installed on a large number of RN ships. The measured power is compared to baseline measurements that have been taken after drydocking, refit, or any other hull paint renewal occasion. According to Walker and Atkins (2007), the decision factor of whether to clean a hull or not, is the time to recoup the cost of the cleaning. If this is within three months, then it is considered as profitable. The shaft power that meets this criterion is called the "trigger value."

A lower threshold of an 18% increase in shaft power at 13 kt is used, which coincides with the formation of hard fouling. Similarly, the upper limit is set at a 30% in-crease in shaft power at 13 kt, when mature shell growth has developed. Measurements of shaft power are taken each month and the results are compared to the annually published trigger values. When the measurements at 13 kt exceed the trigger value, two further measurements at 8 and 18 kt are taken. The results are analyzed, and a hull clean is considered, depending on operational planning (Walker and Atkins, 2007).

The Hellenic Navy recently revised its underwater ship husbandry policy that relates to the inspection and maintenance of hull coatings. Systematic underwater hull and propeller inspection is performed by the diving crews of the ships and the naval bases, while underwa-ter cleaning is performed by the diving crews of the naval bases, as well as private providers.

No matter how the monitoring of the hull and propeller condition is performed, it is essential to clean both at regular intervals, even when the ship is in service, in order to ensure their smoothness. In the case that there are time, resource, or operational restrictions, partial cleaning should be performed in the following order according to Hydrex (2012): propellers, forward one-third of the hull, and after two-thirds of the hull. Furthermore, buffing is preferred to propeller polishing, following the philosophy "little and often" (Hydrex, 2012). The additional benefit in the case of buffing is that no material removal pollutes the sea.

Except for the maintenance of the exterior of the ship (hull and propeller), the maintenance of the internal machinery, such as the engines, can have a great im-pact on the operational costs of the vessel. Condition-based maintenance is a method which is used lately in combination with manufacturer's guidelines and can yield significant savings if applied correctly. It is a maintenance which is performed based on information received by the

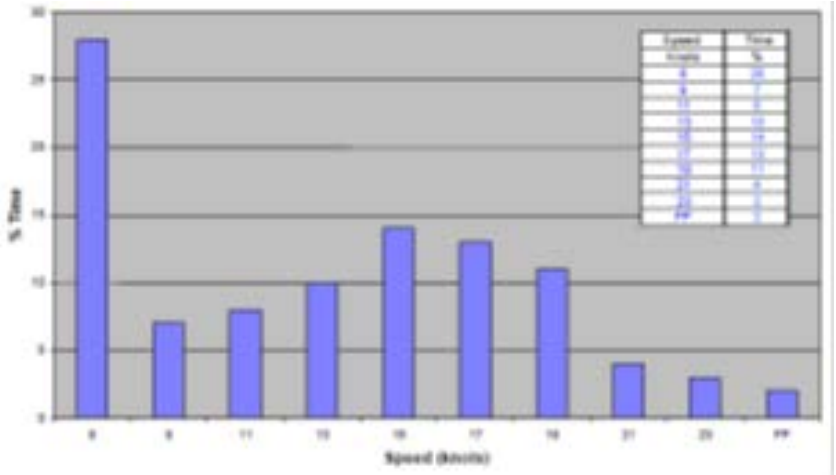


Fig. 1: Speed profile for the DDG-51 class of the US Navy [DDS 200-2]

EFFECT OF FOULING ON MARINE HULLS

Type of Ship	Standard Displacement (tons)	Loss of Maximum Speed (knots)	Percentage increase in Fuel Consumption to maintain a speed of: 10 knots	20 knots
Battleship	35000	1.5	45	40
Aircraft Carrier	23000	1.5	45	40
Cruiser	10000	1.5	50	45
Destroyer	1850	2	50	35

Fig. 2: Effect of fouling after 6 months after docking in temperate waters [Hydrex (2010)]

Fig. 3: Hard fouling on an S-type frigate of the Hellenic Navy

equipment and on evaluation of this information by experts. As long as a reliable monitoring system is used, then maintenance decisions can be based on it.

Finally, a parameter which is usually underestimated is the actions and habits of those who actually operate the systems. The behavior of the crew is a factor which is often disregarded but can have a great impact particularly for naval ships, which have significantly larger crews compared to typical merchant ships. Training personnel and nourishing a culture towards energy-saving attitudes and behavior will have an immediate effect on the reduction of energy-spending. In the beginning of this process, special incentives or bonuses can be given based on fuel savings. Simple practices, such as shutting down the air-conditioning plant when the weather is favorable and using only the blowers, or simply switching off lights in areas, such as cabins, recreation rooms, mess rooms, etc., when not required can yield unexpected savings.

A relevant example is the US Navy's iENCON (Incentivized Energy Conservation) program. The iENCON program provides rewards to the units that outperformed the class average, even in the form of cash. Moreover, the program provides training to ship crews on a regular basis and gives guidelines on ship energy conservation. To understand the significance of the program, according to the Great Green Fleet Fact Sheet (n.d.), 1.1 million barrels of fuel were saved, representing a cost reduction of over 11% during the year 2011 alone.

5. Technical Measures

5.1 Hydrodynamics

5.1.1 Bulbous bow

The effect of the bulbous bow in the reduction of the wave-making resistance is well-studied and recognized. Bulbous bows have been used for decades and are standard on the majority of commercial vessels. They are designed to provide a reduction in resistance within a specific speed range, out of which they may have adverse effects.

Naval combatants are ships of high speeds for which the wave-making resistance component is significant. However, many of the designs of the recent past did not incorporate a bulb in the bow area. This trend seems to have been reversed, as most of the new designs incor-porate a bulb at their bows. A relevant example of crafts belonging to the same family of vessels are the MEKO class frigates by Blohm+Voss. The Hellenic Navy acquired in the 90's four MEKO 200 HN frigates that do not have a bulb at the bow. On the other hand, the newer member of the family (00's), the MEKO A-200 of the South African, or Algerian Navy incorporate a bulbous bow. The two designs differ slightly in dimensions and displacement, while the top speed of the newer class is 29 kt instead of 32 kt.

Another design complication that is not found in commercial vessels is the need for sonar. This comprises a design challenge for naval combatants. During the 90's, the US Navy conducted research on a bulbous bow redesign for the DDG-51 class of ships. The goal was to integrate the sonar dome into the bulb. The study yielded a 4% fuel reduction, a 4% increase in range, and a 0.2 kt increase in maximum speed. O'Rourke (2006) refers to a 2000 DoD statement that fitting bulbous bows onto 50 DDG-51s could save $200 million in life-cycle fuel costs. A similar

study conducted by the Royal Navy about fitting a bulbous bow above the sonar calculated savings in the order of 5% (Bailey and Hardy, 2014).

5.1.2 Stern Flaps And Wedges

On the aft body part of the ship, one of the most com-mon practices to improve efficiency is the use of stern flaps. Stern flaps increase the pressure at the aft part of the hull by slowing down the flow and additionally, creating a vertical lift force. As a result, form resistance is reduced due to the reduced aft-body suction force. Salas, Rosas and Luco (2004) concluded that stern flaps could offer a 5-12% powering resistance reduction. When combined with a bow bulb, a 15% increase in fuel efficiency can be achieved for certain ship types.

Probably the most extensive study on stern flaps has been done by the US Navy. Stern flaps have been in use since 1989 and have been installed in more than 170 ships. A stern flap installed on USS Copeland frigate in 1989 realized a 5.4% fuel reduction and a speed increase of 0.3 kt. The most typical example presented by Cusanelli and Karafiath (2012) is the DDG-51 class of ships of the US Navy. According to a 2006 DoD report, the class achieved a savings of 7.5%

The use of stern flaps on various US Navy ships has been calculated to have cumulated a fuel savings of $665 million between the years of 1989 and 2011. According to Cullom (2010), stern flaps have an average payback period of less than a year when installed on FFGs, CGs and DDGs. Stern flaps have also been used successfully by other navies such as the Royal Navy (Type 23 Frigates & Type 42 Destroyers), the Royal Canadian Navy, and the Chinese Navy, among others.

to reduce resistance. According to Bojovic, Sahoo, and Salas (2004), when wedges are combined with spray rails, they are the most effective devices for drag reduc-tion of semi-displacement round bilge hulls.

Not long after the US Navy, the Hellenic Navy conducted a series of experiments and decided to install wedges on a series of semi-displacement patrol boats in 1996. The positive results encountered of using these crafts led the Navy to apply the same solution to another series of FPBMs (Fast Patrol Boat Missile), while the newest class of the Super Vita FPBMs incorporates a 5 deg wedge-type shape of the aft part of the hull in the initial design.

In the first case, the installation of the wedge resulted in a 10% reduction of the required Effective Horse Power (EHP). Alternatively, the maximum speed was in-creased by 8.6%. In the second case, a combination of a stern wedge and bow spray rails were installed, yield-ing a 9.8% reduction of the EHP at a speed of 32 kt.

A not so popular method applied to the aft-body is the use of a Stern End Bulb (SEB), a method studied mainly by the US Navy. The working principle is exactly the same as the bulbous bow, based on the interaction of the two wave systems. Cusanelli and Karafiath (2012) discuss the US Navy's experiments with two different classes of ships: the T-AKE and the DDG-51. The results of the model and CFD tests showed a 4.5% reduction at 20 kt for T-AKE. DDG-51 was fitted with a combination of a SEB and stern flaps. The study showed that the savings in fuel consumption could yield a cost reduction of $130,000 per ship annually.

5.1.3 Other Hydrodynamic Enhancing Devices

Contracted & Loaded Tip (CLT) propellers are propellers fitted with endplates on the tip of the blades,

Fig. 4: Stern flap installed on a DDG-51

at the pressure side. The endplates eliminate the communication between the two sides of the blade, resulting in a significant restriction of tip vortices formation. Gennaro (2012) states that 5-8% efficiency improvement can be achieved while reducing noise, cavitation, and pressure pulses at the stern. The Spanish Navy has used CLTPs successfully. BAM Class Corvettes are fitted with 4-blade twin controllable pitch CLTPs with a diameter of 3.45m.

Another energy-saving device is the Propeller Boss-Cap Fins (PBCF), a device that looks like a small propeller installed on the hub cap of the original ship propeller. The system is able to recapture an amount of the rotational and hub vortex losses, thus reducing the resistance. Additional benefits include the reduction of noise and vibration. Such a system is installed on the newer class of submarines of the Hellenic Navy under the name HDW Dr. Schulze.

Fig. 5: A stern wedge retrofit on a Hellenic Navy FPBM

Fig. 6: The Rolls Royce Promas system

Finally, another way to minimize the losses behind the propeller hub is the integration of the rudder with the hub cap. In this context, Rolls Royce developed the Rolls Royce Promas system while Wärtsilä has developed a similar system under the name Energopac. As many other ideas which were conceived long ago, a Promas-like system can be found on a 1943-built tug boat owned by the Hellenic Navy, which is depicted in Fig. 7.

Except for the systems described earlier, the U.S. Navy has studied a number of different hydrodynamic improvements for its DDG-51 class destroyers, including a larger propeller, contra rotating propellers, propeller pitch monitoring and improvement, twisted rudders, and shaft strut alignment. According to Cusanelli and Karafiath (2012), a relatively moderate estimation of fuel cost savings would be $300K per ship, or a 3% savings, representing a total ownership-cost savings of $735 million, assuming a fleet of 70 DDG-51s with a service life of 35 years.

5.2 Coatings

The influence of the fouling of the hull and propeller to the performance of a vessel was previously analyzed whereas the coatings used to prevent fouling were not. Naval vessels do not differ and use the same antifouling systems as their commercial counterparts. The basic antifouling coatings are biocidal substances, which fall into three main categories: Control Depletion Polymers (CDP), with an effective lifetime of 3 years; Self-Polishing Copolymers (SPC), with an effective lifetime of 5 years; and Hybrids, with an in-between performance.

Fig. 7: The predecessor of Promas on a 1943-built tugboat

However, in the last decade, various navies started to experiment with advanced antifouling coatings. By the term advanced, we are referring mainly to coatings that fall into the Foul Release (FR) category. These are coatings that do not use biocides, but instead, they take advantage of their non-stick surface, where fouling organisms detach easily when the ship reaches a certain speed.

In 2014, the Royal Navy completed the application of Foul Release coatings on all its ships under the Optimizing Fleet Fuel Usage program. The FR coating program took over 10 years to complete and it has just recently started to deliver full benefits according to Bailey and Hardy (2014). However, performance data received for the years 2012 and 2013 indicates that up to 50% of the ships in service still operate at less than optimum efficiency.

Similarly, the US Navy applied FR coatings on USS Port Royal (CG 73) and USS Cole (DDG 67) back in 2009, in an effort to assess their performance. In order to do this, the Navy installed Ship Power Condition Monitoring Systems (SPCM) on the aforementioned ships, as well as on two sister ships coated with traditional antifouling paints (Doerry, McCoy and Martin, 2010).

Although the Hellenic Navy uses biocidal coatings for the protection of its fleet, it has experimented in the past with FR coatings. Silicon-based FR coatings were applied on two fast patrol missile boats. Although the project proved to be successful as the FR coating provided satisfactory antifouling performance for a period of 12 years, no further actions were undertaken in terms of adopting an FR coating policy, nor was any further testing of alternative advanced antifouling technologies performed.

FR coatings work better beyond a certain speed and for this reason, the high-speed naval combatants are those which can benefit the most. Although FR coatings have started becoming popular among naval vessels, a widespread adoption of them has not yet occurred. The main reason for this is probably the higher cost compared to conventional antifouling coatings. According to Doerry, McCoy, and Martin (2010), the cost of the paint itself is 2.7 times higher than the traditional copper ablative coating while labor costs are 12% higher for cruisers and 15% for destroyers.

5.3 Machinery

There is a large number of mechanical and electromechanical systems onboard a ship that can be improved to increase efficiency. However, most of the times, the main focus goes to the engines of the vessel. There are several options, but not all of them apply to naval vessels. The majority of the engines used on commercial ships are two-stroke, slow-speed diesel engines. On the contrary, a large number of naval ships is equipped with medium-, or high-speed four-stroke diesel engines, as well as gas turbines. As such, some of the technologies (i.e. super long stroke engines, derating, cylinder cut outs) are not suitable for engines of naval ships. On the other hand, there are measures that can be equally used by both commercial and naval vessels. Such examples are the electronic injection of the engine, the tuning for a specific range of load, or the use of common rail systems.

Although the aforementioned systems can yield significant savings in some cases, the main portion of the energy lost onboard a ship goes into the cooling systems and the exhaust system. Thus, waste heat recovery is a significant method for saving energy. The ex-haust heat that would be otherwise lost, can be used to power an exhaust gas turbine and/or to generate additional steam to power a steam turbine. The combination of both an exhaust gas turbine and a steam turbine yields the maximum savings. A typical example is the Type 45 destroyers of the Royal Navy, which use the Rolls-Royce WR-21 gas turbine with an intercooler and recuperator. Additionally, the Royal Navy is conducting a study on the Organic Rankine Cycle (ORC) for the types of diesel generators and gas turbines found on warships (Bailey and Hardy, 2014).

Concerning gas turbines, the US Navy is exploring a variety of improvements to increase efficiency (Doerry, McCoy, and Martin, 2010). These improvements include replacing analog with digital fuel controls, and modifying exhaust ducting to reduce back pressure, among others. However, the most important of all is the automated online water wash. This process allows for the compressor to be washed while the engine runs. As a result, there is no impact on the operations of the craft while at the same time, maintenance is reduced, improving the vessel's

Fig. 8: FR coatings on a Hellenic Navy fast patrol boat after 12 years

overall efficiency.

An entirely different approach to reduce energy con-sumption in propulsion systems is the use of a Hybrid Electric Drive (HED) arrangement. The term hybrid electric involves the use of electric drive for low speeds, while mechanical drive is used at high speeds. In the electric drive mode, the diesel or gas turbine generators provide power for the ship's electrical load and the propulsion motors simultaneously. In order to accomplish this, an electric motor is connected to the main reduction gearbox along with the main engine. When the mechanical system is used at high speeds, the motor operates as an alternator. Consequently, main engines can be shut down, resulting in fewer running hours and fuel savings.

In this context, the US Navy is planning the modification of the propulsion train of 36 DDG-51 Flight IIA destroyers. The ships are driven by four GE LM2500-30 gas turbine engines while electricity is produced by three Rolls-Royce AG9140 gas turbine generator sets. Under normal operations, two of the sets are used although less than half of the power produced is actually needed to cover the electrical loads required (Reynolds, 2013). This extra energy will be used by the HED system and provide power to the propeller shaft. One such system is used on the port shaft while the starboard shaft is used in trailing mode at low speeds (Warship Technology, 2014). In this way, as ships operate primarily at low speeds, all four GE LM2500-30 gas turbines can be shut down.

The USS Truxtun was the first DDG-51 ship to be fitted with this system serving as a test platform. The first operational ship with the new drive system is scheduled for 2016. This technology has also been used on the LHD USS Makin Island since 2009 while the new America-class amphibious assault ships (LHA 6) will also be fitted with the HED system.

According to Reynolds (2013), the US Navy expects to save at least 5,000 barrels of oil per ship per year with the adoption of the HED system, a number that could reach up to 10,000 barrels per ship depending on the speed profile, thus increasing efficiency by 9-15%.

Another navy with a tradition in electric propulsion systems is the Royal Navy. The new Military Afloat Reach and Sustainability (MARS) tankers of the Royal Fleet Auxiliary's (RFA) will be fitted with a HED system by General Electric (Reynolds, 2013). Similarly, the new Royal Norwegian replenishment-at-sea vessel currently built by Daewoo shipyards will be equipped with a HED system (Laursen, 2014). Finally, the Khareef-class corvette of the Royal Navy of Oman built by BAE Sys-tems also uses the same technology.

A slightly different propulsion concept in which there is no mechanical transmission is the Integrated Electric Propulsion (IEP), installed on Type 45 destroyers of the Royal Navy, as well as on the new US Navy destroyer of the Zumwalt class.

5.4 Alternative Fuels

The fuels used by naval ships are higher distillate fuels (mainly the NATO F-76 type), compared to the heavy fuel oils that are mostly used in the shipping industry. There is a great array of candidate alternative fuels in the shipping industry, with the most popular currently being the LNG. Other options include methanol, biofuels, and hydrogen.

LNG has gained a great deal of popularity in the last years and several ships are propelled by LNG. Its predominance lies in the fact that it is considered the most environmentally-friendly fuel and can be used in Emission Control Areas (ECAs) instead of the more expen-sive low sulphur fuel. However, there are safety and space considerations, and thus, it could be used on certain types of ships, such as auxiliary ships (oilers, support ships, etc.)

The other more prevalent category of alternative fuels is biofuels. Biofuels include a wide range of alternative fuels produced by biomass, or bio waste. They are mostly used as blends with conventional fuels, with the most common blend being the one with Fatty Acid Methyl Esters (FAME biodiesel). These are first-generation biofuels, and are usually derived from the esterification of vegetable oils. Their greatest advantage is that they are sulphur-free, so there are no SOx emissions. On the other hand, there are some technical issues, such as fuel instability or corrosion problems in addition to their higher cost. According to Bailey and Hardy (2014), second- and third-generation biofuels cost four times more than F-76 fuel, and for this reason, they are not expected to play a significant role in the fuel market for the next 15 years.

Although there are concerns regarding the use of FAME in marine systems, the US Navy has put a great focus on biofuels since they can ensure, to some degree, fuel independence from traditional oil sources. Moreover, the US is a dominant producer of agricultural products such as corn, which can be used to produce biofuels. For this reason, the US Navy and the USDA agreed at the end of 2013 on making biofuel blends part of the Navy's regular fuel purchase

under the "Farm-to-Fleet" venture (USDA, 2013). These blends will consist of biofuel blended with 10-50% conventional F-76 fuel. The projections are that drop-in biofuels will be available for less than $4 per gallon by 2016, making them competitive with traditional fuels.

Earlier, in 2011, the US Navy and Maersk had announced their collaboration to test third-generation algae-based biofuels on the container vessel Maersk Kalmar (IRENA, 2015). Since 2010, the US Navy has carried out a series of tests with biofuels produced from Hydroprocessed Esters and Fatty Acid (HEFA) feed-stocks. The primary sources for these biofuels were algae, camelina, as well as waste oils. The tests, which proved successful, included a number of different plat-forms, such as the Riverine Command Boat Experi-mental (RCB-X) and the LCAC, among others.

The first large-scale application, though, was the demonstration of the aforementioned Great Green Fleet in 2012. The biofuels that were used were 50-50 blends of biofuel (made from used cooking oil and algae) and marine diesel F-76. Great Green Fleet Fact Sheet (n.d.)

Other alternative fuels include methanol and more recently, glycerol. Thus far, there is no known application of methanol on a naval combatant. In the commercial sector, however, there are some experimental applications, such as the Stena Scanrail, where methanol is converted into dimethyl ether (DME) before being injected into the cylinder.

Glycerol, which is a by-product of the biofuel industry, is used as a mixture with diesel oil. The Royal Navy is involved in the GLEAMS project (Glycerine Fuel for Engines and Marine Sustainability), which is working on this technology in order for glycerol to be used by marine diesel engines (Bailey and Hardy, 2014).

Finally, another alternative fuel mainly used in Fuel Cell (FC) systems is hydrogen. Fuel Cells are systems that utilize an electrochemical process to convert chemical energy directly into electrical energy. A hydrogen FC system has a minimal environmental impact since the product of the chemical reaction is water. Additionally, they have certain advantages which are important in military applications. Specifically, they do not have any rotating parts, thus resulting in a reduction in noise and vibration, as well as in lower maintenance and operational costs. On the other hand, FC systems are more costly than internal combustion engines. Generally speaking, this technology is considered to still be at the developmental stage and its use is currently limited to submarines.

6. Conclusions

Although naval ships are not strictly restricted by regulations, they are energy intensive systems due to the large amount of electronics, sensors, and weapons used. This trend does not seem to be decreasing since new weapon systems are even more energy demanding, as is the rail gun, for example. According to Doerry, McCoy, and Martin (2010), the US Navy's ships consumed 10.1 million barrels of fuel in 2008, while the projection for 2020's consumption increases this amount by 20-25%. Thus, the need for increasing the energy efficiency of the entire ship is imperative.

However, naval crafts have a number of limitations that are not found in commercial vessels. Naval combatants are weight-sensitive vessels since high speed is a priority. As a consequence, the use of heavy equipment to save energy would be undesirable. Another limitation involves space availability. Generally speaking, most naval crafts are compact platforms built around their weapon suite, and they lack free deck space for the installation of bulky equipment, such as renewable energy systems (solar panels or sails, for example). Additionally, there are limitations that relate to the firing sectors of the weapons, as well as the scanning sectors of the radars.

Of course, this does not mean that increasing the energy efficiency of naval ships, or implementing an energy efficiency policy is impossible. As was previously presented, there are several examples of systems that have been adopted by various navies with encouraging results. For some of these technologies, such as the stern flaps, there is extensive experience and savings are significant. For other more recent technologies, such as the alternative fuels, tests are promising and the potential savings can be high. On the other hand, the successful energy management of a large naval fleet is probably a more challenging task. Adopting a cost-effective energy efficiency policy is a multidimensional problem. A proposed policy would include investing more resources on the ships which have greater energy demands. Another criterion could be the annual operational time of a vessel. Ships which travel more frequently than others should be given priority in installing an energy-efficiency system, compared to the ones that remain idle for long periods of time.

Finally, and probably the least costly measure to apply but not always the easiest, is to change the crews' cul-

ture as energy consumers, towards a more environmentally responsible attitude.

7. Acknowledgements

I would like to acknowledge Laura V. Paz for her assis-tance in editing this paper.

References

Bailey, JJ, Hardy, RJ (2014). "The Green Ship Challenge - Delivering More With Less," The Naval Engineer, Royal Navy, Autumn 2014

Bojovic, P, and Sahoo, PK, and Salas M (2004). "Effect of Stern Wedges and Advanced Spray Rail System on Calm Water Resistance of High-speed Displacement Hull Forms," Proceedings of Pacific 2004 International Maritime Conference

Cullom, P (2010). "Navy Energy Program - Bridging The Energy Gap"

Cusanelli, DS, and Karafiath, G (2012). "Hydrodynamic Energy Saving Enhancements for DDG 51 Class Ships," ASNE Day 2012, Crystal City, Arlington, VA

Design Data Sheet DDS 200-2 (2012). "Calculation of Surface Ship Annual Energy Usage, Annual Energy Cost, And Fully Burdened Cost of Energy," Department of the Navy Naval Sea Systems Command

Doerry, NH, McCoy, TJ, and Martin, TW (2010). "Energy And The Affordable Future Ship," United States Navy

Environmental Protection Agency (EPA) Report EPA-842-D-06-013 (2013). "Underwater Ship Husbandry Feasibility Impact Analysis Report"

Gennaro, G (2012). "Improving the Propulsion Efficien-cy by means of Contracted and Loaded Tip (CLT) Propellers," The Society of Naval Architects & Ma-rine Engineers, Athens, Greece

Great Green Fleet Fact Sheet (n.d.) Retrieved from http://greenfleet.dodlive.mil/energy/great-green-fleet/

Hydrex (2010). "The Slime Factor," Hydrex White Paper No 2

Hydrex (2012). "Ship Propeller Maintenance: Polish or Clean?" Hydrex White Paper No 10

IMO (2012). "Guidelines For The Development Of A Ship Energy Efficiency Management Plan (SEEMP)," IMO MEPC 63/23 Annex 9, Resolution MEPC.213(63), Adopted on 2 March 2012

IRENA (2015). "Renewable Energy Options For Shipping," International Renewable Energy Agency Technology Brief

Kane, D (2013). "Developing A More Fuel Efficient Tonnage Through Blasting Of Hulls And Timely In Water Husbandry," Ship Efficiency Conference Hamburg, Germany

Laursen, W (2014). "Royal Norwegian Navy Goes Electric," Electric And Hybrid Marine Technology International, April 2014, p4-8

Mabus, R (2009). "Naval Energy - A Strategic Approach," Naval Energy Office, Office of the Secretary of the Navy

O'Rourke, R, (2006). "Navy Ship Propulsion Technolo-gies: Options for Reducing Oil Use — Background for Congress," CRS Report for Congress

Reynolds, H (2013). "US Navy Goes Electric," Electric And Hybrid Marine Technology International, April 2013, p20-24

Salas, M, Rosas, J, and Luco, R (2004). "Hydrodynam-ic Analysis of the Performance of Stern Flaps in a Semi-displacement Hull," Latin America Applied Research, vol 34, pp 275-284

Schultza, MP, Bendickb, JA, Holmb, ER, and Hertelb WM (2011). "Economic Impact Of Biofouling On A Naval Surface Ship," Biofouling, vol. 27, No. 1

USDA (2013). "Agriculture, Navy Secretaries Promote U.S. Military Energy Independence with 'Farm-to-Fleet' Program," United States Department of Agriculture, News Release No. 0237.13, Retrieved from ttp://www.usda.gov/wps/portal/usda/usdamediafb?contentid=2013/12/0237.xml&printable=true&contentidonly=true

Walker, M, and Atkins, I (2007). "Surface Ship Hull And Propeller Fouling Management," The Royal Institution of Naval Architects, Warship 2007: The Affordable Warship Conference, Bath, UK

Warship Technology (2014). "Hybrid Electric Programme Powers Up," Warship Technology, a Publication of the Royal Institution of Naval Architects, March 2014, p17Wärtsilä (2009). "Boosting Energy Efficiency," Energy Efficiency Catalogue/Ship Power R&D

George Gougoulidis

Dr. George Gougoulidis is a Lieutenant Commander in the Hellenic Navy, as well as a Naval Architect. He graduated from the Hellenic Naval Academy with a BSc Degree in Marine Engineering and completed his graduate studies at the Massachusetts Institute of Technology (MIT), where he obtained a Naval Engineer Degree, an MSc in Ocean Systems Management, and a PhD in Naval Architecture and Marine Engineering.
During his career as a naval officer, he has served on various types of naval ships in several positions. After fulfilling his service onboard, he served on the Technical Directorate of the two major Naval Bases. He currently serves at the Hellenic Navy's Detachment at Elefsis Shipbuilding and Industrial Enterprises S.A. and he is also a member of the Navy Permanent Committee Quality Assurance (PCQA-6) of the General Directorate for Defense Investment and Armaments (GDDIA).
His research interests include the study and design of advanced marine crafts, as well as the analysis of energy-saving and environmental issues
Dr. Gougoulidis is a member of the Society of Naval Architects and Marine Engineers (SNAME), the American Society of Naval Engineers (ASNE), the Royal Institute of Naval Architects (RINA), and the National Defense Industrial Association (NDIA).

Visit of COM SNMG-2, Rear Admiral Jorg Klein DEU(N), 08 Feb 16

Change of Command Ceremony, 08 Mar 16

Visit of the Director of A7
Directorate of Hellenic MFA, 20 Apr 16

Visit of the Swedish Defence University Delegation,
10 May 16

Exercise NOBLE DINA 2016, Training of Israeli Navy SNAPIR Team, 31 Mar - 03 Apr 16

Exercise NOBLE DINA 2016, Training of US Team, 31 Mar - 03 Apr 16

NMIOTC TRAINING

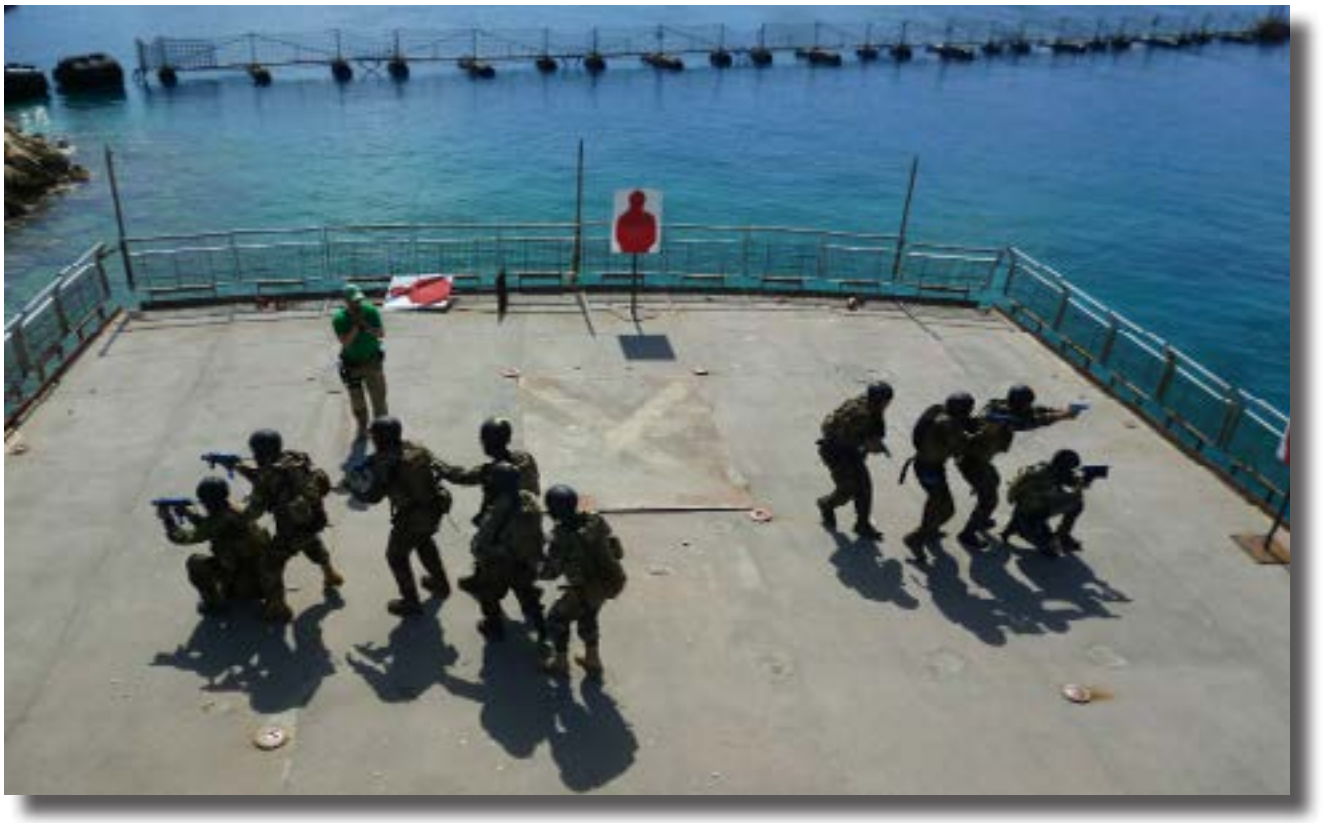
NMIOTC MTT in Bahrain, 03-10 Apr 16

Resident Course 7000, 08-12 Feb 16

Training of FS VAR, 07-08 Mar 16

Training of German Forces for Boarding Deployments Team, 09-19 May 16

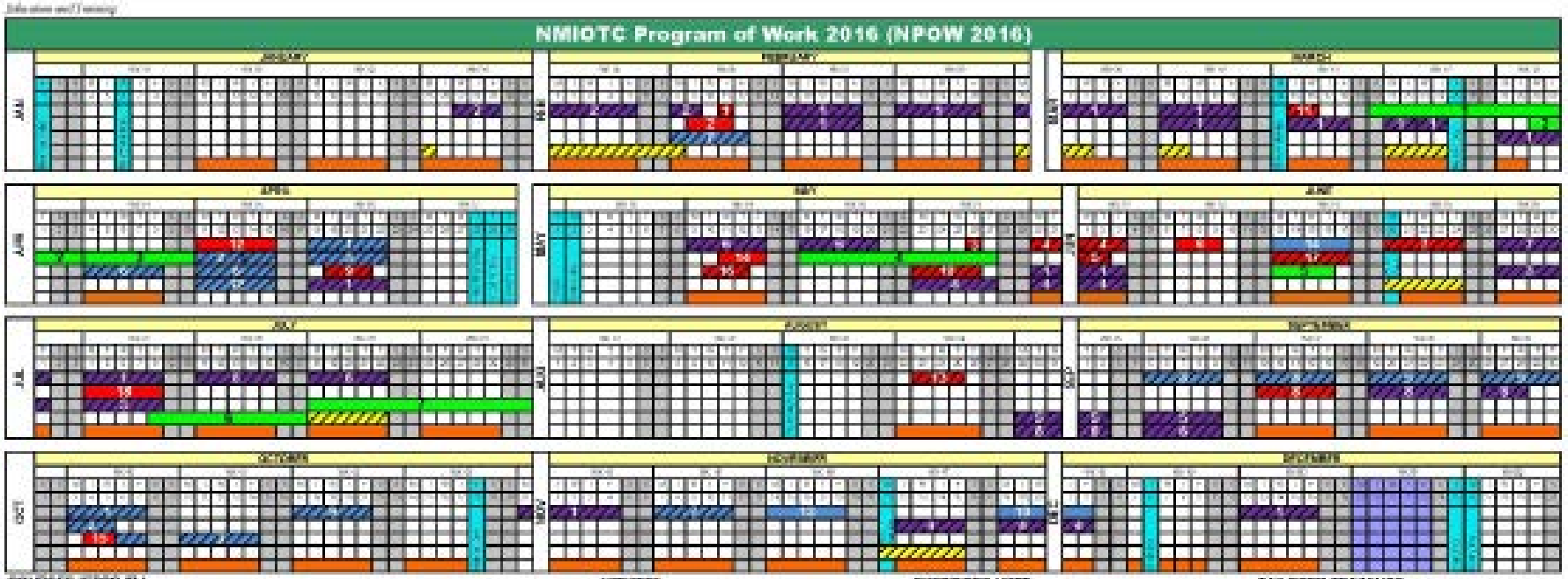
Training of Hellenic Army SOF Team, 29 Feb-11 Mar 16



Training of Hellenic Navy SOF Team, 07-11 Mar 16

Training of German Forces for Boarding Deployments Team, 09-19 May 16

WMD in MIO Experiment with US NPS Monterey and the Hellenic Naval Accademy, 11-15 Apr 16



COURSES (E/TOC (E.)

- Course 1000 - Command Team MIO Issues (OPS-MA-3110)
- Course 2000 - Boarding Team Classroom Issues (OPS-MA-3210)
- Course 3000 - Boarding Team Practical Issues (OPS-MA-4010)
- Course 5000 - Maritime Operational Terminology Course (OPS-MA- 2500)
- Course 6000 - Weapons of Mass Destruction in MIO (OPS-MA-4510)
- Course 7000 - MIO in support of Counter piracy OPS (OPS-MA-4010)
- Course 8000 - C-IED Considerations in Maritime Force Protection (OPS-MA-3507)
- Course 9000 - Legal Issues in MIO (LGL-LG-3125)
- 10 Course 10000 - MIO in Support of Countering Illicit Trafficking at Sea (Pilot) (TBC)
- 11 Course 11000 - AWPD Course (on demand)
- Course 12000 - C-IED Considerations in MIO
- 13 Course 13000 - Illegal Immigration (Pilot) (TBC)
- 14 Course 14000 - Maritime EOD (Pilot) (TBC)

ACTIVITIES

- 1 NAB (NMIOTC)
- 2 FPC NOBLE DINA
- 3 NESA Event (PS1)
- 4 NATO Maritime Operations Law Seminar
- 5 NCB (HNGS)
- 6 NMIOTC Annual Conference
- 7 SACT CUAxS Concept Development Assessment Game (TBC)
- 8 ATP-71 WORKSHOP (TBC)
- 9 Above Water Warfare Capability Group (AWWCG) Meeting
- 10 Maritime Information Services Conference (MISC SPRING 2016-1)
- 11 Maritime Issues for Joint Ops TNA WS
- 12 WMD in MIO NFS Experiment
- 13 NS5M Requirement panel no 31 (TBC)

EXERCISES / MTTs

- 1 MTT (JEDDAH)
- 2 "NOBLE DINA 2016"
- 3 MTT WSS (BAHRAIN)
- 4 "PHOENIX EXPRESS 2016" Underway phase (20-26 May)
- 5 MTT "WORKING LUNCH '16"
- 6 MTT "BREEZE '16"
- 7 MTT "SEA BREEZE '16"

TAILORED TRAININGS

- 1 DIRC ISDF team (Army, Navy, Air Force, Coast Guard, Police, etc)
- 2 Technical Instructor - ToT Course
- 3 USA Team
- 4 MLO EOD Team
- 5 BMC BBIT team
- 6 SDU team
- 7 DEA Training
- 8 SWE BT Training

- 14 International Cyber Summit, Maritime , Cyber Port Security 2016
- 15 Cyber Security Conference
- 16 NATO Individual Education & Training Planning Board(PS-IB)
- 17 5th CIMIC Conference
- 18 Cyber Security Training on Advanced Incident Handling Techniques (CIS-116)

► **Training Tuition Fees on NMIOTC Dir 00-1 (Change 8)**

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

Updated 08 Apr 16

NMIOTC

NMIOTC/ΚΕΝΑΠ
Souda Bay 732 00 Chania
Crete, Hellas

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

Webpage: www.nmiotc.nato.int