

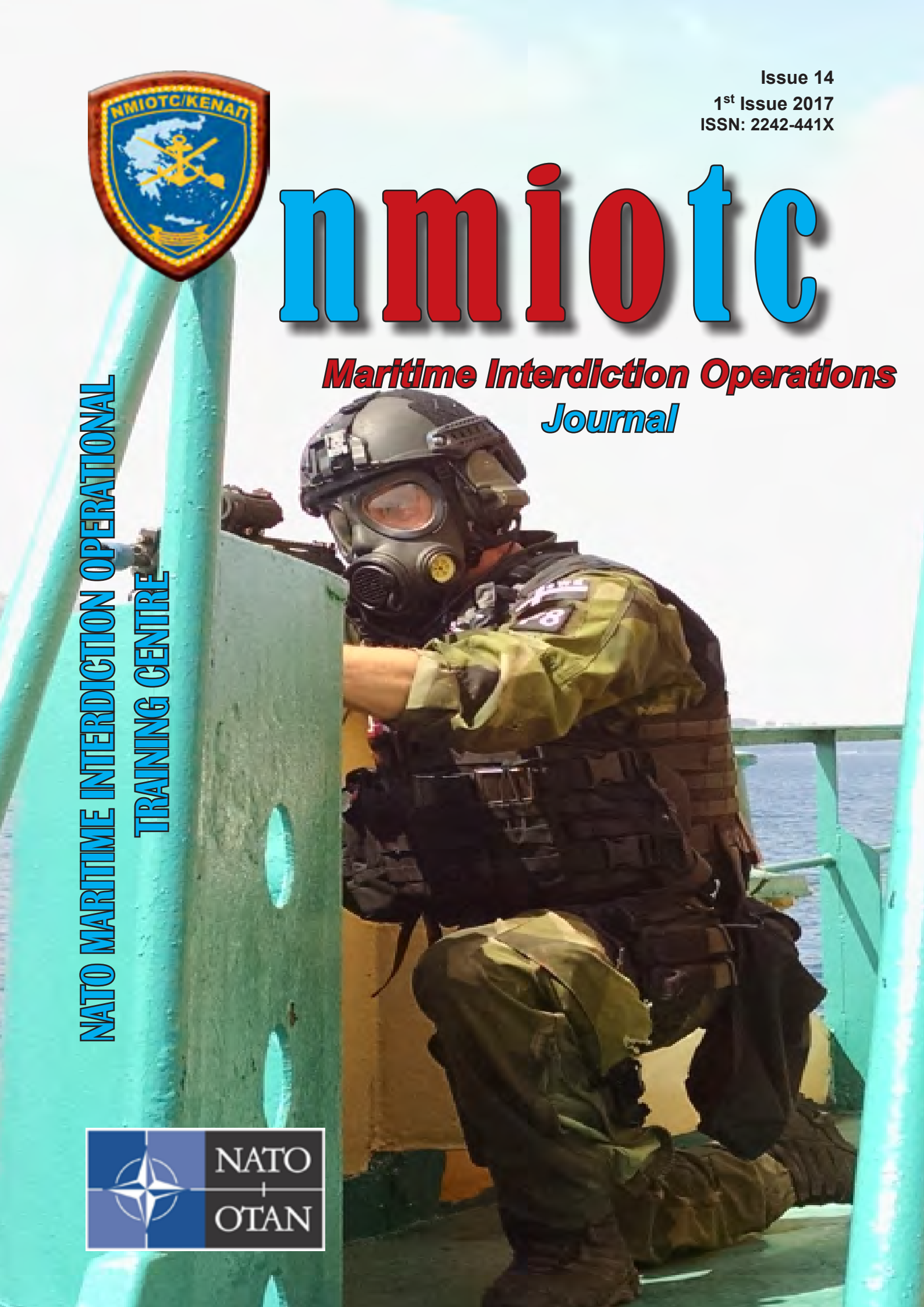


Issue 14
1st Issue 2017
ISSN: 2242-441X

nmiotc

*Maritime Interdiction Operations
Journal*

NATO MARITIME INTERDICTION OPERATIONAL
TRAINING CENTRE





NATO Maritime Interdiction Operational Training Centre

2nd Conference on Cyber Security



**“MARITIME CYBER SECURITY AND
CYBER DEFENSE: NATO-EU COOPERATION
IMPLEMENTING THE OUTCOMES OF THE
WARSAW SUMMIT.
RECENT INTERNATIONAL EVOLUTIONS IN
THE ENVIRONMENT.”**

21st to 22nd September 2017

CONTENTS



COMMANDANT'S EDITORIAL

4

Editorial by Georgios Tsogkas
Commodore GRC (N)
Commandant NMIOTC

MARITIME SECURITY

6

Operation Sea Guardian - The NATO Maritime Security Operation in the Mediterranean Sea
by Captain Corrado Campana ITA (N)

8

Toward a Comprehensive Approach to Addressing Transnational Threats in the Mediterranean
by Mr Christopher Kremidas

CYBER SECURITY

15

Maritime Cyberpower Projection
by Mr Adrian Venables

ENERGY INFRASTRUCTURES SECURITY

29

Holistic Protection of Critical Infrastructures. Resilience and protection of dependencies between Greek Critical Infrastructures.
by George Stergiopoulos, Dimitris Gritzalis, Panayotis Kotzanikolaou, Manos Margkos and Georgia Lykou

TECHNOLOGICAL ISSUES

42

Securing Maritime Logistics and Supply Chain : The Medusa and MITIGATE approaches.
by Dr. Spyridon Papastergiou and Associate Professor Nineta Polemi

HIGH VISIBILITY EVENTS

49

VIP visitors to NMIOTC

NMIOTC TRAINING

52

Photos from NMIOTC Training Activities

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 G. Tzevelekis GRC (N)
Head of Transformation Section

Layout Production

CPO E. Miskou GRC (N)
Journal Assistant Editor

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

All content is subject to Greek Copyright Legislation.
Pictures used from the web are not subject to copyright restrictions.

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



NMIOTC Commandant's Editorial

The world continues to face a serious threat from terrorism – a global threat that knows no border, nationality or religion. NATO Heads of State and Government stated at Warsaw, “terrorism has risen to an unprecedented level of intensity, reaches into all Allied territory and now represents an immediate and direct threat to our nations and the international community”.

NATO is as essential as ever. At this pivotal time, the Alliance is strong and continues to adapt. This was the core of NATO's Summit in Brussels in late May. NATO's Framework for the South focuses on improving the Alli-

ance's regional understanding and situational awareness, its capabilities for expeditionary operations and its ability to project stability in its neighborhood.

Maritime environment is characterized by complexity and diversity. The oceans are an increasingly accessible environment for transnational criminal and terrorist activities. Disruption of international maritime transportation and distribution networks would undermine equally the industrial production and the flow of energy sources, thus it will have a significant impact in our security and at the welfare of our populations.

It is anticipated that the Warsaw / Brussels Summit outcomes would call for enhanced training opportunities along with our partners providing security. 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 environment, offers education and training opportunities to Allies and Partners.

With Operation Sea Guardian and EU Operation Sophia under which the demand for training of the Lybian authorities is increasing, the emphasis on partner capacity building and the es-

establishment of the Hub for the South at JFC Naples, the request for NMIOTC expertise and services to serve as the Trainer for the Hub in the South at both JFC Naples and MARCOM disposal, can only grow.

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, Mr. Christopher Kremidas US European Command Liaison to NATO and EU, on his paper "Toward a Comprehensive Approach to Addressing – Transnational Threats in the Mediterranean" draws upon building a comprehensive approach culture within NATO, enabling

closer co-operation with international stakeholders to address the security challenges. Adrian Venables, PhD Student at Lancaster University and Commander UK RN (reserve), on his article "Maritime Cyberpower Projection" investigates the unexplored area of how cyberspace can be used to influence a target population. Senior Researcher George Stergiopoulos and Professor Dimitris Gritzalis, deals with the "Holistic Protection of Critical Infrastructure" a subject of high importance for the welfare of each country. Finally, Dr Spyridon Papastergiou and Associate Professor Nineta Polemi, at their paper explore the risks and vulnerabilities of the Maritime Logistics and Supply Chain presenting two European research projects.

As a conclusion, I would like to announce with great pleasure, the 2nd NMIOTC Cyber Conference which will be held at our premises (Souda Bay – Crete) from 21st to 22nd September 2017, with theme "Maritime Cyber Security and Cyber Defense: NATO-EU cooperation implementing the outcome of the NATO Warsaw Summit. Recent international evolutions in the environment".

Given the opportunity, please mark your calendars for the 9th NMIOTC Annual Conference from 5th to 7th June 2018 with the main topic to be determined and announced in due time.

Georgios Tsogkas
Commodore GRC (N)
Commandant NMIOTC





by Corrado Campana
Captain ITA (N)

The NATO Operation Sea Guardian started in November 2016 as a result of the July 2016 Warsaw Summit, during which the Alliance decided to launch a new maritime security mission in the Mediterranean Sea. As reported in the Warsaw Summit Communiqué: “We have transitioned Operation Active Endeavour, our Article 5 maritime operation in the Mediterranean, which has contributed to fight against terrorism, to a non-Article 5 Maritime Security Operation, Operation Sea Guardian, able to perform the full range of Maritime Security Operation tasks, as needed”.

Operation Sea Guardian (OSG) constitutes the first actual activation of one of the tasks assigned to NATO’s maritime forces by the Alliance Maritime Strategy (AMS) of March 2011, the Maritime Security Operations, and directly derives from its predecessor Operation Active Endeavour (OAE), which was launched after the events of September 11 with the purpose to deter and disrupt terrorist activity in the Mediterranean Sea.

The broad and long-lasting experience gained by OAE, with NATO Standing Naval Forces ensuring presence, collecting information, monitoring, con-

trolling and boarding merchant vessels in the Mediterranean for more than a decade, has provided the Alliance with a strong expertise in the deterrence and prevention of maritime terrorist and criminal activities, and this proficiency is exploited by OSG as it continues with the efforts of OAE, but with a significantly broader scope.

As mentioned in the “Operation Sea Guardian Factsheet” of the Allied Maritime Command: “Operation Sea Guardian is a standing Maritime Security Operation (MSO) aimed at working with Mediterranean stakeholders to deter and counter terrorism and

mitigate the risk of other threats to security". In this context, the three main missions of OSG are to provide maritime situational awareness, to counter terrorism and human trafficking, and to contribute to the regional capacity building, while additional tasks – such as countering the proliferations of Weapons of Mass Destruction (WMD), ensuring the freedom of navigation and protection of maritime critical infrastructure – can be performed as necessary.

Further to a Joint Declaration signed by the NATO Secretary General, the President of European Council and the President of European Commission in July 2016, OSG also cooperates with the European Union Naval Force (EU-NAVFOR) MED Operation Sophia. In the Joint Declaration, it was recognized that "a stronger NATO and a stronger EU are mutually reinforcing", and with this in mind NATO contributes to the activities of Operation Sophia in the Mediterranean Sea with the provision of information, surveillance and logistic support, while also contributing

to the implementation of the arms embargo in the high seas off the coast of Libya in accordance with the UNSCR 2292 (2016).

The NATO involvement in tackling the worst migration crisis since the Second World War and, more in general, in securing the Mediterranean Sea, can be considered as a remarkable accomplishment for the Alliance, as it demonstrates its willingness and readiness to take action to cope with a challenge affecting the Allies, and also because it proves the capability to make the Allied Maritime Strategy operational. Indeed, with the Operation Sea Guardian in the Mediterranean Sea NATO is not only implementing the AMS, but also – for the first time since its approval in 2011 – executing the full spectrum of Maritime Security operations.

Within the framework of the AMS, Operation Sea Guardian is an updated version of the precedent Operation Active Endeavour, with a broader scope and mission, though a relevant change from OAE is that the resources

allocated to OSG are separated by the assets (ships, submarines and maritime patrol aircrafts) that compose, on a rotational basis, the NATO Standing Naval Forces. This characteristic allows OSG to keep the focus on its main tasks without being committed to the responsibilities of the NATO Response Force (NRF).

The launch of OSG represents the first real implementation of the NATO-EU Joint Declaration and, while accomplishing the task of crisis management in the Mediterranean Sea, it promotes the dialogue in the region and improves the cooperative maritime security ensuring presence and surveillance.

The efforts to address the migrants and arms smuggling, to fight the maritime terrorism and, in broader terms, to contribute to maritime security and stability in the Mediterranean Sea, are performed by NATO in the full awareness that the security in Europe can only be granted by ensuring stability in this strategic Sea and in the region of Middle East and North Africa.

Captain Corrado Campana

Attended the Italian Naval Academy from 1987 until 1991, when he was commissioned as Ensign. He has achieved the qualification in Naval Artillery and Missile Systems and the specialization in Naval Weapons Direction. He served onboard several Italian Navy ships such as the frigates Libeccio and Maestrale and the destroyers Ardito and Luigi Durand de la Penne, and was appointed as Commanding Officer of the auxiliary ship Ponza and of the frigate Granatiere. He served in international staffs such as the Force HQ of the Multinational Force and Observers (M.F.O.) in El-Gorah (Sinai, Egypt) as Naval Advisor, and the EU Naval Force OHQ in Northwood (UK) as ACOS CJ3 Operations within the anti-piracy Operation ATALANTA. He served in national staffs such as the Command in Chief of the Italian Fleet as Head of the Artillery and Missile Systems Section, the Command of Italian Maritime Forces in Taranto as ACOS N3 Operations and at the Italian Joint Operations HQ in Rome, as Head of Maritime Operations Section (J3). He attended the Italian Joint War College and the Course in International Humanitarian Law at the Centre for Defence High Studies in Rome and also served as Tutor for the attendees. Captain Campana has achieved the Degree in Maritime and Naval Science at the University of Pisa, the Degree in Political Science at the University of Trieste, and the Master in International and Military-strategic Studies at the L.U.I.S.S. University "Guido Carli" in Rome. Since the 1st August 2013 he is appointed at the NATO Maritime Interdiction Operational Training Centre in Souda Bay, Crete, Greece as Director of the Training Support and Transformation Directorate.





Toward a Comprehensive Approach to Addressing Transnational Threats in the Mediterranean

by Mr. Christopher Kremidas
US European Command Liaison to NATO and the EU

Abstract

In recent years the challenges posed by the current security environment include instability in fragile and failing states and the resulting cycles of violence and humanitarian disasters has led NATO to adopt the Comprehensive Approach to improve coordination.

dination among international actors. At the same time, some of the most prevalent challenges facing the Euro-Atlantic community today are transnational threats such as organized crime, terrorism, illicit trafficking in humans, drugs, and weapons and weapons, cyber crime, and the possibly destabilizing challenge of irregular migration. Within this context, the Euro-Atlantic community should take a more proactive approach to employing the Comprehensive Approach, starting with addressing transnational threats in the Mediterranean before they reach the crisis stage. At the same time, building a Comprehensive Approach culture within NATO and in conjunction with other international actors will help to transform its relationships with the and enable closer cooperation and collaboration in addressing common security challenges.

1. Introduction

In recent years the challenges posed by the current security environment include instability in fragile and failing states and the resulting cycles of violence and humanitarian disasters. More recently, we have also seen the impact of spillover from these fragile and failing states. In some cases, these effects have been serious enough to impact and endanger previously stable states. At the same time, some of the most prevalent challenges facing the Euro-Atlantic community today are transnational threats such as organized crime, terrorism, illicit trafficking in humans, drugs, and weapons and weapons, cyber crime, and the possibly destabilizing challenge of irregular migration. In some cases, we can be dealing with

a number of tasks required to bring stability to a failed state while simultaneously addressing the impact of transnational threats, some of which seek to take advantage of a vacuum in governance.

2. The Comprehensive Approach

The Comprehensive Approach (CA) is a way to achieve a common understanding and approach among all actors of the International Community through the coordination and deconfliction of political, development and security efforts in solving an international crisis.

The requirement to work with partners and the nature of these new challenges have made operations increasingly complex, requiring a closer level of coordination and collaboration. On the ground, partners generally find a way to work together successfully but at the operational and strategic levels, coordination has been characterized by a lack of understanding and insufficient awareness and coordination of each other's planning. A strategic and operational level process was needed to build coherency and the answer has been the Comprehensive Approach, which focuses on building a shared understanding of the problem, developing a shared overarching vision of the solution and facilitating coordination of effort while respecting the individual mandates of multiple entities. NATO heads of state and government recognized the need for a Comprehensive Approach when it tasked the North Atlantic Council to develop pragmatic proposals for it during the Riga Summit in November 2006. In 2008, at the Bucharest Summit, Allied lead-

ers endorsed an Action Plan for the development and implementation of NATO's contribution to a Comprehensive Approach.

At the Lisbon Summit in November 2010 and in its new Strategic Concept, the Alliance "...decided to enhance NATO's contribution to a comprehensive approach to crisis management as part of the international community's effort and to improve NATO's ability to deliver stabilization and reconstruction effects". To support this decision, NATO agreed to form a modest civilian capability to interface more effectively with other actors and conduct appropriate planning in crisis management. The effective implementation of a comprehensive approach requires all actors to work together with a shared sense of responsibility and openness, taking into account and respecting each other's strengths, mandates and roles, not to mention their decision-making autonomy. In other words, the Comprehensive Approach is not hierarchical but rather it is a collaborative effort among equals.

NATO's experience from operations, including Afghanistan and in addressing piracy, has demonstrated that managing complex conflicts and crises requires a wide range of internal and external actors, including governments, civil society, the private sector and international agencies, to work together in a coherent and coordinated effort. In a Comprehensive Approach, the military can provide a secure space to enable other actors to address immediate humanitarian needs and the root causes of the problems.

Given the requirement to include civil society, nongovernmental organizations (NGO), and private enterprise - no single organization or nation can

MARITIME SECURITY

conduct an effective Comprehensive Approach by itself. This large number of actors and the complexity involved in coordinating actions are particularly challenging from the perspective of the Comprehensive Approach (CA). Actors can vary from local governmental officials and parties in the conflict to private sector entities and local NGOs. The variety of international actors includes other international organizations and NGOs, humanitarian actors, donor governments and representatives of the private sector.

The risk of not working together through a Comprehensive Approach is to have our efforts result in fragmented and inconsistent programs and policies, which can duplicate efforts leading to inefficient spending and a reduced capacity for delivering results. At the same time, a failure to work together to address the often linked conditions of underlying causes can force us to start over again and again, much like Sisyphus endlessly trying to push the rock up the hill.

3. Toward a Proactive Application of The Comprehensive Approach

Since its inception, the Comprehensive Approach has been applied in the aftermath of emergency situations where international actors found themselves thrust together by necessity – in other words, we've used it only when reacting to security challenges. Given the two main challenges facing the alliance today: hybrid warfare threats from the east and transnational threats from the south, a more proactive application of the Comprehensive Approach is urgently needed.

3.1 Since 2014, Russia's use of broad-spectrum tactics to splinter Europe's ability for collective action has been given a name; hybrid warfare. The concept of hybrid warfare is the mix of conventional and unconventional, military and non-military, overt and covert actions employed in a coordinated manner to achieve specific objectives while remaining below the threshold of a formally declared warfare.

3.2 Hybrid Warfare targets critical vulnerabilities and seeks to create ambiguity in order to hinder swift and effective decision-making. There are a wide range of measures applied as part of a hybrid campaign; from cyber attacks on critical information systems, through the disruption of critical services, such as energy supplies or financial services, to undermining public trust in government institutions or exploiting social vulnerabilities. While the concept of hybrid warfare is not new, its application by Russia, and to a lesser extent by Daesh, against NATO member states' interests has presented a new challenge to the Alliance.

3.3 In response, NATO finds itself at a transformative juncture once again. Post-2014 NATO has adopted the Readiness Action Plan (RAP) as a means of responding rapidly to new threats as they present themselves along the eastern and southern flanks.

3.4 More recently, NATO adopted a Hybrid Warfare Strategy in December 2015 and the European Union adopted its Joint Framework for Addressing Hybrid Threats in April 2016. Both documents speak to taking a proactive "whole-of-government" approach in conjunction with a variety of actors in order to improve resiliency, security,

and continuity of governance in the face of hybrid threats. At the same time, both documents call for greater NATO-EU cooperation in addressing hybrid threats and the staffs of both organizations have worked together to agree upon a number of areas where they can focus their cooperative efforts.

3.5 As we can see, both NATO and the EU are proactively applying some (but not all) of the principles of the Comprehensive Approach as they address the challenges of hybrid warfare. But even this method is not sufficient in dealing with the broader challenge of transnational threats on NATO's southern flank nor does it address root causes. Thus, the work that remains to be done is for the Comprehensive Approach to be applied to the challenge of Transnational Threats in the south, especially in the Mediterranean Region.

4. Transnational Threats: A Challenge to Governance

Transnational threats are commonly defined as threats such as organized crime; terrorism, illicit trafficking in humans, drugs, and weapons, cyber crime, and the destabilizing challenge of irregular migration. In the Mediterranean, this broad group of threats can also take the form of proliferation of weapons of mass destruction (WMD), cyber attacks targeting the commercial shipping and port security sector, natural and manmade disasters, illegal, irregular and unreported (IUU) fishing and environmental pollution. The three aspects most discussed currently are transnational organized crime, terrorism, and irregular migration.

4.1 Transnational organized crime refers to self-sustaining groups that operate transnationally to obtain power, influence, and commercial gains, wholly or in part by illegal means. They also protect their activities through corruption and/or violence, while exploiting and creating gaps and seams in the framework of transnational commerce, communications, and financial mechanisms.

Increasingly, their illicit activities across borders and communities not only adversely impact security and economic health but also contribute to an illicit underworld operated by powerful criminal networks that can present a challenge to governance.

These illicit criminal organizations pose an immediate threat to public trust and weaken governance since unlike legitimate business, they require a system of impunity that gives them the freedom of action to conduct their illicit activities. In building, maintaining, and growing this system of impunity they corrupt government officials, computer systems, financial institutions, and deny governments the ability to maintain their sovereign borders and exclusive economic zones. This in turn weakens their ability to collect taxes and customs fees to fund their government's activities.

It is important to note the challenge to governance is not just a threat to troubled states but to our own as well. As criminal networks' influence spreads outward, it brings corruption with it – even into currently well-governed nations.

4.2 Terrorists require and use the same financial and transportation pathways and system of impunity to move people, weapons, and coordi-

nate their activities. In addition and unlike organized crime groups, terrorists also require sophisticated strategic communications capacities in order to gain the maximum impact for their actions.

Terrorists also present a challenge to governance in that they stress the system to respond which can lead to harsh measures, disrupted economic activity and reduced freedom of movement for citizens – all of which can drive a wedge between the people and their government.

4.3 Irregular migration is a complex



problem because it presents a wide variety of human security, law enforcement, development, and governance challenges in dealing not just with the symptoms but also the root causes. This issue can also be a sensitive problem internally when absorbing large irregular migrant flows.

In many cases, these arrivals are viewed as unwelcome and a potential threat to national identity, unity, and stability. The typical response has

been to erect stronger immigration barriers that affect both regular and irregular migrants as well as refugees. These policies have a number of unintended consequences such as increasing illicit entries, causing them to attempt riskier methods to gain entry, and fostering the growth of sophisticated criminal trafficking networks.

At the same time, irregular migration is seen as more than just a humanitarian concern. One danger is the potential of terrorists exploiting illicit crossings to facilitate their operational aims. Two possible forms come to mind:

using migrants as a cover to secretly enter Europe and taxing smugglers to access departure points under militant control as a means of raising money.

5. Applying the Comprehensive Approach to addressing Transnational Threats in the Mediterranean

So, what would a Comprehensive Approach in the Mediterranean look like?

MARITIME SECURITY

In order to know for certain, it would require the actors to come together to work through the stages of conducting a common assessment of the challenges, developing common approaches to address them, and planning for coordinated actions among nations and organizations. Until then, there are some indications of what their results may look like.

In the last few years of facilitating international discussions among law enforcement, diplomatic, military, intelligence, and humanitarian actors on how to collectively address transnational threats in the Mediterranean, a few common themes emerge.

5.1 First, is the need for complementarity, coordination and collaboration. Unilateral and/or partial responses are recognized not only as limited and short sighted but also as leading to secondary effects which expose neighboring governments to a new array of challenges to their national security.

5.2 Secondly, it is general recognized that most all of the transnational threats in the Mediterranean are of a law enforcement nature and thought must be given to how military capabilities can support and amplify law enforcement efforts while not crossing any legal boundaries which may prohibit military forces from directly conducting law enforcement activities. Finding ways to achieve this is necessary because no government can afford to purchase these same capabilities twice.

5.3 Thirdly, because of the large number of security-related agencies from more than a dozen countries operating in the Mediterranean, rapid and comprehensive information dissemination is necessary to enable a Comprehen-

sive Approach in action.

In this case, it is necessary to move from a culture of “need to know” to one of the “duty to share” information. This is the most effective way to build trust, enable coordinated action, ensure true interagency cooperation, and facilitate the production of common threat assessments.

While information sharing is generally viewed as essential in dealing with maritime threats, instituting a robust information fusion capability encompassing military, law enforcement, and commercial sources can be a real challenge,

This is due to the number of laws and agencies involved and the reality that many agencies are reluctant to release real-time actionable information. Often this stems from the inherent cultural tension between entities involved in interdiction (with a bias for immediate action) and those responsible for investigations (whose concern is to collect and protect evidence on an entire network for successful criminal prosecutions).

5.4 Finally, reducing the tension between security concerns and human rights in this context is an area where the Comprehensive Approach can help us to find common ground. In this case, a Comprehensive Approach could include contributions from experts in Law of the Sea, maritime security, migration and refugee studies, and human rights, to address the position of migrants and refugees from an integrated perspective. Through the inclusion of these perspectives, we can develop an approach on how to respond to differing needs and legal entitlements of migrants and refugees and how to reconcile them with State

obligations and security constraints.

Despite this seemingly large number of obstacles to closer cooperation, applying the Comprehensive Approach to addressing transnational threats can show us the areas where we can work together to achieve our common goal of security and stability in the Mediterranean.

“Don’t Let What You Cannot Do Interfere With What You Can Do” ~ John Wooden

6. Potential Areas For Further Exploration

6.1 Situational awareness: Seeking shared awareness and developing a common understanding of evolving threats through a continuous exchange of information among actors in the Mediterranean region. The Information Fusion Centre (IFC) in Singapore is a good model for a non-hierarchical multinational maritime security information fusion capability. Through the timely sharing of information, it facilitates timely and effective responses from partners through linkages to 65 agencies in 35 countries, and with 16 International Liaison Officers (ILOs) from 15 countries. The IFC also conducts capacity-building activities such as international information-sharing exercises and workshops, for example, the biennial Maritime Information Sharing Exercise (MARISX).

6.2 Planning and Conduct of Operations: Enhance integrated civilian-military-law enforcement planning throughout the planning process and in operations in adjacent waters. FRONTEX’s European Patrols Network (EPN) is an excellent example of how to accomplish this among sev-

eral nations, ministries, and agencies. The EPN is a permanent regional border security concept that enables the synchronization of national measures of EU Member States and their integration to joint European activities. It is based on Member States' existing activities and on strengthening of cooperation and coordination at national and EU levels.

6.3 Lessons Learned, Training, and Exercises: Commonly collect and share lessons learned and best practices from putting the Comprehensive Approach into action in the maritime environment and incorporate them into training and exercises. At the same time, invite other actors to participate in exercises and training to strengthen cooperation and mutual trust. With its experience and connections to a wide variety of maritime experts and actors, especially from years of addressing counter-piracy and its more recent emphasis on transnational threats, the NATO Maritime Interdiction Operations Training Center (NMIOTC) is uniquely suited to serve as a focal point for the Comprehensive Approach in the maritime environment.

6.4 Strategic Communications: Where possible, share information strategies and campaigns regularly to ensure complementarity and mutual reinforcement with other involved international organizations and local actors.

6.5 Cyber Defense: Seek to build shared threat awareness and mutually supportive improvements to resist cyber attack. Enhance cyber information sharing of best practices at the technical level – including on technical innovations, incident handling methodologies, and secure configuration of networks in order to improve cy-

ber incident prevention, prediction, detection, and response. The NATO Cooperative Cyber Defence Centre of Excellence in Estonia can serve an important role in bridging the civ-mil gap in cyber security.

7. Summary and Recommendations

The Comprehensive Approach is now a recognized method to achieve a common understanding and approach among various actors of the international community through the coordination and deconfliction of political, development and security efforts in solving an international crisis.

Currently, both NATO and the EU are applying some principles of the Comprehensive Approach in their strategies to address the challenges of hybrid warfare. But even this approach is not sufficient in dealing with the broader challenge of transnational threats on NATO's southern flank since it does not address root causes nor include the collaboration of a number of entities to include private enterprise, NGOs, and civil society.

Taking into account the increasing recognition of the Comprehensive Approach as an essential process to improving coordination among various actors in solving major security challenges, the following recommendations are offered.

7.1 A Comprehensive Approach for the Mediterranean. On NATO's southern flank and in particular the Mediterranean region, the Hybrid Warfare Strategy is insufficient to address the variety of transnational threats since they are much broader in scope. Thus, a Comprehensive Approach Work-

ing Group of regional actors must be convened at once to apply the process to the problem of both Transnational Threats and threats from state actors in the Mediterranean Region. This group can provide a holistic assessment of the issues and make recommendations for a common approach and enable the Alliance to develop its own strategy in concert with other regional and international actors. A similar effort for the Black Sea region should also be considered.

7.2 A More Proactive Use of the Comprehensive Approach. When major international challenges arise, rather than waiting until the crisis stage is reached, a Comprehensive Approach Working Group should be convened at the problem recognition stage to provide a holistic assessment of the issues and make recommendations for a common approach among regional and international actors. This would also allow for the NATO Secretary General to provide a more comprehensive strategic assessment to better frame the issues for SACEUR when asking for military options and advice to be provided to the North Atlantic Council.

7.3 Build a Comprehensive Approach Culture. Sponsor and host Comprehensive Approach Awareness Seminars at headquarters throughout the NATO Command Structure and Centers of Excellence to engage and build habitual relationships with regional actors to enable the Alliance to enhance its readiness to put the Comprehensive Approach into action at the strategic, operational, and tactical levels. This will enable a Comprehensive Approach culture to take root at all levels within the Alliance and help

MARITIME SECURITY

to transform its relationships with other international actors.

7.4 Move the Comprehensive Approach into the Mainstream. Finally, within NATO it is time to mainstream the Comprehensive Approach so it is

no longer seen just as a Civilian-Military (CIMIC) or J9 function but rather one that is equally owned and supported by operators, strategists, and logisticians.

The views presented in this paper rep-

resent the author's personal opinion and findings and not the official views or policy of the United States government.

References

European Commission (2016), Joint Framework on Countering Hybrid Threats. <http://ec.europa.eu/DocsRoom/documents/16201>

"Effective Cooperation: The Bedrock of Any Security Architecture" ADM (ret) P. Xinofotis, NMIOTC Journal, July 2013. <http://www.nmiotc.nato.int/files/NMIOTCjournal7.pdf>

European Commission (2014). "Maritime Security Strategy", http://ec.europa.eu/maritimeaffairs/policy/maritime-security/index_en.htm

Guptill, Murray "Sandy," Course Designer, NATO Comprehensive Approach Awareness Seminar, Interviews Sept 2015-April 2016

NATO (2011), "Alliance Maritime Strategy", http://www.nato.int/cps/en/natohq/official_texts_75615.htm

NATO (2010), "NATO's Strategic Concept 2010", http://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120214_strategic-concept-2010-eng.pdf

NATO Defense College (2011), NATO Comprehensive Approach Awareness Seminar, Course Guide



Christopher Kremidas

Chris Kremidas currently serves as Liaison to NATO and the EU for US European Command (EUCOM). His previous positions include service as Political Advisor to the Commander, NATO Training Mission – Iraq and Assistant Political Advisor to Commander, Joint Forces Command Naples.

He has also served as Chief Strategist for US Joint Task Force North, Policy Planner at the US Delegation to NATO, and as Deputy Defense Policy Advisor for the US Mission to the European Union (EU). Previously he served as Regional Cooperation Manager for the Mediterranean region at the EUCOM Joint Interagency Counter-Trafficking Center (JICTC).

He earned a master's degree with honors in Strategic Studies from the Swiss Federal Institute of Technology (ETH Zurich) and a Bachelor of Arts in Political Science from Ball State University. He is also a distinguished honor graduate of the NATO Defense College and a veteran of

Operation Iraqi Freedom.

Mr. Kremidas is a recognized expert on the NATO Comprehensive Approach and has published several articles on it as well as serving as facilitator and course designer for NATO Comprehensive Approach seminars throughout Europe. Chris Kremidas is also a sought-after expert on multinational maritime border security cooperation and has facilitated numerous dialogues on information sharing, coordinated responses, and addressing irregular migration.



Maritime Cyberpower Projection

*by Adrian Venables,
PhD Student at Lancaster University, UK and
Commander UK Royal Naval Reserve
a.venables2@lancaster.ac.uk*

Abstract

UK military doctrine recognises five operating environments, Maritime, Land, Air, Space and Cyberspace. These are not regarded as totally separate war-

fighting arms as demonstrated by the use of amphibious troops, maritime aviation and the use of satellite derived communications and intelligence illustrating how naval forces can utilise the distinctive attributes of other envi-

ronments in the projection of seapower. This paper examines the as yet unexplored area of how cyberspace can be used as a mechanism by which the maritime environment can generate cyberpower to influence a target popu-

lation afloat or ashore. The maritime and cyber environments have many similar characteristics such as their dependence on manufactured resources to exploit their potential and that their size prevents them from being under the total control of a single power, but that temporary regional control is vital for trade, communication or to achieve an effect on an adversary's behaviour. By examining the components of cyberspace that are dependent upon the maritime environment, methods to identify the components that can project the new concepts of maritime cyberpower and cyber seapower are explored with particular emphasis on addressing the potential cyber vulnerabilities of ship systems.

Introduction

The maritime operating environment is one of five recognised by UK Ministry of Defence (MoD) doctrine, the others being Land, Air, Space and Cyberspace. This paper describes the relationship between the maritime and cyber environments and introduces the concept of maritime cyberspace in terms of cyberpower projection. The nature of maritime power is an important one for states that are either dependent on the seas for trade or security or wish to have an influence in the areas surrounding their coasts. Drawing on UK maritime doctrine, the concept of power at sea and from the sea in terms of control and denial is explained in which free access to areas of the oceans are required to be maintained by nation states. Allied to sea power is the issue of maritime security and its related tasks, which may include a cyber element that will

present additional unique challenges of operating at sea or in coastal regions. The link between the maritime and cyber environments is a subject that is poorly researched, yet the two have many similarities and have mutual dependencies in their use for trade, communication and the projection of national power. Current doctrinal definitions are explained and the two environments are compared leading to the introduction of the new terms of Maritime Cyberpower and Cyber Seapower. This is followed by an examination of the composition of maritime cyberspace and its characteristics to show how they contribute to security and the influence of others through power projection. The paper concludes with methods to identify the components of maritime cyberspace in order to project maritime cyberpower and cyber seapower with particular emphasis on the need to address the potential cyber vulnerabilities of ship systems.

Defining the maritime environment

At the heart of any definition of the maritime environment is an acceptance of its critical importance to global trade, security and as a source of fuel and food. With the growth of globalisation, climate change and over population resulting in unsustainable regional pressure on natural resources, this role is not going to diminish in the foreseeable future. Indeed, it is predicted that a high proportion of future conflicts will occur in or adjacent to a zone of maritime influence.¹ From a military perspective, the sea also provides access for amphibious, land and embarked

air forces to embark on expeditionary operations as part of a coordinated strategy to achieve their government's strategic objectives. The maritime operating environment is described in UK Ministry of Defence (MoD) doctrine as providing critical access for joint assets allowing influence in support of political objectives, the conduct of a wide range of maritime security and international engagement and when necessary, the means to assemble and apply decisive combat power at a time and place of political choice.² The Doctrine highlights that maritime power is not an end in itself, but operates within a wider national security framework and that the environment comprises six dimensions; Physical, Economic, Political, Diplomatic, Legal, and Military. These are noted as being interrelated and of equal importance although the physical element provides the overarching context for all and highlights its uniqueness.³

Cyberpower and the maritime environment

The UK Ministry of Defence defines maritime power as the ability to project power at sea and from the sea to influence the behaviour of people or the course of events.⁴ As such, it is coherent with other more general descriptions of the concept of power and to achieve this maritime forces have a number of unique attributes that they can exploit such as Access, Mobility, Lift Capacity, Sustained Reach, Versatility, Poise, Resilience and Leverage.⁵ Although cyberspace is viewed as a unique environment alongside land, air, sea and space, these are not regarded in isolation as operating areas.

This is demonstrated in the UK by the coordinated use of the Royal Marines amphibious troops, the Royal Navy's Fleet Air Arm and the deployment of satellite supported communications and intelligence capabilities illustrating how naval forces can utilise the distinctive attributes of the other environments in the projection of seapower. However, although the dependencies between these physical elements is well recognised, each one's unique link to cyberspace is not and the concept of how the projection of cyberpower could be conducted from the sea has not attracted much, if any, discussion and requires further investigation. This may be due to a lack of understanding of the unique conditions of the coastal and oceanic regions or that they are not considered suitably different from the other environments to warrant particular investigation. What effort has been devoted to the subject has been concentrated on the related security aspects of shipping, which in 2016 is now gaining increased interest from both the mercantile industry and suppliers of cyber security products. The maritime environment and its relationship with cyberspace in the projection of power introduces the concept of maritime cyberpower as a facilitator of maritime power. The role of cyberspace in contributing to maritime power is acknowledged as going beyond just information systems and reaching into command and control, intelligence, surveillance and reconnaissance activities as well as the physical control of systems. Thus the importance of the cyber environment is recognised as a facilitator in the effective operation of other systems, but not as a means to exert power at sea

in its own right.⁶ However, the use by both state and non-state actors of cyberspace as an asymmetric means to seek an advantage over an otherwise militarily superior force is also recognised. This is significant as it implies that the maritime community afloat is no longer platform centric and detached from cyberspace, but an integral part of it if connected via satellite, mobile telephony or via radio transmission of digitised navigation or other maritime related information. Although this brings advantages, it also exposes the maritime community to the same risks and vulnerability to attack as their land based counterparts. This is exacerbated by the issue of software aging in which a ship's lifespan may exceed that of the software that is required to operate it. This will require regular, but potentially expensive and time consuming 'software refits' to mitigate for any vulnerabilities in their systems, but which may in reality offer no additional functionality and may even reduce performance if the hardware upon which it is running is not upgraded at the same time.⁷ This may well also be combined with increased automation and the integration of different functions into a single system to reduce the manpower required afloat, which further limits its ability to operate without the aid of the computer systems. Ocean going vessels are also increasingly reliant upon a robust logistics organisation to provide global support – a system that itself is dependent upon Internet based communications and disruption of such networks may have a significant effect on the seaworthiness or ability of a ship to embark on transcontinental passages. This emphasises the integrated nature of cyberspace and that

cyberattacks experienced at sea must not be investigated in isolation, but that evidence, precedence and developments in other environments should be considered as part of a holistic approach in their resolution.⁸

Maritime Power at sea

In order to project maritime power, it is necessary to be able to deliver an effect at sea and from the sea. Initially the term Command of the Sea was used to be able to exploit the environment to an advantage. However, as this implied total control of the entire ocean all of the time, which was impractical, other terms are now used that refer to a more realistic aspiration of temporary control limited in time and space to that required to conduct a given task or operation. Sea Control is defined as the freedom to use an area of the sea for one's own purpose for a period of time and if necessary to deny its use to an opponent if it is contested and requires dominance of the surface and sub surface environments including the seabed and the air above.⁹ This may range from being able to exercise the right of innocent passage in a state's territorial water or Exclusive Economic Zone to using force to eliminate another naval force from challenging control over an area of sea. As Sea Control is a temporary condition, it would usually be an objective in order to conduct a particular mission or as a precursor to other operations. Depending on the threat, obtaining it may involve actual military action against an opponent at sea or their containment by blockade to prevent them from accessing the disputed area. The concept of Sea Denial dif-

CYBER SECURITY

fers from Sea Control in that it occurs when one party prevents another from controlling an area, but without controlling the region itself. Historically minefields or the threat of submarines were used to deny access to an area or threaten opposition surface forces. More recently and especially in littoral areas, surface to surface missile or gun batteries have been used to present an increased level of risk that may deter maritime forces from operating in coastal regions. Sea Control and Sea Denial may also be used in conjunction as denial in one region may facilitate control in another.

Maritime security

There is a direct correlation between power and security, which is applicable in all environments including maritime and cyberspace. As power seeks to influence the behaviour of people or the course of events, this may be perceived as a threat, particularly if it is detrimental to a government or society's policy, social norms or strategic ambitions. Among multiple definitions of security, the Oxford English Dictionary includes Freedom from threat or danger, and safeguarding the interests of a state.¹⁰ Effective security can thus be used as a means to counter the effects of a campaign of power projection or influence – it is a counter power strategy. At sea, maritime security can be utilised as a means to counter some of the measures used to exert control over people or systems by a threat actor, be they state sponsored or criminally motivated. These may range from efforts to exercise power through Sea Control or Denial to protecting fisheries or maintaining

the operation of offshore oil platforms from the adverse influence of others. The UK National Strategy for Maritime Security defines it as:

*...the advancement and protection of the UK's national interests, at home and abroad, through the active management of risks and opportunities in and from the maritime domain, in order to strengthen and extend the UK's prosperity, security and resilience and to help shape a stable world.*¹¹

Within the military context, British Defence Doctrine notes that the role of national security encompasses the safety of the State and its protection from both external and internal threats, but is also integrated within, and dependent upon, the security of neighbouring states and partners. The former of these counter the threat of invasion, attack or blockade and the latter includes the dangers from terrorism, subversion, civil disorder, criminality, insurgency, sabotage and espionage.¹² The role of cyberspace is referred to within the context of an attack on the country's critical national infrastructure. This document also obliquely refers to the maritime component by highlighting that the government's primary duty is to maintain the freedom and integrity of the UK and that its stability, prosperity and well-being depend on international trade and investment. This it notes requires raw materials being imported and goods exported by sea and are facilitated through access to global information flows. In highlighting the threat posed to the UK by criminals operating in the maritime environment; terrorism, disruption to trade or the freedom of

navigation, maritime attack against the national infrastructure, arms proliferation, drugs and people smuggling are all listed.¹³

Defining the cyber environment

Although there is no formally accepted definition for the cyber environment, the UK Ministry of Defence's Cyber Primer describes it as the interdependent network of information technology infrastructures, (including the Internet, telecommunications networks, computer systems, as well as embedded processors and controllers), and the data therein within the information environment.¹⁴ At the heart of cyberspace is information and the information environment is defined by the UK Ministry of Defence as a logical construct whereby assured information can pass unhindered from point of origin to point of need, with assured meaning that the information can be proven as authentic and that the originator can be identified.¹⁵ The Cyber Primer also moves beyond just describing cyberspace to what comprises military operations in the environment, defining them as the employment of capabilities where the primary purpose is to achieve effects in, or through, cyberspace. This has significant coherence with the definitions of maritime power projection and security in being able to influence the behaviour of people or the course of events. In an attempt to explain cyberspace as part of the Information environment, the Primer describes it in terms of three domains; the Physical (hardware, location and networking components), Virtual (software, networking protocols and information),

and Cognitive (people, their roles and groupings). Noting that cyberspace is a complex and dynamic environment, the Cyber Primer emphasises its importance to military operations and the reliance it places on defence communications. However, it also notes the need to use Commercial Off The Shelf (COTS) hardware, software and civilian owned and operated infrastructure for its essential operations.¹⁶ This requires protective measures to be implemented to enable mission critical systems and the information they carry to function with the requisite resilience in order to maintain the same confidentiality, integrity and availability of data as military systems. A key facet of this is its relationship and interdependency with the electromagnetic spectrum, which is an integral part of the cyber environment, particularly for mobile platforms that do not have access to a fixed infrastructure for communication. However, data exchange via radio frequency transmissions have the significant disadvantage in that they can be intercepted and unless encrypted can be subject to collection for analysis, manipulation or interference by persons other than the intended recipient thereby making them a valuable target for espionage, sabotage or subversion.

Comparing maritime and cyber environments

Although the maritime and cyber environments may appear very dissimilar at first inspection, there are a significant number of parallels that can be drawn between them and many of the factors that need to be considered when operating at sea can also apply

when seeking to achieve an effect in cyberspace. For example, the totality of the two environments are both ungovernable by a single authority, indicating that sea control and denial may have equivalents in cyberspace for power projection. Both also require manufactured devices to effectively use them, be they ships or computing devices as unlike land warfare, a human cannot enter and engage with the environment unaided. Furthermore, the maritime and cyber environments are international in nature with ships at sea originating from many countries and cyberspace comprised of components manufactured worldwide, with no single country having total dominance in either. However, influence can be exerted as seen by some states having large merchant fleets or being dominant in the computer or networking markets. Similarly, in order to function, there are global agreements that govern both environments – The United Nations Convention on the Law of the Sea (UNCLOS) in regulating the use of the oceans and the use of internationally accepted addressing and routing protocols that control how data is exchanged in the networks of cyberspace. By adapting the UK's definition of Maritime Power of The ability to project power at sea and from the sea to influence the behaviour of people or the course of events and by using the concept of seapower as the basis for projecting cyberpower, the notion of Maritime Cyberpower can be introduced as:

The ability to project cyberpower at sea and from the sea to influence the behaviour of people or the course of events through and within the medium of cy-

*berspace.*¹⁷

In addition to using the features of the maritime environment as a means of influencing others in the wider medium of cyberspace, it is also conceivable to use the properties of cyberspace to develop the concept of power at sea in the conventional sense. This presents a new theory of cyber seapower, which can be termed:

'The ability to use cyberpower to project power at sea and from the sea to influence the behaviour of people or the course of events in the maritime environment'

There is a distinct difference in these new concepts of maritime cyberpower and cyber seapower as whereas the former seeks to achieve an effect from the sea that influences events anywhere in cyberspace, the latter seeks to use cyberspace to achieve an effect solely in the maritime environment, including the littoral. An example of maritime cyberpower would therefore be to use a maritime platform to disrupt or influence a cyber infrastructure at sea or ashore to prevent access or to alter the content of systems in order to affect the behaviour of a population ashore. Cyber seapower however would be to utilise the medium to directly affect the ability to facilitate Sea Control or Sea Denial. This would include adversely affecting the ability of ships, ports or offshore installations to operate normally. The concepts of Maritime Cyberpower and Cyber Sea Power within the contexts of Cyberpower and Sea Power are shown in Figure 1 below, which emphasise their contributory nature to the wider power component and their role in circumventing the security of the defender:

CYBER SECURITY

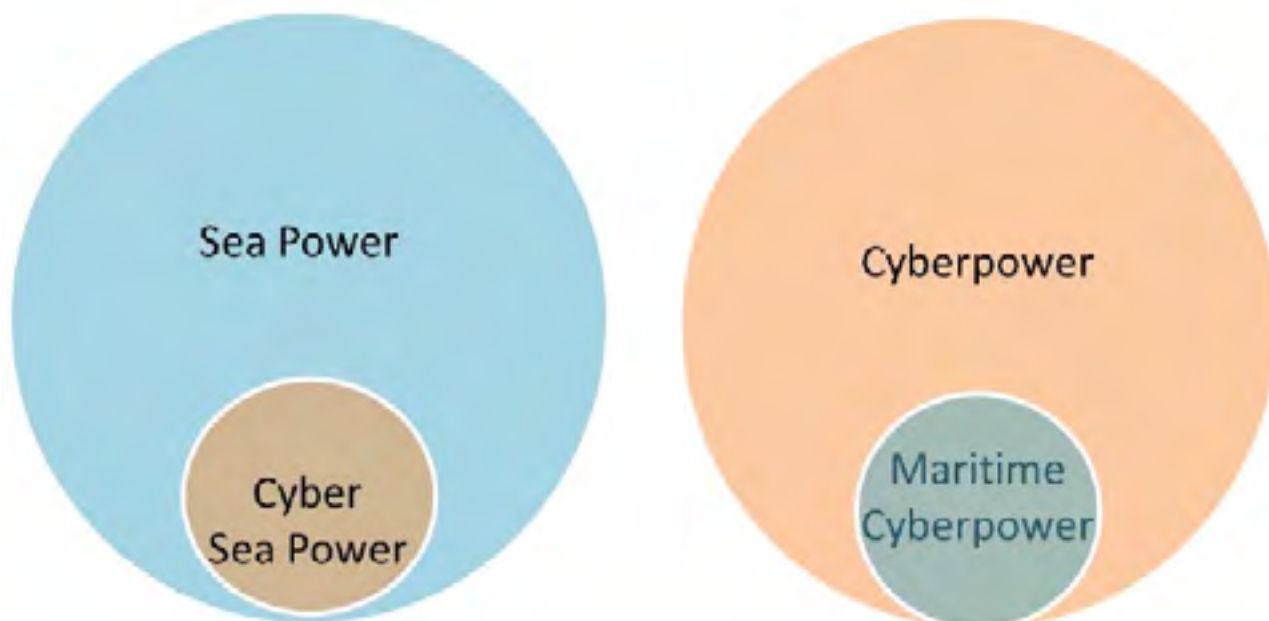


Figure 1: The relationship between Sea Power, Cyberpower, Cyber Sea Power and Maritime Cyberpower

Characteristics of maritime cyberspace

Maritime cyberspace relies on a range of technologies to function with some unique to the environment, but others widely used in all areas of cyberspace. Combined, they form the elements upon which shipping is now dependent for their safe and effective operation with the use of satellite based navigation systems arguably the most significant. The primary system in use is the Global Positioning Satellite (GPS) constellation, which is an American owned capability that provides users with position, navigation and timing (PNT) services. The system is quoted as operating to an

accuracy of a millionth of a second, velocity to within a fraction of a mile an hour and location to within 100 feet.¹⁸ It should also be noted that although GPS is the predominant satellite based PNT system, there are two others in use; the European Galileo and Russian Glonass systems. When fully deployed in 2020, the Galileo system will comprise 24 satellites with initial services available from the end of 2016.¹⁹ The Russian Glonass system also comprises 24 satellites and provides worldwide coverage, although it is optimised for northern latitudes. Initially developed for military use, it is now being exploited commercially and many receivers are able to receive

signals from multiple systems to increase their accuracy.²⁰ Although primarily regarded as an aid to navigation, satellite based PNT systems are fundamental to ensuring maritime platforms remain connected to cyberspace by providing network timing, altitude and azimuth information to enable receivers to acquire the satellites. They are however very vulnerable to a variety of attacks including spoofing (imitating), hijacking (altering) and corrupting the transmissions, which interfere with the data due to the relative weakness of the signals received from space being easily overwhelmed by malicious terrestrial based transmitters.²¹ Although illegal to own or use

in many countries, jammers are widely available with well documented examples of their use denying maritime and port services.²² Satellite based navigation systems are also a primary component of the second element of maritime cyberspace, the Automatic Identification System (AIS). This is a system introduced to enhance the safety of vessel traffic by automatically exchanging information in real time as well as being able to track and monitor ships.²³ The use of AIS transponders is a mandatory requirement for all passenger vessels and international shipping over 300 tons and comprises Very High Frequency (VHF) data transmissions broadcasting a range of information types including the platform's identity, position acquired from GPS and infor-

mation about its passage.²⁴ It is a vital aid used by shipping for collision avoidance and for transmitting data relating to search and rescue operations, meteorological, hydrological and navigational safety information.²⁵ AIS is also used for tracking vessels within a nation's territorial waters and is fundamental to the safety of shipping in areas of high concentration such as the English Channel, where it is integral in the Dover Straits Channel Navigation Information Service.²⁶ More recently, satellites have been used to receive AIS data, which is updated hourly to provide global coverage of information on shipping outside the range of shore based receivers. By accumulating this data, it is possible to show worldwide shipping and areas of high traf-

fic concentration as shown in Figure 2. This enables AIS data to be integrated not only in the maritime cyber environment, but also accessed by anyone with an Internet connection. There are several websites such as www.vesselfinder.com that offer near real time AIS data overlaid on mapping software that not only indicate the position of vessels active on AIS, but enable searches to be made for individual ships and respond to searches about the information that they are transmitting.²⁷ However, as an open standard using unencrypted message formats and with data accessible via the Internet, it has also been found to be vulnerable to a range variety of attacks including spoofing, hijacking and jamming.²⁸



Figure 2 – Global satellite AIS coverage²⁹

CYBER SECURITY

In addition to providing position, navigational or time information and enabling the reception of AIS information transmitted from ships, satellites are also fundamental to maritime data and voice communications. There are two main systems in use; the UK based International Maritime Satellite Organisation (INMARSAT) set up by the International Maritime Organisation (IMO) in 1979 and the UAE based privately owned THURAYA network. Both provide near total global coverage, although INMARSAT has a greater footprint at extreme latitudes, but as both systems employ geostationary equatorial satellites, they are limited in performance at the poles. INMARSAT's maritime service offers a range of telephony and broadband Internet connections providing comparable services to land based fixed infrastructures and

provide the option of bespoke applications tailored for shipping.³⁰ THURAYA also offer a maritime communications service with an option of voice and / or data services. Their data services are similar to that of a terrestrial provider, but do not offer the specialised maritime applications of INMARSAT.³¹ Both systems do however enable ships to establish a permanent connection to the cyber environment with similar functionality to a land based subscriber. Despite the space based segments of commercial satellite systems being regarded as resilient to common forms of cyber attack, recent research has revealed a range of vulnerabilities in the user terminals. These include hardcoded credentials common to all devices, the use of insecure protocols and backdoors that could be exploited by an attacker in a

range of scenarios.³² Although details of these weaknesses were made known to the manufacturers to enable software patches to be developed, they emphasise that notwithstanding the investment in communication infrastructure and end user devices, software can still be the weak point in any computer based system. In addition to space based connectivity to the cyber environment, it is possible to use more traditional radio frequency (RF) communication methods to transfer data using the same protocols as the Internet. These however can be more challenging to engineer and have significant restrictions; both in the limitations of the medium and their sensitivity to changes in atmospheric conditions. The propagation of radio waves depends on their frequency as shown in Figure 3 below:

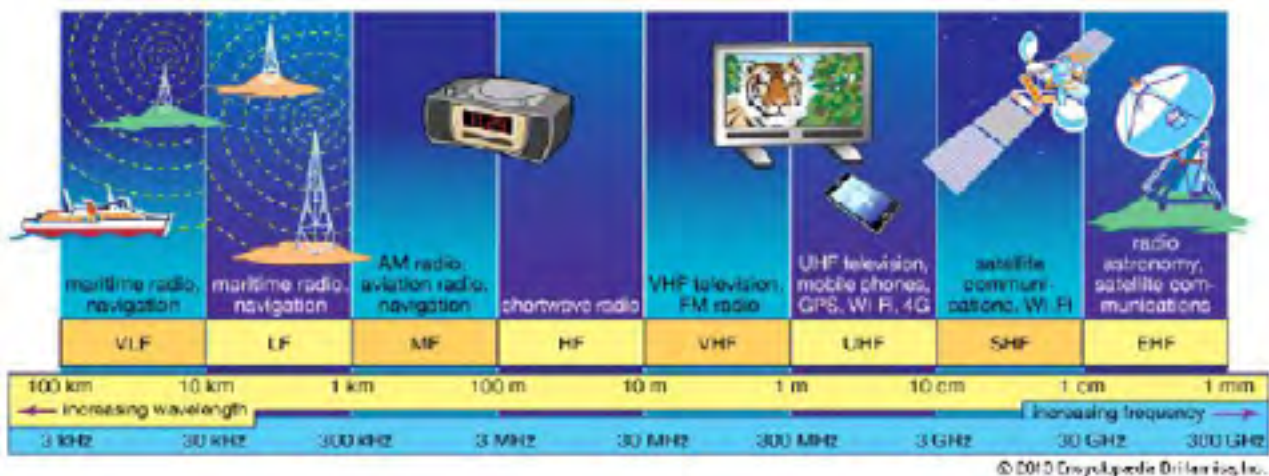


Figure 3 - Commercial radio frequency spectrum³³

Within the RF spectrum, information is transmitted by changing the value of the signal. The faster the signal is changed, the more information can be passed and as frequency is a direct measurement of the rate of change in values, the higher the frequency of the signal, the more information can be passed – hence the use of Super High Frequency (SHF) transmissions for high data rate satellite communications.³⁴ Transmissions at the Very High Frequency (VHF) and above are line of sight and so are ideal for point to point links to satellites, but using these elements of the spectrum for non-space based communications is limited in range to the visible horizon and the lower the frequency, the lower the data rate. Below VHF, High Frequency (HF) radio transmissions have the property that they can refract off the ionosphere layer of the atmosphere and be received over the horizon from the transmitting station. Known as ‘sky wave’, this range of frequencies is commonly used for long range marine radio and despite their lower frequency restricting the potential data rates of communications, they can be used for the transmission of e-mails. In addition to a compatible transceiver, this requires the use of a radio modem, computer hardware and an account with a specialist service provider such as sailmail.³⁵ It should be noted though that

long range HF communications are not as reliable as SHF based satellite communications as reception depends on frequency, atmospheric conditions and time of day. Dead zones can also occur close to the transmitter where no signal is received and ranges achieved at night can be twice that of day time communications.³⁶ RF based E-mail systems such as sailmail use dedicated file transfer protocols in addition to the standard Internet protocols of Transmission Control Protocol and Internet Protocol (TCP/IP) that are required for web browsing. To be effective, TCP/IP relies on a continuous transfer of data packets, not only to exchange information, but also to check that the packets have been received correctly. The quantity of these additional data packets and the latency of the transmission if skywave is used is beyond that which can be realistically transmitted over the limited data rates of HF and packet loss due to unreliable connections could render the communications channel ineffective. However, there have been some attempts at using IP over HF, particularly by the military, which have developed their own standards to make the most efficient use of the limitations of the medium.³⁷ As with all RF transmissions, communications are open to interception and measures must be taken to ensure their security. Communications denial is also pos-

sible, although depending on the distances and transmitted power, the jamming station may be required to be either within the line of sight of the target or close by. The final component of maritime cyberspace is without doubt the most important and yet is mostly out of sight with the majority of its users of oblivious to its existence. Despite the increasing use of wireless devices to interact with cyberspace via mobile telephony or Wi-Fi, beyond the cell phone mast or wireless router, the majority of data communication is wired and for international communication this involves fibre optic cable laid on the ocean floor. This network of more than 300 undersea cable systems stretches over 550 000 miles and transports 99% of all trans-oceanic digital communications. The longest single cable has 39 landing points from Germany to Korea and spans 24 000 miles.³⁸ Their essential role in data and voice communications has resulted in its reliability being deemed by some countries as absolutely essential for the functioning of governments and the enforcement of national security and because of this they are regarded by many as being part of their critical national infrastructure.³⁹ This network is also relatively centralized and follow similar routes across the globe with some laid over 25 000 feet below the ocean’s surface.⁴⁰ This routing pattern is due to the lower risk of using

CYBER SECURITY

paths which have previously proved successful and some seabed topography being more suited to laying cables than others. Routes tend to avoid shipping lanes to avoid damage from dragging anchors and are also highly politicized with cable companies often having to overcome objections from local communities for a variety of reasons including economic and environmental concerns, resulting in their paths often being circuitous rather than direct.⁴¹ They also tend to terminate in or near traditional port cities following conventional trading routes.⁴² Compared to satellite communication, undersea cables are cheaper to use, have a longer lifespan and have shorter transmission times as geostationary communication satellites are placed in orbit at altitudes of 22 000 miles above the earth. This means that a signal travelling between London

and New York takes one eighth the time to reach its destination by cable than by satellite.⁴³ As the numbers of these cables expand they offer increased redundancy of communication as well as capacity and a range of routing options leading to a greater resilience in global communications. The combination of their known approximate location, quantity of traffic that they carry and importance to national communications has not been lost on governments who have taken a keen interest in the cables used by their adversaries. In the 1970s the US National Security Agency conducted Operation Ivy Bells against Russian telephone cables off the Kuril Islands to the east of the country. Divers operating from submarines positioned recording pods on the lines, which would then be retrieved after a period of time for later examination.⁴⁴ More

recently, both US and Russian submarines and spy ships have been reported operating near undersea fibre optic cables leading to fears that they might be able to either tap into them to intercept the data or be planning to attack them in times of tension or conflict.^{45,46} The ability to monitor or even sever direct communications with its allies and the rest of the world would significantly degrade a nation's cyberpower and may result in data having to be rerouted across other networks that may have increased latency or already be subject to monitoring activities. These four elements of cyberspace; satellite based PNT, AIS and wired as well as wireless communications are now fundamental components of the maritime environment and together form the new concept of maritime cyberspace. The relationship between them is shown in Figure 4 below:

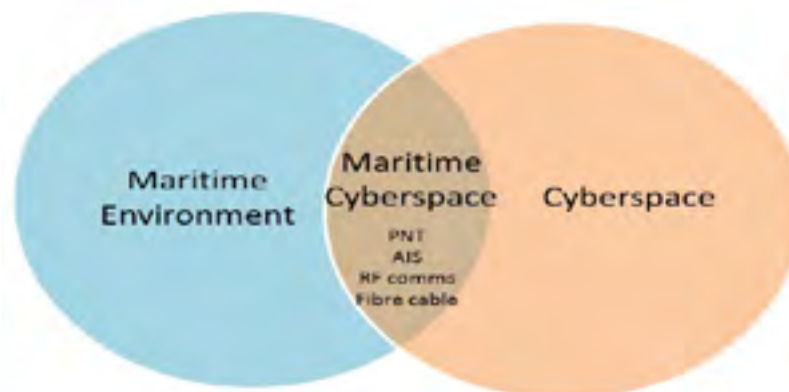


Figure 4 – The composition of maritime cyberspace

Exploiting Maritime Cyberspace

Having identified the similarities and dependencies between the maritime and cyber environments and their use for the projection of power in both areas, it can be seen that the exploitation of maritime cyberspace offers significant potential for developing national power, whilst emphasizing the importance of maintaining its security to protect it from those that would wish to degrade it. By combining Figures 1 and 4, a composite model of power projection in maritime cyberspace can be derived, which is shown

in Figure 5. This demonstrates that both maritime cyberpower and cyber seapower can be developed either separately or as part of a combined strategy.

The challenge of preventing adversaries from using maritime cyberspace to exert maritime power by compromising ships' systems is being addressed by several organisations, including Security Lancaster. In a paper published in February 2016, the risks were highlighted of integrating previously separate components into a single integrated network, which is then connected to the Internet. The practice of automating the control and management of differ-

ent capabilities is becoming increasingly common with commercial providers offering Integrated Platform Management Systems (IPMS) that oversee all aspects of a vessel's propulsion plant and systems, whilst interfacing with communication suites and PNT systems. This provides a remote monitoring and control capability that reduces the number of personnel needed to check systems in situ and enables the rapid detection and response to maintenance issues as they occur. Suppliers of IPMS reduce risk and cost by relying on well-established technologies including operating systems and networking

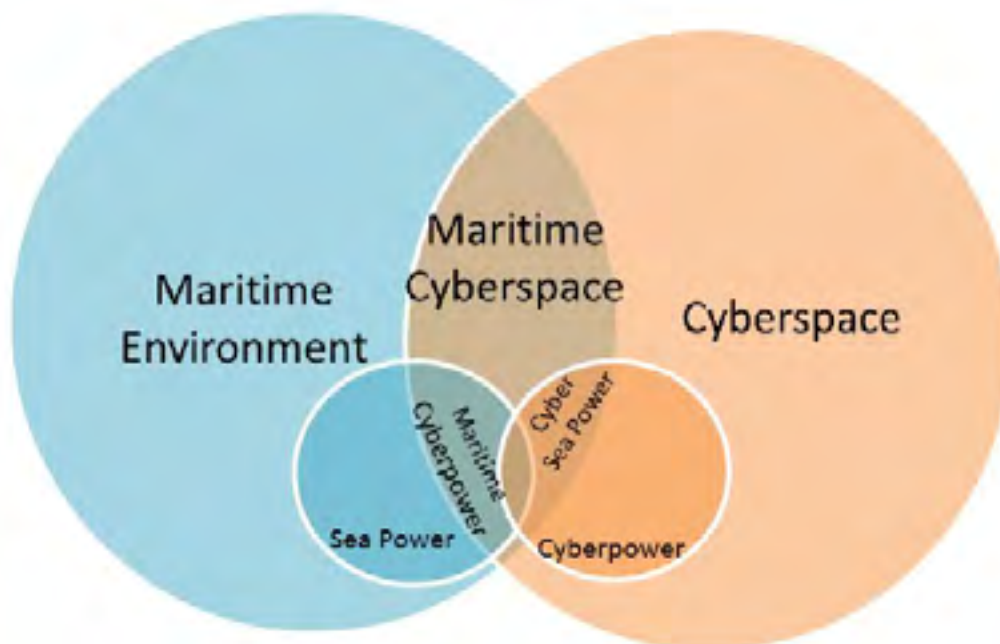


Figure 5 – Power projection in the maritime and cyber environments

CYBER SECURITY

components that would be familiar in a home or office environment. Reliability is ensured by incorporating proven COTS components that have already been used in a range of environments and using open architectures with industry standard protocols. This enables systems to be easily configured, re-configured and upgraded with a range of software packages to suit the individual needs of the customer. However, although using commonly available products and software that are proven and reliable provides reassurance that a system will work, they may also introduce a range of vulnerabilities caused by a failure to properly secure and patch systems that can be exploited by those of malicious intent. Software that is in widespread use is also the most frequent to be targeted by malevolent parties as their efforts in understanding and developing techniques to access and alter computer code will be rewarded by being able to be used effectively against a broad range of targets. An appreciation of what type of technology is used in ships and then being able to easily acquire copies to work on will also make their task easier. Similarly, components that are intended to be upgradable are designed to be easily accessible, which further increases their potential vulnerability to malicious interference. There is no shortage of methods available by which a ship's

system integrity can be compromised by a human operator, either intentionally or by accident. A direct connection to the network by an infected laptop or USB stick may be the easiest method, but wireless networks or remote access logins via an Internet connection may also be a convenient means to access the system. A vessel in port with a network that is unencrypted or protected by a weak password would also offer an attractive and easily accessible target. In addition, the use of multifunctional control terminals presents another system weakness as once compromised they could provide access to the entire network and its subsystems.⁴⁷ The use of cyber seapower as a means to threaten shipping and the maritime environment is now being recognised as the subject of several conferences and by the UK shipping industry, which offers guidance to ship owners and operators on how to assess their networks and put in place the necessary procedures and actions to maintain the cybersecurity of their ships.⁴⁸

Conclusion

This paper has introduced the concept of the maritime cyber environment by bringing together the individual attributes of both elements to highlight their importance and mutual dependence. Understanding the maritime environment is vital both in

terms of appreciating its role to society in supporting trade and in the projection of political power and influence. The seas are often a source of conflict as neighbouring nations compete for limited resources in adjacent waters and are used as a means of transporting essential materials. This results in issues that could previously be regarded as being matters of foreign policy quickly becoming of domestic importance as legal and diplomatic disputes can quickly become militarised as nations seek to protect what they regard as their own, while exerting influence in those areas claimed by other nations. By developing the two distinct but related terms of maritime cyberpower and cyber seapower, the maritime environment can be seen to contribute to the ability to project national cyberpower, which may have global impact. Whereas the former utilises the maritime environment to lever the properties of cyberspace to alter the behaviour of a target individual, group or population, the latter uses the cyber environment to facilitate Sea Control or Denial to establish the free use of an area of sea for a period of time or to deny its use to an adversary. In this way, the comparable properties of both environments enable parallels to be drawn as to how these different forms of power can be exercised. A key conclusion from investigating

maritime cyberspace is the link between security and power projection. In order for an adversary, whether a state or non state actor, to be able to exert a cyber influence on a target, they have to be able to access it either directly or indirectly. Cyber security measures will prevent or limit the access that an attacker will have and therefore restrict the effect that they hope to achieve. This highlights the need to understand the potential vulnerabilities that may exist in maritime cyberspace and the need to be self-critical in how this environment can be seen from the perspective of both attackers and defender and how offensive and defensive strategies can be developed. Academic institutions are now becoming aware of the issues

that have arisen from combining elements of the maritime and cyber environments and in particular how this may affect operations from a security context and the importance of the role of the user in maintaining system integrity. This is coherent with one of the most significant elements of both environments; that in order to fully engage with them, operators have to understand and interact with manufactured elements whether these are ships or computing devices. Maritime cyberspace is unique in both comprising and relying on a number of discrete capabilities including space based systems for position, navigation and time information, the Automatic Identification System for a range of navigational

safety based capabilities and wireless communication from either space or terrestrial radio frequency based systems. The final element of maritime cyberspace consists of the thousands of miles of fibre optic cables that cross the ocean floor connecting continents and which are crucial to the very existence of the environment. With the increasing trend to combine previously separate ship systems onto a single network controlled by an IPMS, which may be connected via satellite to shore based networks, whole vessels can now be considered part of maritime cyberspace and must be protected from those wishing to influence the behaviour of nations by compromising the systems upon which their shipping depends.

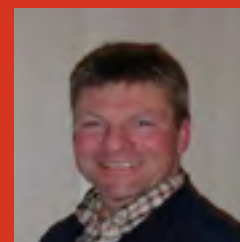
References

- ¹ Ministry of Defence, 2011. British Maritime Doctrine. 1st ed. London: Development, Concepts and Doctrine Centre. P.v
- ² Ibid. Para 123
- ³ Ibid. P.iii
- ⁴ Ibid.
- ⁵ Ibid.
- ⁶ Ibid. para 355.
- ⁷ Fitton, O., Prince, D., Germond, B. & Lacy, M., 2015. The Future of Maritime Cyber Security, Lancaster: Lancaster University. p.9.
- ⁸ Ibid. p.28.
- ⁹ NATO, 2014. Allied Joint Doctrine for Air Maritime Coordination AJP-3.3.3. 1st ed. Brussels: NATO. para 0303
- ¹⁰ Oxford English Dictionary, 2016. Oxford English Dictionary. [Online] Available at: <http://www.oed.com/> [Accessed 12 Apr 2016].
- ¹¹ HM Government, 2014. UK National Strategy for Maritime Security, London: Her Majesty's Stationery Office.
- ¹² Development, Concepts and Doctrine Centre, 2014. Joint Doctrine Publication 0-01 UK Defence Doctrine. 5th ed. London: Ministry of Defence.p3
- ¹³ Ibid. p.9
- ¹⁴ Development, Concepts and Doctrine Centre, 2013. Cyber Primer. 1st ed. London: Ministry of Defence. p1-1
- ¹⁵ Ministry of Defence, 2013. Defence Information and Communications Technology Strategy. 1st ed. London: Ministry of Defence. P8
- ¹⁶ Development, Concepts and Doctrine Centre, 2013. Cyber Primer. 1st ed. London: Ministry of Defence. p1-3
- ¹⁷ Ibid. p.iii
- ¹⁸ US Air Force, 2015. Global Positioning System. [Online] Available at: <http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104610/global-positioning-system.aspx> [Accessed 12 Apr 2016].
- ¹⁹ European Space Agency, 2016. Galileo navigation. [Online] Available at: http://www.esa.int/Our_Activities/Navigation/The_future_-_Galileo/What_is_Galileo [Accessed 12 Apr 2016].
- ²⁰ Beebom, 2015. What is GLONASS And How It Is Different From GPS. [Online] Available at: <http://beebom.com/2015/05/what-is-ghonass-and-how-it-is-different-from-gps> [Accessed 12 Apr 2016].
- ²¹ Hayes, G., 2016 GPS can be jammed and 'spoofed'—just how vulnerable is it? Part 2. Available at <http://www.marineelectronicsjournal.com/content/news/news.asp?show=VIEW&a=129> [Accessed 24 July 2016]

CYBER SECURITY

- ²²Ibid.
- ²³Balduzzi, M., Wilhoit, K. & Pasta, A., 2014. A Security Evaluation of AIS, Texas, USA: Trend Micro.
- ²⁴International Maritime Organisation, 2016. AIS Transponders. [Online] Available at: <http://www.imo.org/en/OurWork/Safety/Navigation/Pages/AIS.aspx> [Accessed 12 Apr 2016].
- ²⁵HM Government, 2014. Mapping UK shipping density and routes from AIS (MMO 1066). [Online] Available at: <https://www.gov.uk/government/publications/mapping-uk-shipping-density-and-routes-from-ais-mmo-1066> [Accessed 12 Apr 2016].
- ²⁶Maritime and Coastguard Agency, 2014. Dover Strait crossings: channel navigation information service (CNIS). [Online] Available at: <https://www.gov.uk/government/publications/dover-strait-crossings-channel-navigation-information-service/dover-strait-crossings-channel-navigation-information-service-cnis#how-cnis-works> [Accessed 12 Apr 2016].
- ²⁷Vessel Finder, 2016. Real-Time AIS Data. [Online] Available at: <https://www.vesselfinder.com/> [Accessed 12 Apr 2016].
- ²⁸Balduzzi, M., Wilhoit, K. & Pasta, A., 2014. A Security Evaluation of AIS, Texas, USA: Trend Micro.
- ²⁹Marine Source, 2016. Satellite AIS Data. [Online] Available at: <http://www.marinetraffic.com/en/p/satellite-ais> [Accessed 12 Apr 2016].
- ³⁰Inmarsat, 2016. Fleet Broadband. [Online] Available at: <http://www.inmarsat.com/service-collection/fleetbroadband/> [Accessed 12 Apr 2013].
- ³¹Thuraya, 2016. Marine Comms. [Online] Available at: <http://www.thuraya.com/marine-comms> [Accessed 12 Apr 2016].
- ³²Santamarta, R., 2014. A wake-up call for SATCOM Security. [Online] Available at: http://www.ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf [Accessed 23 July 2016].
- ³³Encyclopaedia Britannica, 2016. Transmission media and the problem of signal degradation. [Online] Available at: <http://www.britannica.com/topic/telecommunications-media> [Accessed 12 Apr 2016].
- ³⁴Computernetwor (Balduzzi, et al., 2014)kingsimplified.com. Relationship between Bandwidth, Data Rate and Channel Capacity. [Online] Available at: <http://computernetworkingsimplified.com/physical-layer/relationship-bandwidth-data-rate-channel-capacity/> [Accessed 12 Apr 2016].
- ³⁵Sailcom Marine, 2016. HF shortwave SSB radio email systems. [Online] Available at: <http://www.sailcom.co.uk/pactor/> [Accessed 12 Apr 2016].
- ³⁶yachtcom, 2016. Long Distance Communications Made Clear and Simple. [Online] Available at: <http://info.yachtcom.co.uk/HF/> [Accessed 12 Apr 2016].
- ³⁷Isode, 2016. Why IP over HF Radio should be Avoided. [Online] Available at: <http://www.isode.com/whitepapers/ip-over-stanag-5066.html> [Accessed 12 Apr 2016].
- ³⁸Business Insider Science, 2015. Animated map shows the undersea cables that power the internet. [Online] Available at: <https://www.youtube.com/watch?v=IIAJJ-qG2k> [Accessed 12 Apr 2016].
- ³⁹Starosielski, N., 2015. The Undersea Network. 1st ed. Durham and London: Duke. p.1
- ⁴⁰Business Insider Science, 2015. Animated map shows the undersea cables that power the internet. [Online] Available at: <https://www.youtube.com/watch?v=IIAJJ-qG2k> [Accessed 12 Apr 2016].
- ⁴¹Starosielski, N., 2015. The Undersea Network. 1st ed. Durham and London: Duke.p.31
- ⁴²Blum, A., 2012. Tubes - Behind the scenes at the Internet. 1st ed. London: Penguin. p.194
- ⁴³Starosielski, N., 2015. The Undersea Network. 1st ed. Durham and London: Duke.p.9
- ⁴⁴<http://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/>
- ⁴⁵Sanger, D. E. & Schmitt, E., 2015. Russian Ships Near Data Cables Are Too Close for U.S. Comfort. The New York Times, 26 October, p. A1.
- ⁴⁶Fung, B. & Peterson, A., 2016. America uses stealthy submarines to hack other countries' systems. [Online] Available at: <https://www.washingtonpost.com/news/the-switch/wp/2016/07/29/america-is-hacking-other-countries-with-stealthy-submarines/> [Accessed 4 August 2016].
- ⁴⁷Venables, A., 2016. Protecting Ships - The Threat of Hackers. Port Technology, 69 Edition, pp. 30-31.
- ⁴⁸BIMCO, CLIA, ICS, INTERCARGO, INTERTANKO, 2016. The Guidelines for Cyber Security Onboard Ships, Bagsvaerd: BIMCO.

Adrian Venables
PhD Student at Lancaster University
Commander UK Royal Naval Reserve



Adrian served in the Royal Navy as a Communications, Warfare and Intelligence officer for 24 years responsible for the provision and security of a range of services worldwide, including the management of specialist teams deployed to operational theatres. Since leaving the Service, he has extensively studied the cyber threat landscape and how the Internet is used by malevolent parties and for the projection of power and influence by state and non-state actors. A Certified Information Systems Security Professional, he has worked for both government and industry clients advising on computer security with a particular interest in education and training as a method of countering the cyber threat. He is a frequent visiting speaker on both military and university courses in which he aims to raise awareness of the techniques used by cyber criminals and of the need to improve personal security online. A firm believer in Continuous Professional Development, Adrian has undertaken an uninterrupted programme of academic study over the past 14 years and is currently studying for a PhD at Lancaster University in the UK where he is researching the relationship between the maritime and cyber environments in the projection of cyberpower. In addition to his current academic research programme he holds two Bachelor of Science degrees with Honours in Computing and Information Technology and Intelligence and Security and four Masters Degrees in the Design of Information Systems, Business and Computer Studies, Technology (Maritime Operations) and Cyber Security. He is also a Chartered Information Technology Professional Fellow of the British Computing Society, Chartered Engineer Member of the Institution of Engineering Technology and Fellow of the Chartered Management Institute.



HOLISTIC PROTECTION OF CRITICAL INFRASTRUCTURES

Resilience and protection of dependencies between Greek Critical Infrastructures

- *George Stergiopoulos*
Senior Researcher
INFOSEC Laboratory
Athens Univ. of Economics & Business
- *Dimitris Gritzalis*
Professor & Associate Rector
INFOSEC Laboratory
Athens Univ. of Economics & Business
- *Panayiotis Kotzanikolaou*
Assistant Professor
University of Piraeus, Greece

- *Manos Magkos*
Associate Professor
Ionion University, Greece
- *Georgia Lykou*
Researcher
INFOSEC Laboratory
Athens Univ. of Economics & Business

INTRODUCTION

The protection of Critical Infrastructures (CIs) is, by definition, of high importance for the welfare of citizens

of each country; especially nowadays, both because of direct threats (dictated by the current international political situation) and also due to emerging interactions or dependencies developed

between national CIs at international and European levels.

Today, Greece remains one of the few countries of the European Union, which (besides the formal transposi-

ENERGY INFRASTRUCTURES SECURITY

tion of the 114/2008/EC Directive into domestic legislation) has no comprehensive strategy to safeguard national CIs, nor any process of developing such an integrated plan, except for some initiatives taken from the General Secretariat of Digital Policy.

Basic goals

1. The initial creation of an inventory and corresponding assessment of existing national CIs along with their supervised entities to identify critical services, their dependencies and security measures to be applied to adequately protect and increase their resilience against known or unknown threats.
2. The Risk Assessment of services and interdependencies between candidate national CIs using an appropriate, new methodology for the classification of national critical components. The methodology will be able to assess the degree of impact from potential threat manifestation, with a view to prioritization and implementation of appropriate security measures for all national CIs. Objectives of this project do not include the full and comprehensive coverage and assessment of all CIs in the country, nor the proposal of a detailed security policy for each CI. This would not be feasible in the context of an independent study, since the complete recording and evaluation of all CIs nationwide requires an authorized body with the institutional and legal feasibility of collecting and processing classified information along with the cooperation of all national CI operators. However, this systematic recording and evaluation of Greek CIs can act as a catalyst for conducting such an indepth, which should be developed in the context of registration and evalua-

tion of European Critical Infrastructure.

Contribution

1. The creation of an inventory of all stakeholders, i.e. actors who have some form of power (legislative, supervisory or regulatory) to protect CIs in Greece.
2. The identification and indicative cataloguing of potential national CIs, as well as their interdependencies. In particular, an attempt is made to record national CIs on the Energy, Transport and Information and Communication Technologies (ICT) sectors.
3. The development of a structured identification and risk assessment methodology of national CIs, taking into account internationally applied CI assessment methodologies. A range of three evaluation levels (criticality), and specific evaluation criteria for the integration of critical components in criticality levels will also be developed and utilized, as part of the proposed methodology.
4. The pilot implementation of the proposed methodology to a list of candidate national CI fields in order to rank their Criticality; namely on the Energy and ICT sectors.

Preliminary record of Greek Critical Infrastructures

The identification and evaluation of national CIs first requires the creation of an initial list of potential CIs, at sector and subsector levels. In this section, the services of three key critical areas of the country are being mapped; namely those concerning the Energy, Transport and Information and Communications Technologies (ICT) sectors.

Compilation of a National Protection Program for Critical Infrastructures

As part of a national CI protection program, each EU Member-State is required to (i) record its National Critical Areas, (ii) record and evaluate the systems or parts thereof which may constitute a CI, and (iii) to record and evaluate (possible) interdependencies between detected CIs. Also, each nation has to plan and/or update a Business Continuity Plan (BCP) and a Contingency Plan (CP) for the protection of national CIs (Directive 114/2008).

Since, in most cases, the owners (operators) and/or operators of CIs are private entities, any national CI identification process (along with all processes in the context of a national protection program) requires the exchange of information between stakeholders, in accordance with the principle of collaboration between stakeholders and the public-private partnership (public-private partnership, PPP).

During the stage of critical area identification, each Member State must establish an initial list of critical national sectors, i.e. sectors existing in the geographical limits of the country that include contingent CIs. Still, the process of selecting national critical sectors and sub-sectors is not obvious.

Towards creating a common framework program for the EPCIP (European Programme for Critical Infrastructure Protection) the establishment of a common list of critical sectors/subsectors is highly encouraged. The concept of service is often used by implication instead of the term infrastructure, since it integrates the existence of a set of goods and processes that need protection in both abstract and descriptive

ENERGY INFRASTRUCTURES SECURITY

levels. The list of CIs is presented in Table 1 and incorporates the concept of service per subsector.

In order to identify candidate Greek CIs, a brief overview of the Critical Sectors reported in Table 1 was held and specific areas were selected which we believe are more significant for the country. Some potential critical services were removed due to non-conformity with the Greece (e.g. Space sector) while others were added due to their potentially high impact on Greece's GDP, like Touristic services. Based on the collection of public information and scientific expertise of the panel members, the following critical areas were selected for our study: (a) Energy (b) Information and Communications Technologies (ICT) and (c) Transport.

Energy sector

In Greece, multiple providers support various sub-sectors of the Energy sector. In some subsectors, only one provider (or a very small number of them) has a dominant position, making him the obvious choice for a CI at the Energy sector. Still, some changes have occurred in the Energy market of other subsectors over the last years; usually because of Greece's need to comply with the relevant European Directives, but also due to the economic situation of the country.

ICT sector

The Information and Telecommunication Technologies (ICT sector) is a sector of high criticality since it provides information assets and services to almost all other critical services in the country. Of all the Information

Technologies and Communications subsectors, it appears that the Telecommunication subsector is the most important in Greece. Hardcore centralization of services is observed at the Greek ICT sector, although for some services there seems to be a more balanced distribution of providers. This leads us to believe that several provid-

ers are candidate for being a Greek CI in this sector.

Transportation Sector

The transport sector provides services to multiple other sectors and supports numerous economic activities such as trading, tourism, industry, rural devel-

Sector	Subsector	Service
1. Energy	Electricity	- Production (p1 sector) - Electricity output - Transportation / Distribution
	Oil	- Mining - Transfer - Refining - Sale
	Natural gas	- Mining - Storage - Transportation / Distribution
2. Information and Communications Technologies (ICT)	Information technologies	- ICL Services - Computer Networks / Services Cloud - Software as a Service (SaaS) - Communications Tools / Data
	Communications	- Internet
3. Water	Drinking water	- Water storage - Water Quality Assurance - Water distribution
	Effluent	- Collection and treatment of sewage
4. Food and Beverages		- Agriculture / Food production - Food Supply - Food distribution - Quality / Food safety
5. Health		- Hospital care - Hospital care - Supply of medicines, vaccines, blood, medical supplies - Control of infectious and epidemics
6. Economy		- Banking - Stock trading - Payment transactions
7. Public Order & Security		- Maintenance of public order - Poison system
8. Transportation	Aviation	- Air Navigation Services - Airport Operation
	Road Transport	- Services Bus / Train - Road Maintenance
	Rail Transport	- railway network management - Railway services
	Shipping	Navigation Control - Cruise Coastal Interconnection
	World Transport	- Transport documents & parcels - Payment Transactions
9. Industry	Chemical/Industrial	- Supply supplies - Storage and disposal of hazardous materials - Insurance of industrial high risk units
	Tourism	Hotel supplies Restaurant supplies
	Agriculture	Agricultural Input Supply Other supply services
10. Public Administration		- Governmental functions
12. Civil Protection		- Fire and Rescue Services
13. Environment		- Monitoring and air pollution control - WASTE TREATMENT AND WASTE - Monitoring and control of ground water - Monitoring and control of marine pollution
	14. Defense	- National Defense

Table 1. The list of potential CIs, sectors and relevant subsectors specifically for Greece

ENERGY INFRASTRUCTURES SECURITY

opment and the exploitation of natural resources of Greece. The sector is subdivided into sub-Rail, Road, Sea and Air transports along with postal services.

Conclusions from mapping these three fundamental CI sectors of our country are presented in Table 2. The table summarizes infrastructures in the

above areas. The table structure contains critical domains, subdomains for each critical service, the key subsystems that are necessary for providing each service, the essential interdependencies with other (sub) sectors, as well as an indicative inventory of the providers of each service involved in the country.

Method for determining and evaluating national Critical Infrastructures

This chapter describes a methodology for identifying and evaluating national HQ, structured as a sequence of steps. Each step provides a brief description, the data (or parameters) input neces-

Critical Subsector	Critical Service	Interdependencies		Main Stakeholders
		Depends upon	Affects	
Electricity	AC/DC Production	Mining of Lignite General Transfer Oil Transfer	All sectors	Public Power Corporation Alternative Producers
	Transportation/storage	Production		ADME
	E. Energy Market	Production Distribution		Public Power Corporation Alternative Producers
Oil	Mining	Refinement Transport Storage	Industry Business Farming Transportation	Energy Oil & Gas
	Refinement	Transport Storage		ELPE Motoroil
	Transport	Shipping Internal Relations		ELPE Shipping Sector
	Storage	Oil Transfer		ELPE Motoroil
Natural Gas	Transportation / Distribution	Cross-Border Interconnections External Relations	Industry Domestic use	Public Gas Corp. (Tap) (Under Construction)
	Storage	Transport / Distribution External Relations		Public Gas Corp. (Log Revithousa)
Telecommunications	Voice / Data Communications	Power Supply Internet Access External Links Voice/Data	All sectors	OTE Vodafone Wind Forthnet Cyta
	Internet access	Communications External Links		
Information Technologies	Data Centers / Cloud Services	Power Supply Providing Telecommunications Internet Access Tel/Stan on External Links	Economy Business Industry	Med Nautilus Landa Hdik Lancom OTE
	Web services	Power Supply Providing Telecommunications Internet Access ICT Connections Abroad	Economy Business	Telecommunications Providers Small Providers

Table 2. Summary of the Energy, Transportation and ICT sectors in Greece

ENERGY INFRASTRUCTURES SECURITY

sary for the execution, implementation actions needed and expected results. Categories of criteria for the integration of candidate CIs were defined inside the methodology. These include direct assessment criteria, time criteria and indirect criteria of importance to CIs. Direct evaluation criteria are based on the assessment of potential

impact (impactbased classification) that are expected to manifest after an attack on relevant infrastructures. Time criteria (estimate recovery time, impact event time estimate) are used for prioritizing CIs within each Risk level. Indirect criteria take into account, amongst others, the number and importance of interdependencies

between CIs, as well as time criteria. The analysis of interdependencies between CIs can identify CIs that might have been underestimated during previous analysis. Then, each subsystem gets a criticality assessment and sectorial and horizontal criteria are utilized for the identification of that subsystem as a possible

Critical Subsector	Critical Service	Interdependencies		Main Stakeholders
		Depends upon	Affects	
Road Transport	Motorways, National And Provincial Roads	Availability Of Oil Ict Systems Interoperability Infrastructure Environment & Weather	Provision of Road Transport Social & Economic Growth	ΥΠΟΜΕΤΕΧ Technical And Contractors (Companies)
	Provision Of Road Passenger Transport And Cargo	Motorways, National And Provincial Roads Availability Of Oil Road Signage Environment & Weather	Trade Government Agencies Business Industry Farming Sector	Transport National And International Transport Companies Private Owners Of Means Of Transport OASA OASTH Buses (KTEL)
Shipping	Ports And Port Infrastructures	Availability ICT Systems Interoperability Infrastructure Environment & Weather	Providing Ferry Transport Trade Industry, Enterprises, Farming Sector	ΥΠΟΜΕΤΕΧ YEN OLP OLTH COSCO
	Coastal Transport & Transportation	Port Infrastructure Availability Of Mineral Resources & Energy Marine Signaling System ICT Systems Environment & Weather	Tourism, Trade Industry, Enterprises, Farming Sector	Ferry Operators Transport Companies Tourist Companies
Air	Airports And Airport Infrastructure	Availability ICT Systems Interoperability Infrastructure Environment & Weather	Provision Of Aviation Tourism	YPA DAA TAIPED
	Air Transport	Availability Petroleum System Radar Air Navigation Services ICT Systems Environment & Weather	Tourism, Trade, Government Agencies	YPA AIRLINES EUROCONTROL
Rail Transport	Network Rail Infrastructure	Communications Systems & Information	Trade Industry	CSE ERGOSE GALAXE
	Rail Transport	Rail Infrastructure Network Energy Availability Ict Systems Interoperability Infrastructure	Trade Industry Business Farming Sector Tourism	TRAINOSE STASY AMEL TRAM SA

Table 3. Summary of the Energy, Transportation and ICT sectors in Greece

ENERGY INFRASTRUCTURES SECURITY

CI.

The methodology does not take into account threats (threats or scenarios), nor does it assess them according to their likelihood. Threat analysis, together with indicative threat scenarios will be described later on as part of a protective strategy for all CIs.

STEP 1: Initial list of critical sectors and subsectors.

Short description. In the first step an initial list of potential national critical sectors and subsectors per sector is catalogued. Sectors and subsectors from the list of services offered in Table 1 are used as input.

Implementation. Cataloguing of the initial sectors/-subsectors list is performed by a central authority. Typically, this can be coordinated by the respective competent body for the protection of national CIs.

Results. The initial list of critical sectors/subsectors will be given as input to Step 2 and Step 3.

STEP 2: Identify potential critical services per sector/subsector

Short description. For each critical area, potential critical services are identified. The list compiled from Step 1 can be considered as initial parameter in the process of identifying potential critical services per sector/sub-sector, along with good-practices from EU members which are mature enough when it comes to implementing strategies for the protection of national CIs.

Implementation. There are two

alternative approaches that can be followed to identify possible national critical services sector/subsector:

Administrative Approach. A list of potential national critical sector services is compiled at a central, administrative level, in cooperation with a competent Authority. Alternatively, a list of national critical services is compiled across sectors. According to this approach, a Critical Managers list is compiled (according to relevant legal frameworks). Managers will be responsible to identify critical services that are involved in.

Results. The list of critical services sector/subsector will be given as input to Step 3 for the risk assessment of possible critical services per sub-sector.

STEP 3: Evaluation of potential critical services

Short description. Possible critical elements from previous steps (sub-sector and/or services by sub-sector) are assessed and prioritized using specific criteria. Initial parameters that can be considered for the evaluation of potential critical subsectors/services are:

- The initial list of possible critical Sectors/Subsectors from Step 1.
- The initial list of potential critical services from Step 2 (this list may include the list from Step 1).
- The non-binding guidelines

of the European Council on the implementation of the horizontal criteria during the evaluation of CIs.

- Good practices from EU members.

Implementation. Depending on the approach taken during Step 2 (Administrative approach or owner-manager driven approach), the following checks are applied, either at central level or in collaboration with Critical Administrators:

Step 3.1. Direct criticality rating. All potential critical services are assessed, based on the immediate consequences that would result from their breach or failure. This is achieved by applying selected horizontal criteria, from the following list:

- Geographic scope: The scope of the area to be affected by an event.
- Human losses: The number of victims and/or injured people.
- Economic impact: The impact in a macro and/or macro-social level.
- Environmental impact: Long-term environmental effects.
- Consequences for the public: Impact of events affecting the people, which does not directly relate to any of the previous criteria.

Step 3.2. Temporal effects analysis. The following are evaluated for each critical service: (a) the time required for the manifestation of maximum impact and (b) the time required to fully restore a service after a possible

ENERGY INFRASTRUCTURES SECURITY

attack manifestation.

Time analysis is used for the classification of critical services within each level of criticality as a criterion for assessing indirect criticality (Step 3.3).

Step 3.3. Indirect criticality rating. Any possible critical service is also analyzed based on the indirect effects that can cause during a failure scenario. Indirect effects depend on two factors:

- Dependencies of the service in question with other critical services.
- The required time needed for maximum impact realization and restoration of the specific service (Step 3.2).

Evaluation of indirect criticality is performed by utilizing one or more horizontal criteria, from Step 3.1.

Results. The list of prioritized sub-sectors and services per sub-sector, as well as a table of interdependencies between sub-sectors/services will be provided as input to Step 4, to assess the criticality of (sub) systems per critical service. This step determines a list of possible European critical sectors/subsectors or services. For each horizontal criterion to be applied, criticality levels are described using a quality scale (e.g. Low, Medium, High). For each level, a minimum quantitative impact threshold is set.

STEP 4: Evaluating Critical (sub) systems per service.

Short description. For each critical

service, a list of involved owners-managers is compiled, from which (or in collaboration with whom) a second list of the most critical subsystems that support this service is compiled.

Implementation. According to the approach proposed by the EPCIP framework (EU Council, 2008; 2008b), certain criteria must be applied at each sub-sector for the characterization of a subsystem as a possible CI inside a service (Step 4.1). This is to check whether a subsystem meets at least one horizontal criticality criterion (Step 4.2).

Results. This step provides a list of the most critical subsystems per service. This is a list of national CIs, according to the 114/2008/EC Directive. As part of a National CI Protection Program, CI owners-managers in collaboration with a qualified national body must identify the most important assets per critical subsystem and develop Operation Security Plans (OSP) and Contingency Plans (CP) to protect the CIs (Annex II - 114/2008 /EC Directive).

Step 4.1: Sectoral Application Criteria: Sectoral criteria are technical or operational criteria used to identify potential critical subsystems. These criteria do not report, although hint, potential repercussions (e.g. obstruction or shutdown of a subsystem). Instead, they only refer to certain inherent characteristics. In particular, the sectoral criteria may refer to (EU

Council 2008b):

- Technical properties. For example, quantifiable characteristics, such as dimensions, capacities, distances, speed, data volume, etc.
- Nontechnical properties. For example, identifiable features such as recovery time, recovery costs etc.

To identify a subsystem as potentially critical, it should exceed a predetermined threshold (threshold) concerning the values of some sectoral criteria.

Step 4.2: Application of Horizontal Criteria: For each subsystem that provides essential services, we assess the severity that its loss or dysfunction would have on society. A subsystem is critical when it meets at least one of the horizontal criticality criteria, concerning the direct (Step 3.1) or indirect criticality (Step 3.2).

Also, criticality evaluation takes into account parameters such as the availability of alternatives, the turning-point for "painful" consequences, as well as the time needed for recovery.

STEP 5: Periodic reassessment of critical infrastructure

Short description. All critical and relevant factors concerning the criticality of a CI and relevant services should be reassessed after some time by applying all steps of the methodology at regular

ENERGY INFRASTRUCTURES SECURITY

intervals.

Input data. All results of the previous evaluation of critical components (sectors, sub-sectors, services, systems).

Implementation. The reassessment may be general (step 1, taking into account the previous critical services list), or may refer to a particular sector/subsector (step 3) or service (step 4). The reassessment scope is determined by a qualified body in collaboration with stakeholders. The need for reassessment should be determined on a mid-term basis; the period must be fixed in advance, regardless of whether changes in the collected data occur or not.

Results. The amended list of critical elements and CIs or the update of the previous assessment of critical components (domains, subdomains, services and systems).

Applying evaluation criteria on candidate national CIs

After establishing all parameters for evaluating potential CIs, the description of the national CI assessment methodology is complete and will now be applied to the Greek Energy and ICT sectors. It should be noted here that during the implementation of the horizontal evaluation criteria, the estimated impact always refers to the worst-case scenario. Therefore, when analyzing potential impact values listed in the tables below, the value attributed to each impact

corresponds to the most negative potential effect that is likely to occur. Also when we applied the criteria, there happened to be some cases where the assessment could not get unique value assignments, thus values were assigned on the 1-2 impact scale. When a qualified national body implements a full version of the above methodology, every service criterion should be assigned only one scale value.

Evaluation of the Energy Sector

The Energy Sector includes the following sub-sectors: Electricity, Oil and Natural Gas. Table 4, 5 and 6 summarize the evaluation of each sub-sector and key dependencies recorded, incoming and outgoing, by sub-sector.

Based on the application of the evaluation criteria and taking into account the record from providers/operators per service, our evaluation provided the following:

- In the Electricity sub-sector all services are assessed as high criticality, both for direct and indirect dependencies. To a large extent, they also depend on only one provider/IM (PPC).

- Concerning the temporal analysis of impact, the Production and Distribution services have higher priority than the electricity market service, as far as recovery time is concerned.

- At the subsystems level, all subsystems used to support this

sector's services must be tested using corresponding sectoral criteria.

Evaluation of the ICT sector

The ICT sector includes the Telecommunications and Information Technologies subsectors. Table 7 presents the evaluation of these subsectors.

Based on the application of the evaluation criteria and taking into account the record from providers/operators per service, our evaluation provided the following:

- The Communications sub-sector has increased impact in Greece. All services showed that they are of high criticality, both in direct and in indirect evaluations of dependencies. The Communications sub-sector services depend to a large extent, from a single provider (OTE).

- Concerning the temporal analysis of impact, impact analysis shows that both the voice/data communication services and the provision of Internet services present fast impact effects but rapid recovery times, thus fall within the same priority level recovery.

ENERGY INFRASTRUCTURES SECURITY

	Direct Assessment (horizontal Criteria)					Time Criteria		Indirect Assessment (due to dependencies)
	Geographical width	Economic Loss	Human Casualties	Environmental Consequences	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Services								
Production of Electrical Power	Territory	Important % of GNP	Potential Loss in case of accident	Potential consequences in case of accident	Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery	Affects most CIs	
	LEVEL 3	LEVEL 3	LEVEL 1	LEVEL 1	LEVEL 3	CATEGORY 3	LEVEL 3	
Transmission / Distribution of Electrical Power	Territory	Important % of GNP	Potential Loss due to impact on Health Sector		Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery	Affects most CIs	
	LEVEL 3	LEVEL 3	LEVEL 1		LEVEL 3	CATEGORY 3	LEVEL 3	
Electrical Power Market	Territory	Important % of GNP			Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery	Affects most CIs	
	LEVEL 3	LEVEL 3			LEVEL 3	CATEGORY 2	LEVEL 3	

Table 4 Application of Criteria - Electricity Subsector

	Direct Assessment (horizontal Criteria)					Time Criteria		Indirect Assessment (due to dependencies)
	Geographical width	Economic Loss	Human Casualties	Environmental Consequences	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Services								
Oil Refraction			May cause loss of life	Severe consequences				
			LEVEL 1	LEVEL 1 or LEVEL 2				
Oil Refinement	Territory	Important % of GNP	May cause loss of life	Severe consequences	Effect on the lives of million citizens	Slow consequence manifestation Slow recovery	Affects most CIs	
	LEVEL 3	LEVEL 3	LEVEL 1	LEVEL 1 or LEVEL 2	LEVEL 3	CATEGORY 2	LEVEL 3	
Oil Transportation	Territory	Important % of GNP	May cause loss of life	Severe consequences	Effect on the lives of million citizens	Slow consequence manifestation Slow recovery	Affects most CIs	
	LEVEL 3	LEVEL 3	LEVEL 1	LEVEL 1 or LEVEL 2	LEVEL 3	CATEGORY 2	LEVEL 3	
Oil Storage	Territory	Important % of GNP	May cause loss of life	Severe consequences	Effect on the lives of million citizens	Slow consequence manifestation Slow recovery	Affects most CIs	
	LEVEL 3	LEVEL 3	LEVEL 1 or LEVEL 2	LEVEL 1 or LEVEL 2	LEVEL 3	CATEGORY 2	LEVEL 3	

Table 5 Application of Criteria - Oil Subsector

ENERGY INFRASTRUCTURES SECURITY

	Direct Assessment (horizontal Criteria)					Time Criteria		Indirect Assessment (due to dependencies)
	Geographical width	Economic Loss	Human Casualties	Environmental Consequences	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Services								
Transportation & Distribution of Natural Gas	Territory	Important % of GNP	Potential Loss in case of accident	Low consequences	Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery	Affects > 2 Cls (Industry, Electricity Production)	
	LEVEL 3	LEVEL 3 or LEVEL 2	LEVEL 1 or LEVEL 2	LEVEL 1 or LEVEL 0	LEVEL 3	CATEGORY 3	LEVEL 3	
Natural Gas Storage	Territory	Important % of GNP	Potential Loss due to impact on Health Sector	Low consequences	Effect on the lives of million citizens	Rapid consequence manifestation Slow recovery	Affects > 2 Cls (Industry, Electricity Production)	
	LEVEL 3	LEVEL 3 or LEVEL 2	LEVEL 1 or LEVEL 2	LEVEL 1 or LEVEL 0	LEVEL 3	CATEGORY 2	LEVEL 3	

Table 6 Application of Criteria - Natural Gas Subsector

	Direct Assessment (horizontal Criteria)					Time Criteria		Indirect Assessment (Due to dependencies)
	Geographical width	Economic Loss	Human Casualties	Environmental Consequences	Consequences to the Public	Time of consequence manifestation	Recovery Time	
Services								
Voice/Data communication services	Territory	Important % of GNP	Potential Loss due to impact on Health Sector	-	Effect on the lives of million citizens	Rapid consequence manifestation Rapid recovery	Affects most Cls	
	LEVEL 3	LEVEL 3 or LEVEL 2	LEVEL 1	-	LEVEL 3	CATEGORY 2	LEVEL 3	
Internet Provision	Territory	Important % of GNP	Potential Loss due to impact on Health Sector	-	Effect on the lives of million citizens	Rapid consequence manifestation Rapid recovery	Affects most Cls	
	LEVEL 3	LEVEL 3 or LEVEL 2	LEVEL 1	-	LEVEL 3	CATEGORY 2	LEVEL 3	

Table 7 Application of Criteria - Telecommunications Subsector

ENERGY INFRASTRUCTURES SECURITY

References

- EU Commission (2006). Communication from the Commission on a European Programme for Critical Infrastructure Protection COM (2006) 786 final. Retrieved from:
- EU Commission (2010). European Commission, Europe 2020. A strategy for smart, sustainable and inclusive growth, COM (2010) 2020, Brussels 3.3.2010.
- EU Commission (2012). European Commission, staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP), Brussels. Retrieved from:
- EU Commission (2013). European Commission, staff working document on a new approach to the European Programme for Critical Infrastructure Protection making European Critical Infrastructures more secure), Brussels, Belgium. Retrieved from:
- EU Commission (2013b). European Commission, Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, COM(2013) 48 final. http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1666
- EU Commission 149 (2009). European Commission. "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". Com(2009) 149 final,
- EU Council (2007). Council of the European Union, Adoption of the Council Conclusions on a European Programme for Critical Infrastructure Protection. Retrieved from:
- EU Council (2008b). Council of the European Union, Non-Binding Guidelines for the application of the Directive on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection, Brussels [14808/08]. Retrieved from:
- EU Council (2008c). Proposal for a COUNCIL DECISION on a Critical Infrastructure Warning Information Network (CIWIN). COM(2008) 676 final. Available from: [http://ccpic.mai.gov.ro/docs/COM\(2008\)676_final_CIWIN_EN.pdf](http://ccpic.mai.gov.ro/docs/COM(2008)676_final_CIWIN_EN.pdf)
- Faily S., Lykou G., Partridge A., Gritzalis D., Mylonas A., Katos V., "Human-Centered Specification Exemplars for Critical Infrastructure Environments", in Proc. of the 30th British Human Computer Interaction Conference (HCI-2016), July 2016.
- Faily S., Stergiopoulos G., Katos V., Gritzalis D., "Water, water, everywhere: Nuances for a Water Industry Critical Infrastructure specification exemplar", in Proc. of the 10th International Conference on Critical Infrastructures Security (CRITIS-2015), pp. 243-246, Springer (LNCS 9578), Germany, October 2015.
- FC (2009). Federal Council's Basic Strategy for Critical Infrastructure Protection, Basis for the national critical infrastructure protection strategy. Confédération Suisse, 18 May, 2009. <http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski.parsysrelated1.82246.downloadList.42043.DownloadFile.tmp/grundstrategieski20090518e.pdf>
- FC (2009b). Critical Infrastructure Protection - Second Report to the Federal Council and Measures for the Period 2009–2011. Federal Office for Civil Protection, 18 May, 2009. http://www.bevoelkerungsschutz.admin.ch/internet/bs/en/home/themen/ski/publikationen_ski.parsys.60516.downloadList.59025.DownloadFile.tmp/2berichtski20090605e.pdf
- French Strategy (2015). French national digital security strategy. French Republic, 2015. From:
- FRG (2009). National Strategy for Critical Infrastructure Protection (CIP Strategy). Federal Ministry of the Interior, Federal Republic of Germany. Berlin, June 17, 2009.
- Klaver, M. H. A., Luijff, H. A. M., & Nieuwenhuijsen, A. H. (2011). RECIPE: Good practices manual for CIP policies, for policy makers in Europe. Available from: http://www.oaip.ac.at/fileadmin/Unterlagen/Publikationen/FINAL_RECIPe_manual.pdf
- Kotzanikolaou P., Theocharidou M., Gritzalis D., "Assessing n-order dependencies between critical infrastructures", International Journal of Critical Infrastructure Protection, Vol. 9, Nos. 1-2, pp. 93-110, 2013.
- Kotzanikolaou P., Theocharidou M., Gritzalis D., "Cascading effects of common-cause failures on Critical Infrastructures, in Proc. of the 7th IFIP International Conference on Critical Infrastructure Protection (CIP-2013), pp. 171-182, Springer (AICT 417), USA, March 2013.
- Kotzanikolaou P., Theocharidou M., Gritzalis D., "Interdependencies between Critical Infrastructures: Analyzing the Risk of Cascading Effects", in Proc. of the 6th International Workshop on Critical Infrastructure Security (CRITIS-2011), pp. 107-118, Springer (LNCS 6983), Switzerland, September 2011.
- Lebau-Marianna, D., & E. Roger (2015). France – three decrees reinforced the safety obligations of Operators of Vital Importance. July 8, 2015.
- Livre Blanc (2013). Défense et sécurité nationale, République Française, 2013. From:
- Luijff, E., Burger, H., & Klaver, M. (2003). Critical infrastructure protection in the Netherlands: A Quick-scan. In EICAR Conference Best Paper Proceedings (Vol. 19). EICAR, Denmark.
- MSB (2011). A first step towards a national risk assessment. Swedish Civil Contingencies Agency-MSB, Sweden, 2011. On-line: <https://www.msb.se/RibData/Filer/pdf/26189.pdf>
- MSB (2014). Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure. Swedish Civil Contingencies Agency (MSB), Risk & Vulnerability Reduction Department <https://www.msb.se/RibData/Filer/pdf/27412.pdf>
- Polemi D., Ntouskas T., Georgakakis E., Douligeris C., Theocharidou M., Gritzalis D., "S-Port: Collaborative security management of Port Information Systems", in Proc. of the 4th International Conference on Information, Intelligence, Systems and Applications (IISA-2013), IEEE Press, Greece, July 2013.
- Renda, A., & Hammerli, B. (2010). Protecting critical infrastructure in the EU. CEPS Task Force Report [http://ccpic.mai.gov.ro/docs/Critical Infrastructures Security Task Force Report](http://ccpic.mai.gov.ro/docs/Critical%20Infrastructures%20Security%20Task%20Force%20Report.pdf)

ENERGY INFRASTRUCTURES SECURITY

ture Protection Final A4.pdf

- Salonikias S., Mavridis I., Gritzalis D., "Access control issues in utilizing Fog Computing for Transportation Infrastructures", in Proc. of the 10th International Conference on Critical Infrastructures Security (CRITIS-2015), pp. 1-12, Springer (LNCS 9578), Germany, October 2015.
- Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., "Risk mitigation strategies for Critical Infrastructures based on graph centrality analysis", International Journal of Critical Infrastructure Protection, Vol. 10, pp. 34-44, September 2015.
- Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Gritzalis D., "Using centrality metrics in CI dependency risk graphs for efficient risk mitigation", in Proc. of the 9th IFIP International Conference on Critical Infrastructure Protection (CIP-2015), Springer, USA, March 2015.
- Stergiopoulos G., Kotzanikolaou P., Theocharidou M., Lykou G., Gritzalis D., "Time-base critical infrastructure dependency analysis for large-scale and cross-sectoral failures", International Journal of Critical Infrastructure Protection, Vol. 12, pp. 46-60, March 2016.
- Stergiopoulos G., Vasilellis S., Lykou G., Kotzanikolaou P., Gritzalis D., "Critical Infrastructure Protection tools: Classification and comparison", in Proc. of the 10th International Conference on Critical Infrastructure Protection (CIP-2016), USA, March 2016.
- Theocharidou M., Kandias M., Gritzalis D., "Securing Transportation-Critical Infrastructures: Trends and Perspectives", in Proc. of the 7th IEEE International Conference in Global Security, Safety and Sustainability (ICGS3-2011), pp. 171-178, Springer (LNICST 99), Greece, 2012.
- Theocharidou M., Kotzanikolaou P., Gritzalis D., "A multi-layer criticality assessment methodology based on interdependencies", Computers & Security, Vol. 29, No. 6, pp. 643-658, 2010.
- Theocharidou M., Kotzanikolaou P., Gritzalis D., "Risk assessment methodology for interdependent Critical Infrastructures", International Journal of Risk Assessment and Management, Vol. 15, Nos. 2/3, pp. 128-148, 2011.
- UK (2010). Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards.

George STERGIOPOULOS

Senior Researcher

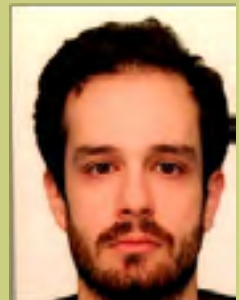
Athens University of Economics & Business, Greece

Dr. George Stergiopoulos (geostergiop@aueb.gr) is a Senior Researcher and a Project Manager with the Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory (www.infosec.aueb.gr) and an Adjunct Lecturer at the Dept. of Informatics of the Athens University of Economics and Business, Greece.

He holds a Ph.D. (Software Security and Critical Infrastructure Protection) and a M.Sc. (Information Systems), both from Athens University of Economics and Business, (Greece), and a B.Sc. (Informatics) from the University of Piraeus (Greece).

His professional experience includes working as Risk Assessment Consultant in projects using ISO-certified methodologies for developing enterprise Security Plans, Business Continuity Plans, and assessing enterprises against IT threats and risks through governance, compliance, identification, and validation. He also works as IT Security Penetration Tester.

His current research interests focus on Critical Infrastructure Protection, Risk Assessment, Application Security and Software Engineering.



Manos MAGKOS

Associate Professor

Ionian University, Greece

Dr. Kotzanikolaou (pkotzani@unipi.gr) is an Assistant Professor in Network Security & Privacy with Dr. Manos Magkos (emagkos@gmail.com) is an Associate Professor with the Dept. of Informatics of the Ionian University, Greece and a Member of the Networks, Multimedia and Security Systems Laboratory (NMSLab) of this department (<http://nmslab.di.ionio.gr>).

He holds a B.Sc. (Computer Science, Univ. of Piraeus, Greece) and a Ph.D. (Computer Security and Cryptography, Univ. of Piraeus, Greece).

His current research focus on Critical Infrastructure Protection, Cyber-Security Training, Privacy-Preserving Data Mining, Location Privacy and Anonymous Authentication.



ENERGY INFRASTRUCTURES SECURITY

Dimitris GRITZALIS

Professor & Associate Rector

Athens University of Economics & Business, Greece

Prof. Gritzalis (dgrit@aueb.gr) is the Associate Rector of Athens University of Economics & Business (Athens, Greece) and a Professor in ICT Security with the Dept. of Informatics. He currently serves as Chairman of the University Research Centre, Director of the Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory (www.infosec.aueb.gr) and Director of the Master's Programme on Information Systems.

Prof. Gritzalis holds a B.Sc. (Mathematics, Univ. of Patras, Greece), a M.Sc. (Computer Science, City University of New York, USA) and a Ph.D. (Information Systems Security, Univ. of the Aegean, Greece).

He has served as Associate Commissioner of the Greek Data Protection Commission and President of the Greek Computer Society. He has provided services, in an Expert's or Evaluator's capacity, for international organizations (ANVUR, CEN, European Union Joint Research Centre, EUROPOL, etc.).

His current research interests focus on Critical Infrastructure Protection, Risk Assessment, Social Media Intelligence and Smartphone Security. He is the Academic Editor of the Computers & Security journal (Elsevier) and the Scientific Editor of the International Journal of Critical Infrastructure Protection (Elsevier).



Panayiotis KOTZANIKOLAOU

Assistant Professor

University of Piraeus, Greece

Dr. Kotzanikolaou (pkotzani@unipi.gr) is an Assistant Professor in Network Security & Privacy with the Dept. of Informatics at the University of Piraeus, Greece. He is, also, a Senior Member of the Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory (www.infosec.aueb.gr) of Athens University of Economics & Business, Greece.

He holds a B.Sc. (Informatics, Univ. of Piraeus, Greece) and a Ph.D. (ICT Security, Univ. of Piraeus, Greece). He holds various professional certifications in Information Security (CISSP, ISO 27001 Lead Auditor).

Dr. Kotzanikolaou has served as a Security Auditor at the Hellenic Authority for the Security and Privacy in Communications (ADAE). He has also worked as a Security Consultant in the private sector, and has participated in various national and European R&D projects.

His current research interests include Security and Privacy in Next Generation Networks, Critical Infrastructure Protection and Applied Cryptography.



Georgia Lykou

Researcher

Athens University of Economics & Business, Greece

Georgia Lykou (lykoug@aueb.gr) is a Researcher and a Ph.D. candidate with the Dept. of Informatics of the Athens University of Economics & Business, Greece, and a Member of the Information Security and Critical Infrastructure Protection (INFOSEC) Laboratory (www.infosec.aueb.gr) of the department.

She holds a B.Sc. (Computer Science, Hellenic Open University, Greece), a B.Sc. (Energy Technology Engineering, TEI of Athens, Greece), a M.Sc. (Information Systems, Athens Univ. of Economics & Business, Greece), and a M.Sc. (MBA, Athens University of Economics & Business, Greece).

She is currently an Engineer with the Hellenic Civil Aviation Authority (HCAA). She has also served as Engineer with the Ministry of National Defence.

Her current research interests focus on ICT Security, Critical Infrastructure Protection and Risk Assessment.





Securing Maritime Logistics and Supply Chain: The Medusa and MITIGATE approaches

• *Dr. Spyridon Papastergiou*

*Dpt. of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 18534 Piraeus, Greece, paps@unipi.gr*

• *Associate Professor Nineta Polemi*

*Director of UNIPI Security Lab, Department of Informatics, University of Piraeus,
Karaoli & Dimitriou 80, 18534 Piraeus, Greece, dpolemi@unipi.gr, dpolemi@gmail.com*

Abstract

During the last couple of years, we have witnessed the emergence of early initiatives that attempt to deal with the risks and vulnerabilities of the Maritime Logistics and Supply Chain

(MLoSC), both in terms of the number of stakeholders and in terms of the complexity and interdependencies of the cyber assets involved. In this paper, the authors present the main outputs and results of two European research projects MEDUSA and MITI-

GATE.

Keywords

Risk Assessment; Maritime Logistics and Supply Chain Services; Critical Information Infrastructures (CIIs).

TECHNOLOGICAL ISSUES

1. Introduction

The Maritime Logistics and Supply Chain (MLoSC) are characterized by significant interdependencies of different types and nature (operational, business, physical, cyber, informational, social, etc.) among the actors (e.g. port authorities, ministries, maritime companies, ship industry, customs agencies, maritime/ insurance companies and other Critical Infrastructures (e.g. transport networks, energy networks, telco networks) involved in these operations in any way. For example, an entity could be dependent on receiving a process or information from another entity or organization as an input to one of its critical business processes. However, if a security-related incident occurs in one entity this may affect the operation of the whole MLoSC.

The main issue is that most of the actors involved in the MLoSC use different risk management methodologies to identify and classify their threats and vulnerabilities and measure the corresponding risks. However, despite the advancement of risk assessment methodologies for Critical Infrastructures (CIs), most available frameworks are limited to the strict corporate and business boundaries without addressing the spectrum of threats and their various cascading effects that are associated with security incidents occurring from interacting entities. Having identified this gap, the Medusa project (medusa.cs.unipi.gr/) focuses on the protection of the port supply chain, in particular, its main objective is to define a methodological approach for the identification and evaluation of multi-order dependencies of security risks,

in the scope of three specific multi-sector cross-border Supply Chain Services (Container Cargo Management Supply Chain, Vehicle Transport Supply Chain and Liquefied Natural Gas (LNG) Transport Supply Chain).

However, maritime of the digital era has become highly dependent on ICT-enabled components to operate. The increasing use of IT systems requires a paradigm shift in the way it assesses risks and vulnerabilities. Most existing risk management methodologies are mostly focused on physical-security aspects ignoring the complex nature of the ICT systems and assets used in the maritime sector (e.g., SCADA), along with their interrelationships. For example MEDUSA approach cannot be considered as an IT oriented risk assessment methodology since it does not support an integrated and effective security management, evaluation and mitigation of IT-based risks; actually it is a supply chain risk assessment methodology at organizational level.

Thus, there is a clear need for rethinking risk management in the MLoSC. To this end, sophisticated global risk assessment frameworks that can deal with cascading effects risks, threats and vulnerabilities of ICT-based maritime supply chain are needed. In this vain, the MITIGATE project (www.mitigateproject.eu/) targets to contribute to the effective protection of the MLoSC that arises from the ICT interconnections and interdependencies of a set of maritime entities. The main goal of MITIGATE is to realize a radical shift in risk management methodologies for the maritime sector towards a collaborative evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA) approach that alleviates the limitations

of state-of-the-art risk management frameworks.

In this paper, the authors will describe the main outputs and results of two European research projects MEDUSA funded under the Security-related Risks Programme of the European Union for the protection of the critical infrastructure and MITIGATE funded under the European programme (H2020) for Cyber security.

2. Medusa methodology and system

The MEDUSA project has introduced a supply chain risk assessment methodology at organisational level comprising of 7 main steps (Step 0: Scope of the SC Risk Assessment, Step 1: Analysis of the SCS, Step 2: Threat Scenario identification, Step 3: Threat Likelihood Analysis, Step 4: Consequence Analysis, Step 5: Risk Assessment and Step 6: Cascading Risk Assessment) that is compliant with ISO28001. The proposed approach aims to assess, for a given a Supply Chain Service (SCS) the partial risk for each business partner, the overall risk for the SCS and the cascading risks for various dependency scenarios, and finally to propose an effective strategy of controls to mitigate those risks that are considered unacceptable.

The MEDUSA methodology is implemented in an innovative, scalable Risk Assessment environment (Fig. 1) which adopts a set of flexible and configurable functions and processes which constitute the fundamental elements for building a solution that facilitates the effective and efficient evaluation of various threat scenarios associated with the MLoSCs as well

TECHNOLOGICAL ISSUES

as the estimation and remediation of their possible consequences.

In order for the proposed system to meet its objectives, it integrates a set of primary components. From a technical perspective, the main components are the following:

- The Risks, Assets and Dependencies Modellers integrates a collection of semantic structures (notably ontologies/taxonomies) to represent the interactions, interrelations and dependencies in the key issues, factors, indicators required for the modeling and execution of risk management scenarios. In particular, this module implements algorithms for identifying and modelling the multi-order dependencies of the different business partners (CII and maritime entities etc.), in the scope of multi-sector cross-border scenarios.

- The Impact Analysis and Visualization Tools embodies mechanisms, procedures and interfaces to provide an in-depth and accurate diagnostic of various threat scenarios and security events related to the examined Supply Chain Services. These tools incorporate methods, algorithms, standards and technologies for enumerating, describing, measuring/quantifying, and encapsulating data required by an integrated risk analysis process (such as threats identification, estimation of impact, evaluation of threats and determination of the corresponding risks).

In addition, these tools provide the means for a quick and visual reference to risk values. In particular, they provide a visualization approach for visually browsing the analysis results and identifying threat scenarios that are applicable to various parts of the SCSs. The visualizations are based

on treemaps, graphs, histograms, etc., which greatly facilitate the exploration and identification of the relevant threats and risks.

- The Simulation Environment incorporates a set of ICT tool that undertake the responsibility to design and execute risks and threats simulation experiments that facilitate the analysis, assessment and mitigation of various threats and risks associated with the examined SCSs. The supported functionalities of this component provide access to the simulation results for further analysis and use, as well as for the formulation of effective mitigation plans.

The aforementioned components are provided through customized intuitive and interactive Web Interfaces (including interactive screens, online forms, Dynamic Questionnaires) to represent the scenarios and steps as well as the information and content (e.g. requirements, rules, obligations, and recommendations of the standardization framework and regime) required by the supported risk assessment routines and functions.

The MEDUSA methodology and system has been tested and evaluated by a large number of Supply Chain stakeholders as well as individuals (such as Port operators, Ports' Security Officers, government officials, leading experts from the Maritime, Oil and Gas sector, IT professionals and Security and risk management experts) engaged in the process of evaluating the capacity of the Medusa methodology and system (<http://medusascsra.cs.unipi.gr/>) to meet their objectives.

In particular, more than 400 port operators, government officials, leading experts from the Maritime, Oil and Gas sector and IT security profession-

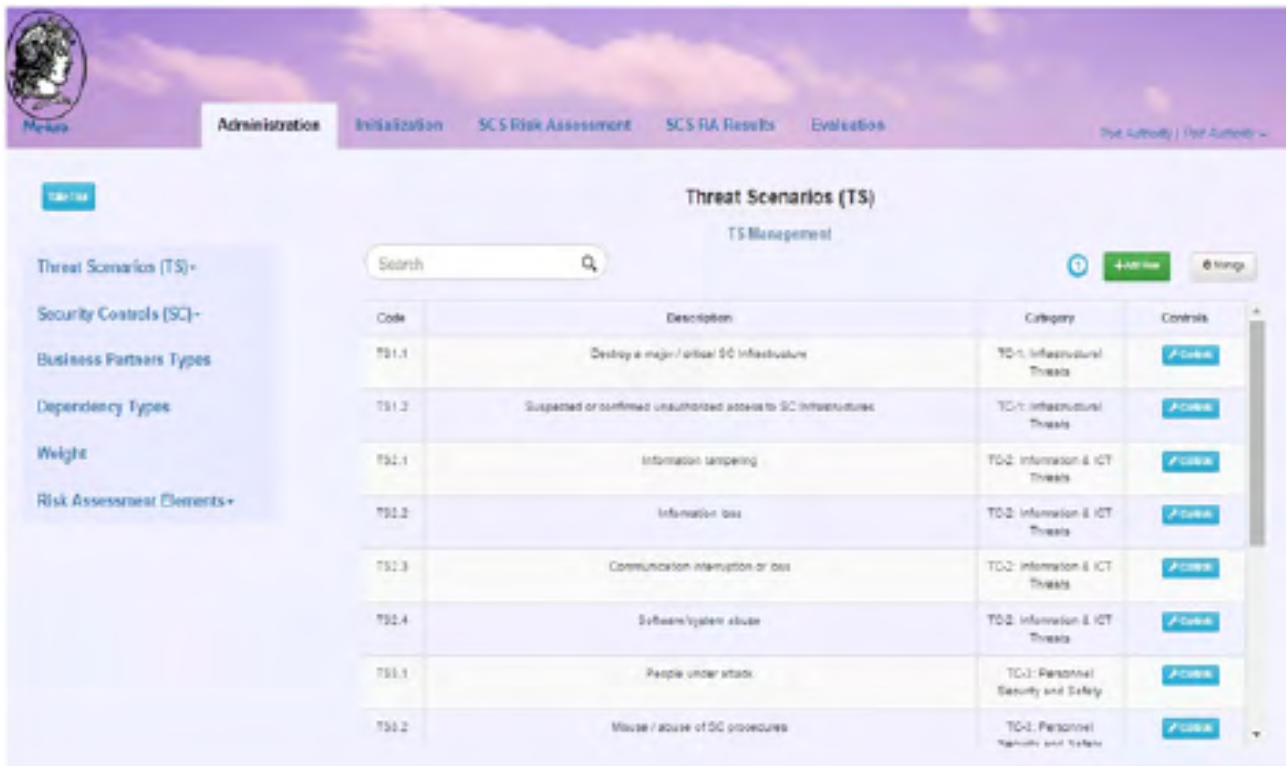
als trained on the functionality and services of the MEDUSA system (including Valencia port Foundation, Port Authorities of Alicante and Castellon and Piraeus Port Authority) and about 123 of them have used the system to identify and assess the threat scenarios and risks associated with the SCSs in which their organization participate.

3. MITIGATE methodology and System

Traditionally, in the existing literature, the analysis and evaluation of the cyber risks are based on a straightforward approach that combines a set of parameters and features such as the likelihood of a security event and the consequences of the event itself, the exploitation level of a vulnerability etc. The MITIGATE project aims to support the risk analysis with rational decision making, in particular, its pursuit is to promote a more rigorous, rational approach that gathers, critically appraises and uses high quality research evidence to enhance the risk assessment process. This is achieved by treating the resolution of the ICT MLoSC risks as a dynamic experimental environment that can be optimised involving all relevant maritime actors. Mitigate approach based on simulations facilitates the identification, analysis, assessment and mitigation of the organization-wise and interdependent cyber threats and risks.

In this vein, MITIGATE has introduced an evidence-driven Maritime Supply Chain Risk Assessment (g-MSRA) methodology which predict all possible at-tacks/threats paths and patterns arising from the global MLoSC, including threats associated with CII and interdependencies and associated

TECHNOLOGICAL ISSUES



The screenshot displays the MEDUSA Supply Chain Risk Assessment System interface. The top navigation bar includes 'Administration', 'Initialization', 'SCS Risk Assessment', 'SCS RA Results', and 'Evaluation'. The main content area is titled 'Threat Scenarios (TS)' and features a search bar, a '+Add New' button, and a 'Filter' button. A table lists various threat scenarios with columns for Code, Description, Category, and Controls. The table contains 10 rows of data, each with a unique code, a description of the threat, a category, and a 'View' button.

Code	Description	Category	Controls
TS1.1	Destroy a major/critical SC Infrastructure	TC-1: Infrastructural Threats	View
TS1.2	Suspected or confirmed unauthorized access to SC Infrastructure	TC-1: Infrastructural Threats	View
TS2.1	Information tampering	TC-2: Information & ICT Threats	View
TS2.2	Information loss	TC-2: Information & ICT Threats	View
TS2.3	Communication interruption or loss	TC-2: Information & ICT Threats	View
TS2.4	Software/system abuse	TC-2: Information & ICT Threats	View
TS3.1	People under attack	TC-3: Personnel Security and Safety	View
TS3.2	Misuse / abuse of SC procedures	TC-3: Personnel Security and Safety	View

Fig. 1: MEDUSA Supply Chain Risk Assessment System

cascading effects. The proposed approach emphasizes the collaboration of various stakeholders in the identification, assessment and mitigation of risks associated with cyber-security assets and international supply chain processes.

In addition, the project has developed an effective, collaborative, standards-based risk management (RM) system (Fig. 2) that enables the involvement and participation of all stakeholders (e.g., port security operators, port facility operators, and supply chain participants) in the cyber-security management. This system has been empowered by a range of: (i) reasoning, data mining, crowd-sourcing and BigData analytics techniques that incorporate and leverage a va-

riety of data sources and data types (e.g. vulnerabilities) retrieved from online repositories; (ii) pioneering mathematical techniques for predicting and analyzing threats patterns; (iii) innovative visualization and simulation techniques, which will optimize the auto-matic analysis of diverse data; and (iv) innovative game theory techniques in order to link optimization and simulation. All these technologies and techniques have been combined for implementing a variety of services (Collaborative Risk Assessment and Mitigation Services, Open Simulation Environment (ORASE) and Simulation Services, Risk and Vulnerability Visualization Services and Prediction, Forecasting, Social Engineering and Open Intelligence Services) as part of

the project's risk assessment system that enable maritime agents to:

- Identify and model assets, processes, risks, stakeholders' relationships/interactions and dependencies.

- Design, execute, analyze and optimize risks and threat simulation experiments that will produce the appropriate evidence, information, indicators, factors and parameters.

- Exploit the simulation results towards formulate of effective evidence-based mitigation plans.

Note that the MITIGATE system and the accompanying services are characterized by flexible, innovative, user-friendly and ergonomic interfaces, which will enable end-users to execute simulations without the need to delve

TECHNOLOGICAL ISSUES

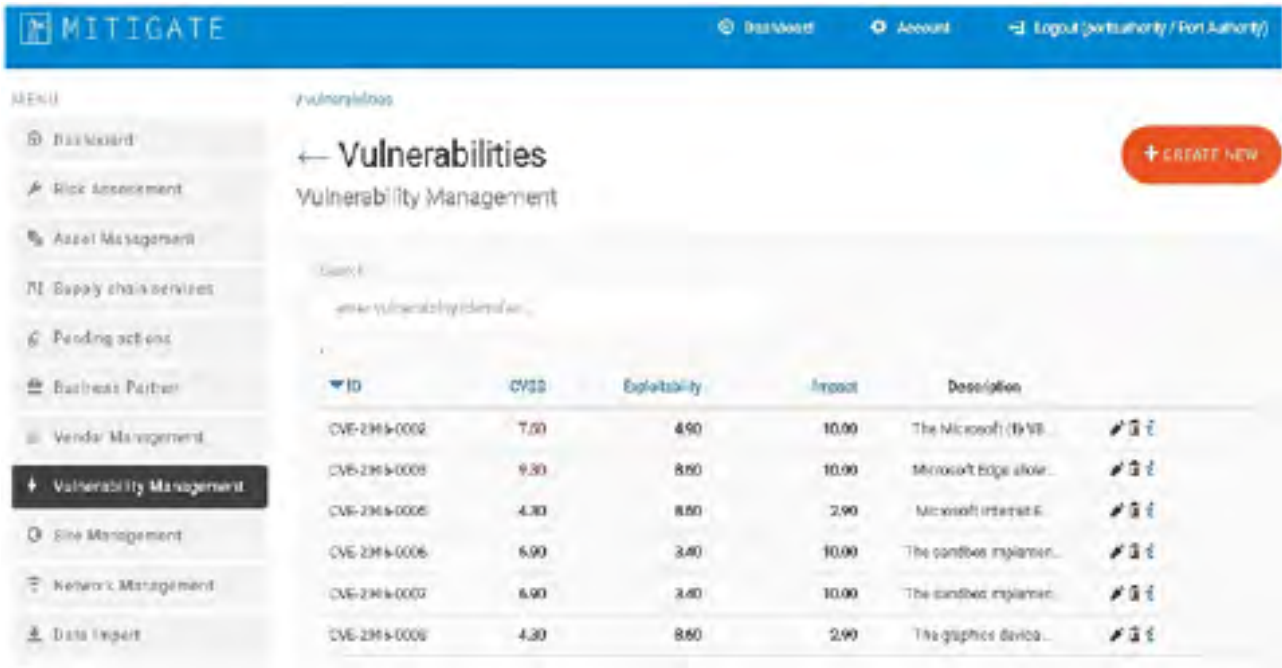


Fig. 2: MITIGATE Supply Chain Risk Assessment System

into the low-level details of the adopted mathematic models. Special emphasis has been put in ensuring the compliance of the MITIGATE risk management methodology and of the associated collaborative security management system with existing security standards (e.g. ISPS, ISO27001, ISO27005, ISO28000, CCIP). Compliance to these standards will ensure that MITIGATE will be directly contributed to the NIS* public-private platform (Network Information Security Platform). In-deed, MITIGATE aims at becoming a best practice standards-compliant blueprint infrastructure for cyber-security management in the maritime sector, which will consider and predict threats arising from the whole MLoSC.

4. Conclusions

Despite the proliferation and advancement of risk assessment methodologies for Critical Information Infrastructures (CIIs) most risk assessment frameworks do not adequately address the various cascading effects that are associated with security incidents occurring from interacting entities. This gap is very critical in the case of MLoSC's security, given that these chains are characterized by significant interdependencies at multiple levels (infrastructural, national/intra-sectoral). The main goal of the MEDUSA and MITIGATE projects is to alleviate the above-mentioned gap, through introducing, specifying and validating multi-dependency approaches to risk assessment. These projects have

therefore opened new horizons in the area of MLoSC's security, through producing and sharing knowledge associated with the identification and assessment of cascading effects in the global MLoSC, with a view to predicting potential problems but also to minimize the consequences of diverge security incidents.

4. Acknowledgements

This work has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 653212, project MITIGATE. The authors of this paper would like to thank the University of Piraeus Research Center for the financial support of this research paper.

TECHNOLOGICAL ISSUES

References

- ISO, "ISO 27001: Information Security Management System Requirements", Geneva, Switzerland 2013.
- ISO, "ISO 27005: Information security risk management", Geneva, 2011.
- ISO, "ISO 28001: Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance", Geneva, Switzerland, 2007.
- NIST, "Notional Supply Chain Risk Management Practices for Federal Information Systems, <http://nvlpubs.nist.gov/nistpubs/ir/2012/NIST.IR.7622.pdf>
- Polemi, D. and Papastergiou, S. "Current efforts in Ports and Supply Chains Risk Assessment" IEEE Proceedings of the 10th International Conference for Internet Technologies and Secure Transactions, London, U.K. 2015
- Papastergiou, S., Polemi, D. and Papagiannopoulos I.. "Business and threat analysis of Ports' Supply Chain Services". Special Session on "Innovative Risk Management Methodologies and Tools for Critical Information Infrastructures (CII)" within the 6th International Conference on Digital Human Modeling and Applications in Health, Safety, Ergonomics and Risk Management (HCI International 2015), 2-7 August, 2015, Los Angeles, CA, USA.
- Polemi, N., Kotzanikolaou, P. "Medusa: A Supply Chain Risk Assessment Methodology, CSP Forum " Cyber Security and Privacy Innovation Forum" 28-29/4/15 <https://www.cspforum.eu/2015>, Lecture Notes, Springer Verlag, 2015
- Papastergiou, S. and Polemi, N. "Harmonizing commercial port security practices & procedures in Mediterranean Basin". Special Session on "Secure and Sustainable maritime digital environment" within The Fifth International Conference on Information, Intelligence, Systems and applications (IISA 2014), July 07th 2014, Chania Crete, Greece.
- Papastergiou, S. and Polemi, N. "Harmonizing commercial port security practices & procedures In Mediterranean Basin" SSMDE: Secure and Sustainable maritime digital environment, IISA 2014, Springer Verlag 2014
- Makrodimitris, G., Polemi, N., Douligeris, C. "Security Risk Assessment Challenges in Port Information Technology Systems", Volume 441 of the Communications in Computer and Information Science series., 2014.
- Pederson, P., Dudenhoeffer, D., Hartley, S., and Permann, M. "Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research, INL, INL/EXT-06-11464, 2006.
- T. R. Peltier, "Information security risk analysis", Auerbach Publications, 2001.
- Polemi, N. and Kotzanikolaou, P. (2015) "Medusa: A Supply Chain Risk Assessment Methodology". In: Cyber Security and Privacy Forum (CSP2015), pp. 79-90, Springer International Publishing.
- Polemi, N., and Ntouskas, T., "Open Issues and Pro-posals in the IT Security Management of Commercial Ports: The S-PORT National Case". SEC 2012: 567-572
- Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies", IEEE Control Systems, Dec. 2001, 11-25
- Zio, E., and Sansavini, G., "Modeling Interdependent Network Systems for Identifying Cascade-Safe Operating Margins Interdependency", IEEE Transactions on Reliability, vol. 60, no. 1, March 2011.
- MEDUSA (Multi-ordEr Dependency approaches for managing cascading effects in ports' global sUpply chain and their integration in riSk Assesment frame-works) <http://medusa.cs.unipi.gr/>
- MITIGATE (Multidimensional, integrated, risk assess-ment framework and dynamic, collaborative Risk Management tools for critical information infrastruc-tures) <http://www.mitigateproject.eu/>

TECHNOLOGICAL ISSUES

Dr Spyros Papastergiou, University of Piraeus Research Center, Greece

Dr. Spyridon Papastergiou has received B.Sc. in Computer Science, M.S. degrees in Advanced Information Systems (Network Information Systems) and Ph.D. in Security, Privacy and Interoperability of m/e-services from the University of Piraeus, Greece in 2004, 2005 and 2009 respectively. Since October 2005, he is security researcher in the University of Piraeus Research Centre and member of the Information Security Laboratory at the Informatics Dept. of the University of Piraeus. His research interests lie in the areas of security, privacy and interoperability of mobile/electronic services, strategies for the anonymization of e/m transactions as well as assessment and management of risks and threats associated with Critical Infrastructures; he has authored over 20 publications in these fields. He has been involved in a set of European (e.g. SELIS/eTen, SWEB/IST, ImmigrationPolicy2.0, CYSM, DAEDALUS, Medusa, MITIGATE and OPERANDO) and national research projects (e.g. PENED2003 and S-PORT) and has active participation in six Cyber Defence Exercises organized by the Hellenic National Defence General Staff (1st, 2nd, 3rd and 4th National Cyber Defence Exercises ("PANOPTIS 2010", "PANOPTIS 2011", "PANOPTIS 2013" and "PANOPTIS 2014"), ENISA (European cyber defence exercises (CyberEurope 2014)) and NATO (NATO «CYBER DEFENCE EXERCISE 2010 (NCDEX 10)). In addition, he has worked for more than 6 years as Security Consultant specializing in Information Security Technology Implementation and Integration and Risk and Vulnerability Assessment.

Associate Professor Nineta Polemi

Director of UNIPI Security Lab, Department of Informatics, University of Piraeus

Associate Professor Nineta Polemi has obtained the Degree in Applied Mathematics from Portland State University (USA), Ph.D. in Applied Mathematics (Coding Theory) from The City University of New York (Graduate Center). She held teaching positions in Queens College, Baruch College of City University of New York and the State University of New York. She acted as President of the BoD and Technical Manager in the security consultancy company, Expertnet. She is currently an Associate Professor in the University of Piraeus (Dept. of Informatics) teaching cryptography, security of ICT systems, port security and e-business & innovation. Her current research interests are in the fields of security and collaborative, trustworthy e/m-services. She has over one hundred publications in the above areas and has organised numerous security scientific international events. She has received many research grants from various organizations such as the Danish Research Foundation, MSI Army Research Office/Cornell University, IEEE, State University of New York (SUNY), and The Graduate School of City University of New York (CUNY). She has been project manager (PM) / technical manager (TM) in security projects of various programmes such as National Security Agency (NSA), NATO, Dr. Nuala McGann Drescher Foundation, Greek Ministry of Defence, INFOSEC, TELEMATICS for Administrations, the last three (5th, 6th, 7th) Framework and Horizon2020 Programmes of the European Commission (E.C.) She has acted as an expert and evaluator in the E.C. and the European Network and Information Security Agency (ENISA). She is the director of the UPRC Dept. of Informatics security graduate programme and she participates in the national and European cyber security exercises in the last four years. She has many publications on maritime cyber security issues.

HIGH VISIBILITY EVENTS



*Visit of COM NATO Special Operations HQ (NSHQ),
Vice Admiral Colin Kilrain USA (N), 16 Feb 17*



*Visit of COM Naval Special Warfare Command (NSW),
Rear Admiral Tim Szymanski USA (N), 24 Mar 17*

HIGH VISIBILITY EVENTS



Visit of Supreme Allied Commander Transformation (SACT), General Denis Mercier FRA (AF), 30 May 17



8th NMIOTC Annual Conference, 06 - 08 Jun 17



Visit of Her Excellency Ambassador of Austria, Andrea Ikić Böhm, 30 Jun 17



Visit of COM Allied Maritime Command, Vice Admiral Clive Johnstone CB CBE (RN), 30 Jun 17

NMIOTC TRAINING



*Training of the Lybian Coast Guard
(EUNAVFORMED SOPHIA) 30 Jan - 09 Feb 17*



Exercise NOBLE DINA, 23 - 26 Mar 17



*Operation Sea Guardian / Opposed Boarding Exercise,
28 Apr 17*



*Training of NLD Maritime - Land EOD Team,
08 - 19 May 17*

NMIOTC TRAINING

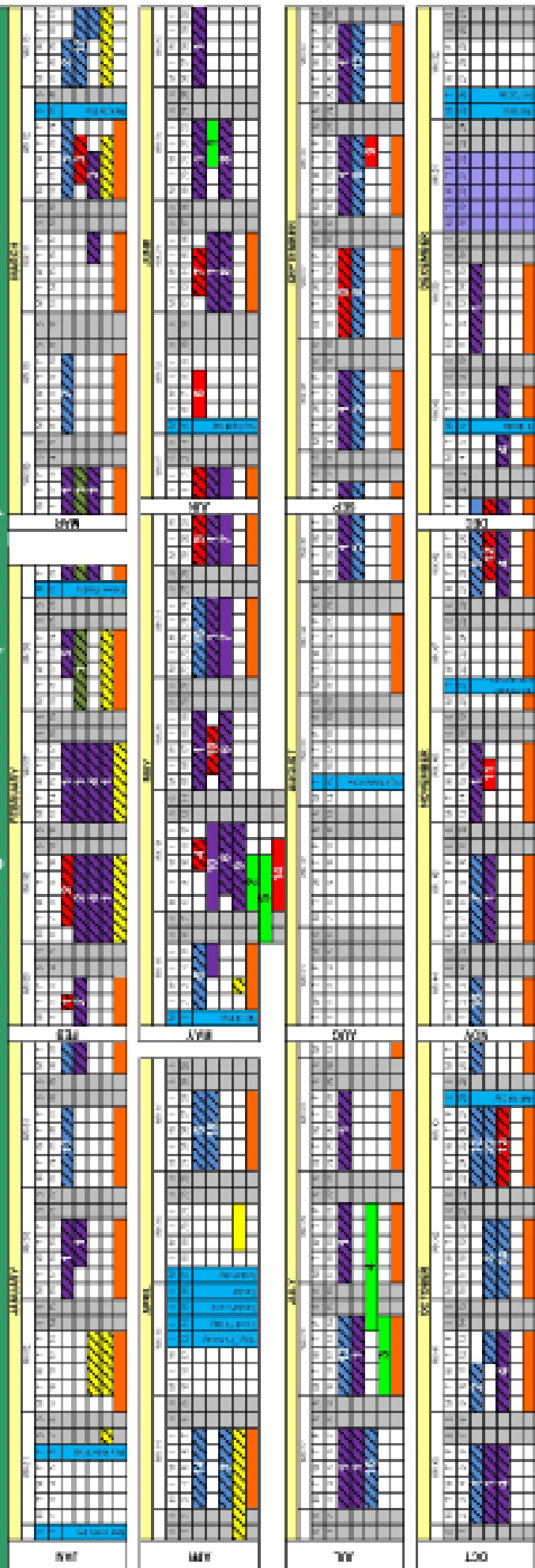


*NATO Maritime Operations LAW SEMINAR,
29 May - 02 Jun 17*



*Exercise ADRION 2017
21 - 29 Jun 17*

Draft NMIOTC Program of Work 2017 (NPOW 2017)



- SOURCES (UNCLASSIFIED)**
- 1 Course 1000 - Command Team MID Issues (MCP-MD-01200)
 - 2 Course 2000 - Boarding Team Classroom Issues (MCP-MD-01200)
 - 3 Course 3000 - Boarding Team Practical Issues (MCP-MD-01200)
 - 4 Course 5000 - Maritime Operational Terminology Course (MCP-MD-11200)
 - 5 Course 6000 - Weapons of Mass Destruction in MIO (MCP-MD-01200)
 - 6 Course 7000 - MIO in Support of Counter Air Ops (MCP-MD-01200)
 - 7 Course 8000 - C-IED Considerations in Maritime Force Protection (MCP-MD-01200)
 - 8 Course 9000 - Legal Issues in MIO (MCP-MD-01200)
 - 9 Course 10000 - MIO in Support of Countering Bad Trafficking at Sea (MCP-MD-02012)
 - 10 Course 11000 - AURR Course (on demand) (MCP-MD-02011)
 - 11 Course 12000 - MIO in a C-IED (MNF) Maritime Environment (MCP-MD-01200)
 - 12 Course 13000 - MIO in Support of International Efforts to Counter Migrant Smuggling Activities at Sea - Practical Issues
 - 13 Course 14000 - Maritime IED Disposal (MCP-MD-02000)
 - 14 Course 15000 - MIO in Support of International Efforts to Counter Migrant Smuggling Activities at Sea - Practical Issues
 - 15 Course 16000 - Maritime Aspects of Joint Operations
 - 16 Course 17000 - Train the Trainers Technical Instructor
 - 17 Course 18000 - Maritime Biometrics Collection and Tactical Forensic Site Evaluation
 - 18 Course 19000 - Cyber Security Awareness in Maritime Environment
 - 19 Course 20000 - Protection of Critical Maritime Infrastructure (CMI)
 - 20 Course 21000 - Medical Combat Care in MIO
- ACTIVITIES**
- 1 MAB (NMIOTC)
 - 2 MARVAL COURSE (20M)
 - 3 MOPCO and H-HAT W6
 - 4 MCB (MNS)
 - 5 NATO Maritime Operations Law Seminar
 - 6 MMTG Annual Conference
 - 7 MCT C-IED Conference
 - 8 ATP-T1 WORKSHOP
 - 9 Cyber Security Conference
 - 10 SMC Operational Planning Conference (SMC-OPC)
 - 11 SDA Maritime Security Conference 2017
 - 12 MISC Fall 2017
 - 13 Reconnaissance Course (MCOSS-MUT)
 - 14 3rd SDCM portal units VEG-AMMHO-Conf
- COURSES/LEADS**
- 1 LINEA NOROCC
 - 2 PHOENIX EXPRESS
 - 3 METT "SEA BREEDER 17"
 - 4 METT "BREEDER 17"
 - 5 TALOSR
- TRAINED TRAININGS**
- 1 (MCS) SOF team (Army, Navy, Air Force, Coast Guard, Police, etc)
 - 2 LBT team
 - 3 MLI team
 - 4 DLI team
 - 5 CAV team
 - 6 NLD team
 - 7 DDA
 - 8 SMC team
 - 9 CDE team
 - 10 AOT team
- TRIAL COURSES**
- 1 Sniper Course Field Trial



Updated 08 May 2017



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

