Issue 15
2nd Issue 2017
ISSN: 2242-442X

nmiotc

Maritime Interdiction Operations Journal

NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE

Cyber Threat Scenarios for Maritime Power

Violence within the Maritime Domain of the CEMAC Region

The NATO Cybersecurity Generic Reference Curriculum - Application to the Maritime Environment

Biometrics in Support of Naval Units to fight Piracy and Terrorism

NATO OTAN

10 Years
2008 - 2018

NATO
Maritime Interdiction Operational Training Centre

9th Annual Conference

Photos from NMIOTC Trai

"FOSTERING PROJECTION OF STABILITY THROUGH MARITIME SECURITY: ACHIEVING ENHANCED CAPABILITIES AND OPERATIONAL EFFECTIVENESS"

5th to 7th June 2018

CONTENTS

COMMANDANT'S EDITORIAL

4 Editorial by Georgios Tsogkas
Commodore GRC (N)
Commadant NMIOTC

CYBER SECURITY

6 Cyber Threat Scenarios for Maritime Power
by Dr. Elena (Helene) Mandalenakis

28 The NATO Cybersecurity Generic Reference Curriculum - Application to the Maritime Environment
by Dinos Kerigan-Kyrou

MARITIME SECURITY

17 Violence within the Maritime Domain of the CEMAC Region
by Judith Akah

32 Biometrics in support Naval units to fight Piracy and Terrorism
by Ioannis Argyriou Lieutenant Commander GRC (CG)

HIGH VISIBILITY EVENTS

35 VIP visitors to NMIOTC

NMIOTC TRAINING

ning Activities 43

nmiotc

MARITIME INTERDICTION OPERATIONS *JOURNAL*

Director
Commodore G. Tsogkas GRC (N)
Commandant NMIOTC

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

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

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

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

NMIOTC
Commandant's Editorial

Cyber has changed our world.

The ongoing digital revolution has fueled unprecedented prosperity and efficiency in our globalized economy, and has become inextricably linked with all aspects of our modern life. These innovations will continue to drive global progress for the foreseeable future, and by most perspectives will continue to evolve at astonishing speeds. In the wake of this progress, a growing number of challenges and risks that threaten the very core of the global security and prosperity lie on.

The recognition of the cyberspace as an operational domain, in analogy to land, air, maritime and space domains by NATO, marks a new era. The cyberspace has become an operational domain that various sectors (industry, commercial, civilian, military) interact and operate on. On the other hand Cyber criminals become more and more intelligent and cybercrime evolves at an astonishing pace. Collaborative actions are needed to effectively defend against advanced attacks and avoid catastrophic impacts to our nations and peoples. Cyber information sharing, collaborative incident handling and cyber situational awareness are the most essential areas that NATO and EU collaboration will lead to successful civilian, industrial, commercial and military cyber defense strategies and operations.

The impact of cyber security incidents on the conduct of future maritime operations may be catastrophic. Maritime operations are conducted by technology-intensive platforms, which today rely heavily on information systems. How will this dependence that navies possess on information technologies affect their ability to maintain security at sea?

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

help detect, deter, disable, and defeat adversaries. Robust intelligence, law enforcement, and maritime along with other military cyber programs are essential to enhancing the effectiveness of Maritime Operations, and deterring, preventing, and responding to malicious activity targeting critical maritime infrastructure. We should recognize that cyber capabilities are a critical enabler of success across all missions, and ensure that these capabilities are leveraged by Commanders and decision-makers at all levels.

Besides the challenges, there are opportunities for collaboration especially in the maritime domain. Alliance relies on strong and resilient cyber defence to fulfill the core tasks of collective defence, crisis management and cooperative security. Our Partners could be engaged as well.

Having said that allow me to highlight that the NMIOTC Cyber Security conferences every autumn are the ongoing commitment of NMIOTC to tackle the cyber security issues in the Maritime Environment, an area and a topic that will dominate our efforts intensively, at least for the next decade. It will be another stepping stone for NMIOTC to engage with the international community to create opportunities for a better understanding and to support the cyber security at sea that will eventually reduce potential cyber threats to the international maritime community for the years to come.

The first article presented by Dr. Elena (Helene) Mandalenakis addresses “Cyber Threat Scenarios for Maritime Power”. It is followed by an interesting take of Ms Akah Judith Ewo épouse Ndze and Mr Dalaklis Dimitrios on “Violence within the Maritime Domain of the Central African Economic and Monetary Community (CEMAC) Region”. Dr. Dinos Kerigan-Kyrou, Chartered Member of the Institute of Logistics and Transport (CMILT) focuses upon the application of the NATO Cybersecurity Curriculum to the maritime environment. Last but not least Lt Cdr Ioannis Argiriou (HEL. CG) presents his views on “Biometrics in support of naval units to fight Piracy and Terrorism”.

At this point, I wish to take this opportunity to announce with great pleasure, the 9th Annual NMIOTC Conference which will be held at NMIOTC’s premises (Souda Bay – Crete) from 5th to 7th June 2018, with the theme “Fostering Projection of Stability through Maritime Security: Achieving Enhanced Capabilities and Operational Effectiveness”.

Georgios Tsogkas
Commodore GRC (N)
Commadant NMIOTC

Cyber Threat Scenarios for Maritime Power

by Dr. Elena (Helene) Mandalenakis [1]

Maritime power is an integral component for a coastal state's existence. The use of maritime trade routes not only benefits the economy and development of the state but it forces it to cultivate its economic and inevitably, its diplomatic relations with foreign states. In an era of globalization, the economic drive of each state has turned into a race of economies much like the arms race of the 20th century. Each state seeks to dominate the economic battlefield in the fastest and most efficient way possible. This led to an ever-increasing, and by now, continuous, use of the maritime trade routes, which have instilled a level of dependency for the viability of a state's economy and prosperity. This level of dependency however, presents a great advantage and a great disadvantage alike. Any disruption or denial of access to maritime trade routes could significantly damage the economic interests of any state to the benefit of another. In the past, any such attempted interruption demanded a disruption by physical means (i.e. naval blockades, naval interception of merchant navy). The downside to any such attempt entailed a de facto declaration of war or initiation of hostilities between the nations involved. Today, it is possible to destabilize a state by disrupting its maritime supply routes through cyber means. The current state of cyber technology allows for this disruption prior to a declaration of war or initiation of hostilities, preemptively, covertly and significantly more effectively than ever before. During military conflict, the cyber technology may disrupt the maritime supply routes, which are vital for the supply of the state and render the resupply of any military offensive obsolete. The emphasis of this paper is centered on the security of the maritime supply routes worldwide by commercial shipping.

State sovereignty and Trade

State sovereignty defines the international system of states, as this has been shaped after the Treaty of Westphalia (1648) after the Thirty-Year War in Europe. According to this principle,

[1] I would like to express my great appreciation to Emmanuel Mandalenakis [LL.B., LL.M., LL.M (Adv)] for his valuable legal contribution to this work in his capacity as Legal Adviser with specializations in EU Law and Air and Space Law.

every state has the absolute authority over its internal affairs without any external interference. The state has the right to control its, clearly by international law, defined territory and its citizens. As all states are equal under international law, the state is also obliged to recognize this same right to all other political entities in the international system and refrain from any interference in their domestic affairs. In order for new states, to have formal relations with other states, they have to be internationally recognized, which justifies the protection of clearly defined borders and precludes any unilateral attempts to change them. Any disagreement regarding the validity of such borders may lead to war and the creation of new political entities which will seek the international community's recognition. This practice has led to the creation of new states and the disintegration or disappearance of others.

In the past, a state would magnify its power by conquering new territories. The additional territory increased the size of the state, its population, and its ownership of natural resources. The geographical location of the newly acquired land and its proximity to maritime routes, further increased the political weight of the state. Hence, certain land-locked states purposely engaged in war in order to acquire access to the sea and enhance their economic activity. This is how some states became empires with regional or even global powers.

The creation of the League of Nations (1919) was the first successful attempt to render war obsolete in favor of global welfare. As a result, war became relegated as the last line of diplomacy. With the elimination of war as a primary means to conduct business, trade was further encouraged between former rivals, neighbors primarily, with the common objective to attain and maintain peace through mutual cooperation and profit.

The dawn of the twentieth century was also marked by considerable improvements over maritime, land and air transport. Innovations in these sectors, further enhanced the ability of states to broaden their trade horizons to include destinations previously unavailable. In conjunction to the already established maritime mode of transport, together, they stimulated the current form of international trade which typically includes overseas destinations.

Maritime Supply Routes

Modern maritime transport is a significant economic sector which lies at the heart of cross-border transport networks that support supply chains, thus, serving both businesses and consumers. Apart from satisfying the interests of the trading partners, maritime transport promotes regional and international economic integration. The International Chamber of Shipping estimates that approximately 90% of world trade is carried by the international shipping industry. This staggering amount is supported by over 50.000 merchant ships, 150 nations and over a million of personnel. In 2015, estimated world seaborne trade volumes surpassed 10 billion tons.[2] The significance of the maritime trade industry is an economic sector that generates employment for high to low-skilled personnel, revenue from trading goods between the involved partners as well as economic and political power for the state.[3] These factors justify the countries' interest to continuously explore new maritime trade routes to increase interconnectivity, efficiency and profit. China's "One Belt, One Road Initiative" for example, aims "to establish new trading routes, links and business opportunities by further connecting China, Asia, Europe, Africa and countries with economies in transition along five routes."[4]

2nd NMIOTC Cyber Security Conference (Sept 2017)

[2] International Chamber of Shipping at http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade Accessed at 27 August 2017.

[3] For more details look at *UNCTAD Review of Maritime Transport 2016* (UNCTAD/RMT/2016), p.5 at http://unctad.org/en/PublicationsLibrary/rmt2016_en.pdf

[4] Ibid., p.21.

Maritime routes are the preferred choice of transport for bulky goods and materials. This is not a random choice as the principles of cost effectiveness, frequency of service and distance, determine the internationally recognized supply routes, as well as the modes of transport. Mode choice involves balancing certain tradeoffs, which are generally influenced by the nature of goods and materials as well as their time sensitive nature and reliability, along with the distance to destination. In that sense, the nature of the goods is divided into low cost mode, for cargo with high or no life expectancy restrictions and, fast mode, for cargo that is very time sensitive and perishable. The difference between them lies in the capacity of the method of transport, with the maritime one bearing the highest capacity available but with the longest delivery times by comparison to the others.

Cyber Threat to State Sovereignty

Cyberspace provides a new virtual arena for actors to interact in attaining their economic and/or political interests. The particularity of this domain is that although it is virtual, the results of any virtual operation may have geopolitical dimensions as it allows the actors to advance their geopolitical strategies. Cyberspace has been mainly used for industrial espionage, sabotage, direct and indirect economic interferences and organized crime. Lately however, it has been increasingly used for offensive operations from one state to another.

These state offensive operations are in the form of hostile cyber interferences which although not violating territorial borders, affect the smooth operation of key sectors of governance by hindering the effective control of national affairs. This infringement of its sovereignty has as a potential consequence the destabilization of the state. The issue of state sovereignty may not seem important to cyber security practitioners, however, its discussion is not a theoretical exercise, as state sovereignty is closely linked to the ability to exercise state power and consequently it determines state foreign policy. The borderless nature of cyberspace presents challenges in the application of the traditional notion of sovereignty. The state's right to respond and defend itself requires a departure from the interpretation of the traditional norms, much like the interpretation afforded for terrorist attacks within the borders of the state. This departure is based on notions of extraterritorial jurisdiction combined with an effects doctrine that establishes a liability regime for acts which originate in a different state or territory and have a direct effect within the borders of the attacked.

In political and military terms, national security is the state's capacity to defend its territory and citizens through its security services. Industrial security refers to the ability to protect a specific industrial sector or agent from unauthorized physical or cyber intrusions. In certain sectors, namely the critical infrastructures, industrial and national security coincide. Hence, critical infrastructures are considered "those used for, inter alia, the generation, transmission and distribution of energy, air and maritime transport, banking and financial services, e-commerce, water supply, food distribution and public health-and the critical information infrastructures that increasingly interconnect and affect their cooperation."[5] It is in the interest of the state to guarantee and protect the security of its vital sectors, as they comprise the pillars of its society and the base for its economic and military prowess. In that regard, the protection of state territory and borders, is extended to the protection of its infrastructure from

Dr Elena Mandalenakis at the 2nd NMIOTC Cyber Security Conference (Sept 2017)

[5] UNGA Resolution 58/199, 23 December 2003.

physical and virtual threats alike.
The safety of physical assets necessitates the continuous presence from the security services and the military alike. On the other hand, the virtual assets, namely the systematic use and flow of electronic information in all critical sectors operating within the state or for its interests, require the use of cyber defence strategies or otherwise known as cybersecurity. The inclusion of cybersecurity on state sovereignty has been guided by perceptions of risk and eventuality of threat. Reference to cyber threats, and not risks, implies a degree of malicious intention and a direct effect to the detriment of the attacked. As William J. Burns said, "patching national cybersecurity vulnerabilities in today's world is often just as important as border security."[6]

State Actors and Cyber Capacity

A cyber-attack that weakens a state by obstructing the attainment of its primary interests is considered an act of war. A cyber offensive superiority could act as a deterrent against other cyber state powers which justifies their growing interest in cyber advancement. The nature of recent cyber-attacks reveals the offensive and destructive nature of cyber weapons such as Stuxnet, WannaCry, NotPetya, etc. As technology evolves, it becomes more difficult to predict future cyber targets or vulnerabilities and develop an efficient defense system.
As a cyber-attack's origin and primary target can eventually be determined, the state may opt to either defend itself with cyber or physical means to protect itself against the hostile action. A cyber-attack may also be instigated as complementary to a physical attack, since a well-organized combined strike is more effective in paralyzing a state. Russia applied this tactic in 2008, when it initiated a cyber-attack against the Georgian government, before and during its military operations at the Georgian province of South Ossetia. This was the first time in history that cyber and military offensives were simultaneously orchestrated. The DDoS cyber-attacks targeted government sites, media, communications and transportation companies, paralyzing Georgia while hindering any communication between the government and its supporters during the fights.[7]
The initial cyber-attacks against Georgia could not immediately be attributed to Russian hackers. The identification of the actor responsible for the attack requires thorough analysis of evidence that is not readily available or not detected at all. The difficulty to instantly recognize a concealed "cyber enemy" hinders the attribution of cyber acts. Furthermore, as the infiltration of a system or network is not usually detectable in real time, or launched from a single platform, it renders the "cyber victim" incapable of containing the effects of the cyber-attack. Keeping these in mind, it is easy to deduct that a state is not in a position to organize a timely counter cyber-attack before the escalation of "cyber hostilities."
Cyber hostilities are not conditioned by a declaration of war as a state can disrupt the functioning of the critical civil and military infrastructure of another and place it under a state of emergency. Once a state engages in or sponsors cyber-attacks on critical infrastructures of another state, apart from the real effects of the attacks, it cultivates a perception regarding its cyber capacity, that may encourage or deter other states to contest it. As Shaheen explains, "in cyber warfare,

[6] William J. Burns, Jared Cohen, "The Rules of the Brave New Cyberworld," *Foreign Policy*, 16 February 2017, at http://carnegieendowment.org/2017/02/16/rules-of-brave-new-cyberworld-pub-68024
[7] John Markoff, "Before the Gunfire, Cyber-attacks," *The New York Times*, 12 August 2008, at www.nytimes.com/2008/08/13/technology/13cyber.html?mcubz=1

given the advantages of mobility, surprise, penetration and precision that cyber weapons offer to an attacker and the underdeveloped defensive side of this warfare, the attacker will develop strong perception about its offensive advantage."[8] In cyberspace then, as in the physical world, perceptions are formed on both sides and determine the initiation or the prevention of war, despite the fact that they may be inaccurate.

The nuclear arms race during the Cold War and recent wars, indicate that political decisions regarding weapon stock piling are not always based on real data but rely on perceptions. Once a state's power is measured in conventional arms, the supremacy of one state over another is more apparent. In the case of nuclear power, a state possesses nuclear power and the potential of creating nuclear arms with catastrophic effects for its enemy states. In the case of cyber power, a state amplifies its offensive cyber capability to use the first strike preemptively against another state. The success of attack will determine the international recognition of its cyber offensive power.

State cyber offensive power does not necessarily imply adequate cyber defense power. Cyber defense strategies exist but are not adequate as a) the network interconnectivity of all critical infrastructures continues to grow and cannot be controlled by the state, b) the actors are also non-state or state sponsored, c) the launching of the attack can take place through multiple points or platforms, and d) the cyber weapons cannot be stockpiled and therefore can only be assessed through the impact of their launch. Despite the designed precision of a cyberattack, such as Stuxnet in 2010, its impact on the intended target is only half of the story, as any collateral damage from its spill over to systems supporting different infrastructures even in different states, should be taken into account. The Stuxnet malware although it hit its primary target it further infected the infrastructure of other states too.

A state's cyber capacity serves as a force multiplier for rising powers in the international system. China for example, has chosen to develop even further its maritime and cyber power domains to become more effective while downsizing and rationalizing its army but without diminishing its war fighting capabilities. It has merged the cyberspace, space and electromagnetic domains under the umbrella of the Chinese Strategic Support Force.[9] Declining states acquiring cyber capability, may not just preserve, but also strengthen their geopolitical position. Accordingly, developing cyber capability is not a choice but a necessity for the once powerful states to increase their power of influence. Russia for example, complements its military strength with cyber capabilities and is very active in cyberspace. On the other hand, small states with cyber capability such as Israel and Estonia, have an opportunity to show their potential, despite their geographical or geopolitical attributes and to enhance their position and influence in international affairs.

Jamie Shea, NATO Deputy Assistant Secretary General for Emerging Security Challenges at the 2nd NMIOTC Cyber Security Conference (Sept 2017)

Maritime supply routes during war

Having established the importance of

[8] Salma Shaheen, "Offense-Defense Balance in Cyber Warfare," p. 90 in J. F. Kremer and B. Müller, eds. *Cyberspace and International Relations: Theory, Prospects and Challenges*, (Heidelberg: Springer, 2014).

[9] Adam Ni, "Why China is Trimming its Army," *The Diplomat*, 15 July 2017 at http://thediplomat.com/2017/07/why-china-is-trimming-its-army

maritime supply routes for the viability of a state's economy during peacetime, it is important to consider the ever-growing importance of these routes used in support of the war effort. The majority of conflicts post WWII, have occurred in countries separated by thousands of miles from each other. The attacking state had to coordinate the deployment of its troops and navigate complex logistical minefields to coordinate a successful attack. The transportation of the military assets required, had to be coordinated to coincide with the strategic planning and initiation of hostilities. Each nation possesses a dedicated fleet of transports for military use alone. Nevertheless, the number of such military freight vessels cannot serve the needs of a large-scale conflict, which will lead to the tried and tested solution of sub-contracting the resupply effort to commercial entities. Historically, in a large-scale war, the military commandeered all civilian assets to aid in the war effort. During WWII, the majority of the merchant navy was used for the transportation of troops, equipment, supplies and ammunition, often at great cost and loss of life. Regarding defensive strategies, cutting off the supply lines of the enemy, thereby denying military effectiveness in the battlefield, ranks within the highest of priorities.

In times of war, where the maritime supply routes will be used for the essential supply and resupply of the military campaign, safety of navigation will be of the utmost concern. The use of any technology that could disrupt this supply line could be of the most strategic importance as an offensive measure. This could be an enormous advantage but at the same time it could be catastrophic for the defence initiative. Regarding the maritime supply routes used during the WWII, a substantial number of military vessels from the Allies were needed and were diverted from the front for the protection of the supply convoys. Conversely, an enormous number of Axis military assets were deployed to intercept the convoys. The most successful wolfpack operation, codenamed "West", was comprised of 23 German U-Boats, attacked 10 convoys in the period of 44 days, sunk 33 vessels and damaged an additional 4. It has been written in history as the most successful wolfpack of WWII.[10]

a) Military Offence

It has already been proven that the cybersecurity of the navy is far more advanced than the cybersecurity of the merchant fleets, therefore the level of difficulty in directing a cyberattack against the navy increases exponentially. At the same time, the possibility of exploiting well known vulnerabilities in the electronic navigation systems of the merchant navy, is considerably easier and comes at a minimum cost. Although the vulnerabilities are well known, there has been neither a uniform strategy nor a uniform implementation on how to effectively shield the merchant fleet from cyber threats, leaving any attempt to do so on the personal initiative of ship owners.

In a previous work concerning maritime security, we highlighted a possible threat scenario that may have seemed unlikely; the threat possibility of using known vulnerabilities of the commercial shipping against the military navy.[11] Four incidents at sea in 2017, involving two US cruisers and two US destroyers, may have elevated that theoretical threat scenario to an actual threat scenario. Although the US Navy investigations have ruled out cyber interference, sabotage, or unlawful interference, cyber security circles are whispering of the possibility of electronic interference. Although there has been no evidence to support any such theories, the high rate of three collisions at sea in less than a year, combined with the news of the US Navy ordering a global pause in operations in order to examine any contributory factors that led to the collision of the USS John S. McCain, only fueled further speculations.[12]

On the 22nd of June 2017, an incident of GPS spoofing was reported involving more than 20 ships off the Russian port of Novorossiysk in the Black Sea. According to the captain who filed the report with the US Maritime Administration, the GPS had placed his ship inland at the vicinity of Gelendzhik Airport, more than 20 miles off his current position.[13] The captain further confirmed that twenty other captains in the area, were reporting the same anomaly on their radios. The RNT Foundation has received numerous anecdotal reports of maritime problems with AIS and GPS in Russian waters. In fact, GPS spoofing in Russia is known to be highly advanced, with over 250,000 cell towers equipped with GPS jamming devices. The technological leap from spoofing the GPS signal from a 213-foot private yacht in 2013[14] to affecting multiple commercial vessels simultaneously, is enormous.

As the commercial maritime sector is the weakest link and the least cyber

[10] For further details regarding Wolfpacks' operations see http://uboat.net/ops/wolfpacks/3.html

[11] Elena (Helene) Mandalenakis, "Political Implications of Cyber Space on State Power," NMIOTC Maritime Interdiction Operations Journal, 13, 2016, p.21 at http://www.nmiotc.nato.int/files/NMIOTCjournal13.pdf

[12] Christopher Woody, "The Navy's 4th accident this year is stirring concerns about hackers targeting US warships," *Business Insider*, 24 August 2017 at http://www.businessinsider.com/hacking-and-gps-spoofing-involved-in-navy-accidents-2017-8

[13] "2017-005A-GPS Interference-Black Sea MARAD Alert," United States Department of Transportation at https://www.marad.dot.gov/msci/alert/2017/2017-005a-gps-interference-black-sea/

[14] "UT Austin Researchers Successfully Spoof an $80 million Yacht at Sea," *UTNews*, 29 July 2013 at https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea

secure, it is the sector that will most likely become the prime target for cyber-attack. Any technologically savvy hacker, would know that to defeat a pair of opponents, the military assisted by the commercial fleet in this case, one simply attacks the weakest one to bring down both. Technological evolution allows for the disruption of the supply line without diverting any military resources from where they are actually needed the most. This can be achieved by interfering with key electronic equipment and signals that could render the concept of safe and automated navigation inoperable. Tampering with the Satellite communication equipment, Voice Over Internet Protocols (VOIP) equipment, Wireless networks (WLANs), Public address and general alarm systems, one can effectively disable the communications capability of any commercial vessel. In addition, interfering with the Positioning systems (GPS, etc.), the Electronic Chart Display Information System (ECDIS), Systems that interface with electronic navigation systems and propulsion/maneuvering systems, Automatic Identification System (AIS), Global Maritime Distress and Safety System (GMDSS), Radar equipment, Voyage Data Recorders (VDRs), Power management, Integrated control system, Alarm system and the Emergency response system, allows for the virtual hijacking of the vessel controls and effectively renders it a remotely operated vehicle, much like a drone that is controlled from thousands of miles away. The ramifications on a threat scenario involving the intentional GPS spoofing of multiple merchant vessels aided by electronic hijacking of controls of one or two ships to use as battering rams against military vessels, becomes a feasible endeavor that could prove quite useful if exploited for military offensive purposes. In reality, not all of the above systems need to be interfered with to disrupt a maritime supply route. Total control would require an unprecedented number of hackers working simultaneously and attacking every seaborne electronic system with known vulnerabilities. Despite the undeniable skills of these individuals, such an endeavor is simply too time consuming for such a time sensitive operation to be effective. What is really effective however, is a strategy that involves random attacks on different systems and components each time with different disruption results that would render the trust and overreliance to automated systems obsolete. Navigating a route riddled with phantom ships, fake weather reports, fake collision alarms, no communication capability, glitchy propulsion and steering systems, could be a challenge for the most experienced seafarer. The only way to operate a maritime supply route under such circumstances, would be to roll back to analog operations with visual navigation and determination of the vessel's position via celestial navigation. Incidentally, the US Navy has already realized that the overreliance on satellites could be a major drawback in a large-scale conflict, especially when these can be destroyed or jammed by the enemy forces. To counter this possibility, the US Navy is reintroducing celestial navigation as a training requirement for its officers.[15]

b) State Defence

The offensive strategy discussed above may be crucial in determining the outcome of war. As important as a military offensive can be, it is equally important to have a defensive initiative at home that relies in exactly the same principles as the military cyber offensive does. The known and unknown vulnerabilities of electronic systems will be exploited by both sides. It is imperative then, to shield the integrity of the state from any unwanted interference that may alter the outcome of war. An elaborate defence strategy would also require an equal amount of attention to other critical infrastructures and ancillary transportation sectors that complement each other during both peace and war. This becomes relevant for this paper in respect to the transport of raw materials and supplies from the factory or warehouse to the port for shipping. Thus, if a state disrupts the supply of cargo directly before reaching the supply vessels, the maritime supply routes become useless. Consequently, other critical infrastructures may become principal targets for cyber-attack, making their protection crucial as a defensive measure. For the purposes of this analysis, we will only focus on the rail transport, as it is the primary means of transport and supply for ports.

Freight trains have been participating in the national and global trade with

[15] Geoff Brufiel, "U.S. Navy Brings Back Navigation By The Stars For Officers," *National Public Radio*, 22 February 2016 at http://www.npr.org/2016/02/22/467210492/u-s-navy-brings-back-navigation-by-the-stars-for-officers

significant financial gains for the states and the companies using them. Rail freight gradually increases its market share due to its capacity for large consignments of goods, as well as its speed and reliability. To enhance this capability even further, the European Rail Traffic Management System (ERTMS) is replacing traditional signaling across Europe. The signaling system directly affects the capacity of the rail corridor along with other system configurations.[16] Wireless technology and the computerization of in-cab signals will transform the basic component of ERTMS, the European Train Control System (ETCS), and trains will become practically automatic.[17] The German Aerospace Centre (DLR) is working on a project for a driverless high-speed intercontinental freight train that would incorporate aerodynamic features already used in passenger trains. The expectation is that in time, it would carry both passengers and cargo. DLR even tested for automatic loading and unloading of packages, as the aerodynamic design would not work with sea containers.[18]

The modernization of the rail system implies its digitization with the benefits and risks associated with it. Some of the benefits are interoperability, safety, and greater capacity, while one of the main risks is the security of the automatic function and remote control of the systems involved. There have been four known hacking incidents in the UK railway in 2015[19], although these hacks were attributed to or supported by foreign state actors and which have been exploratory in nature and not destructive. According to Sergey Gordeychik of the Moscow Kaspersky Lab, these hacks could potentially be used as a "cyber weapon against civil infrastructure" since system vulnerabilities are common and widespread.[20] The UK Department for Transport explains that the "railway systems are becoming vulnerable to cyber-attack due to the move away from bespoke stand-alone systems to open-platform, standardized equipment built using commercial off the shelf components, and increasing use of networked control and automation systems that can be accessed remotely via public and private networks."[21]

In 2015 Japan's Railways Hokkaido new Shinkansen line was hacked just before its operation. The aim was the collection of transport security information. The 2008 case of a teenager taking control of the signaling system of the Polish Rail, indicates how easy it is to interfere in the rail control systems. The boy modified a TV remote control and unaware of the extent of its actions, derailed four vehicles and injured twelve people.[22] The concern of the experts is the security of the control system connection with the outside world.

Countermeasures

Beyond the use of brute force strong countermeasures for a state on a political level, are the use of deterrence and compellence strategies. As Thomas Schelling explained, compellence aims at coercing an opponent to change its behavior or to stop acting at all. Instead, deterrence is designed to persuade and discourage an adversary from initiating an action by threatening the use of military force.[23] The use of actual or potential credible threats is key for the success of these strategies, which were quite effective in relation to the use of nuclear weapons by contending states. The application of these strategies in the cyber domain however, is not as clear as in the physical, political and military domain, largely on account of the virtual nature of the threat. As such, there is an absence of advanced warning of a cyber-attack. With the exception of attacks from groups seeking to further their reputation, a state sponsored cyber-attack will only be made known

[16]"The capacity of a rail corridor is defined as the number of trains that can safely pass a given segment within a period of time. The capacity is affected by variations in system configurations, such as track infrastructure, signaling system, operation philosophy, and rolling stock." In H. Pouryousef et al., "Railroad capacity tools and methodologies in the U.S. and Europe," *Journal of Modern Transport*, (2015), 23(1): 30–42 at https://link.springer.com/content/pdf/10.1007%2Fs40534-015-0069-z.pdf

[17]Gary Peters, "A digital railway: is it cyber secure?" 23 March 2017 at http://www.railway-technology.com/features/featurea-digital-railway-is-it-cyber-secure-5770312/

[18]Gary Peters, "The driverless freight train as imagined in Germany" 21 June 2017 at http://www.railway-technology.com/features/featurethe-driverless-freight-train-as-imagined-in-germany-5848101/

[19]Gary Peters, "A digital railway: is it cyber secure?" 23 March 2017 at http://www.railway-technology.com/features/featurea-digital-railway-is-it-cyber-secure-5770312/

[20]"Cyber attacks on UK railways pose 'real disaster' risk," 12 July 2016 at http://www.theweek.co.uk/74396/cyber-attacks-on-uk-railways-pose-real-disaster-risk

[21]Gary Peters, "A digital railway: is it cyber secure?" 23 March 2017 at http://www.railway-technology.com/features/featurea-digital-railway-is-it-cyber-secure-5770312/

[22]"Monitor without risk of remote cyber attacks – Unidirectional security for railways," 16 January 2017 at https://www.globalrailnews.com/2017/01/16/monitor-without-risk-of-remote-cyber-attacks-unidirectional-security-for-railways

[23] Thomas C. Schelling, *Arms and Influence*, (New Haven: Yale University Press, 1966).

with its adverse effects towards the system that is compromised. Although some attacks leave certain identifiable traits leading to the identity or even nationality of the group involved, these traits cannot be attributed with any amount of certainty to a specific actor. This is even more the case in relation to high-end attacks, where the methods of incursion are custom made and novel. On account of the complexity and interconnectivity of electronic systems that often rely on each other, it becomes even more difficult to assess, with any certainty, the real purpose and scale of the attack in relation to its consequences.

The virtual nature of the attack and the lack of attribution or claimed responsibility, lead to a situation of "non liquet" or otherwise known as legal vacuum. An invisible attack, by equally invisible attackers, invalidates the doctrine of proportional response. Although major cyber states have agreed that there should be international norms on cyber behaviour and that states should refrain from cyber-attacking critical infrastructures of other states, an international institution with the capacity to address such state cyber grievances and to enforce and monitor rule obedience, has not been established. As such, the ability of a state to react within the limits of legality to a threat or attack with force, is hindered by the lack of legal precedence of cyber wars.

Acting or simply reacting?

As of 2016, the number of registered merchant vessels worldwide was estimated at just over 51.400 with 16.892 of them bulk carriers, 10.919 general cargo ships, 7.065 crude oil tankers and 5.239 container ships.[24] The number of vessels sailing the seas is very high, with certain shipowners often owning 500 vessels or more each. These numbers however, do not only reflect the size of the maritime industry but also present 51.400 potential targets for cyber-attack. To this day, the number of known cases is low, as attacks often remain invisible to the company or businesses avoid reporting them for fear of alarming investors, regulators or insurers.[25] This level of underreporting is a major contributory factor to the largely cyber unprotected state of affairs of the industry.

c) Theoretical or Real threat scenario?

The current lack of reporting, has enabled a false sense of security for the major players in the maritime industry. Incidents of cyber-attacks, when experienced, are often treated as isolated incidents and are mostly not even recognized as such. Shipowners tend to treat incidents of electronic tampering as faulty electronic equipment and interference to the propulsion or power management system as faulty mechanical components. Following this logic, the remedy for a potential cyber-attack is the replacement of the affected instruments, equipment, parts and components. This perception of troubleshooting however, could change abruptly in the future and especially in a case of war.

During peace time, the incidents of cyber-attacks are generally limited to economic objectives. The overwhelming majority of cyber criminals are non-state actor individuals or groups, launching commoditized and targeted attacks with a financial cost ranging from 200 dollars to 1 million dollars. From a business point of view, 1 million dollars' worth of damage control, is a number far smaller than the cost of a comprehensive cyber security solution. Thus, companies will undoubtedly prefer to pay that amount for something that they consider a unique or rare situation.

There is however, a smaller segment of cyber criminals that deal exclusively with high-end attacks. These groups possess expert level technical capabilities, they are highly organized, extremely covert and operate internationally. Their attacks are few and numbered but they are customized in tools and vulnerabilities, leaving a permanent post-attack impact in reputation to their victims, costing them anywhere from 1 to 100 million dollars. These groups are often linked or even directly supported by state actors and their target preference is limited to large scale financial systems and critical infrastructure. In case of war, these will become the primary virtual commandos in any cyber offense or defense.

The deciding factor for the shipowners then, in a choice between full cyber protection versus non-protection and damage control, seems to rely exclusively on three factors alone: frequency, severity and cost of a potential cyber-attack.

[24] Statista at https://www.statista.com/statistics/264024/number-of-merchant-ships-worldwide-by-type/

[25] Jeremy Wagstaff, "All at sea: global shipping fleet exposed to hacking threat," *Reuters*, 24 April 2014 at http://www.reuters.com/article/us-cybersecurity-shipping-idUSBREA3M20820140424

Commodore G. Tsogkas (GRC N), NMIOTC Commandant, opening the 2nd Cyber Security Conference (Oct 2017)

d) Frequency and Severity

The first two factors cannot objectively be fully analyzed due to the underreporting of incidents from the maritime industry. Consequently, we will have to make certain logical assumptions based on the existing mentality of the sector, the available technology and the modus operandi of hackers worldwide. We estimate the frequency of attacks during peace time in the low category because if the frequency was any higher, the maritime sector would have already taken aggressive cyber measures to curb the trend of attacks. In addition, the size of the merchant fleet worldwide and the multiplicity of components and parts with vulnerabilities, combined with unclear economic objectives, limit the type of cyber-attack to opportunistic or exploratory attacks.

The opportunistic attacks would be attributable to single hackers, driven by the challenge of intrusion alone and perhaps with some minor illicit mentality (i.e. ransomware attack). On the other hand, the exploratory attacks could be the result of targeted attacks as well as high-end attacks. Their nature is infiltration, collection of information and identification of vulnerabilities. Often, they do not result in disruption or interference and they remain largely undetected. These have the capacity of becoming quite dangerous when the group involved decides to launch an attack, as they have already bypassed the security protocols. In such a case, both factors of frequency and severity will increase exponentially. High-end attacks would dominate the virtual battlefield in case of war.

e) Cost of implementation

The cost of a cyber security solution for large scale enterprises and critical infrastructure is difficult to estimate. There are a variety of factors involved that determine the most effective method of protection, including a) available technical infrastructure, b) dedicated IT human resources, c) size of material assets, d) value of intellectual property, e) number of employees, and f) geographical market and many others. As such, it is virtually impossible to provide one cyber security solution that fits every company and every budget. In addition, even when a suitable cyber protection solution is in place, it suffers from an unavoidable security alert overload. In the third quarter of 2016 alone, Panda Labs reported 18 million new malware samples captured, an average of 200,000 each day.[26] This translates to several thousands of alerts per year for every company. Commercial companies however, have limited human and technical resources, inadequate know-how and insufficient expertise to investigate all security alerts, leaving them with an effective investigation capacity of 4-5%, that has the potential to miss the threat by a huge margin. Therefore, in the eyes of an entrepreneur, who tends to take decisions based on a margin of profit and risk principle, a cyber protection solution that yields such low reliability results is not justifying the investment of millions of dollars.

f) Cost of rectification if no implementation

Questioning the effectiveness and reliability of cyber protection solutions versus the frequency and potential severity of a cyber-attack presents a valid argument, which cannot be elaborated further as it is not the topic of this paper. What every entrepreneur needs to judge before taking a decision, is the post cyber-attack fallout. A cyber-attack insurance could have been procured, which could cover a majority or even a portion of the financial damage incurred, depending of course on the severity of the attack. Despite the potential existence of insurance, there are multiple factors that need to be assessed, that include short term and long-term costs. Short term costs, would arise immediately after the attack and would include among others, a) physical damage to property or equipment, b) injuries or loss of life, c) business interruption, d) forensic investigation, e) legal fees, f) public relations for damage control, g) customer notification, and h) procurement of cyber security protection if not already existing. The values of the long-term costs are subject to the severity of the attack and would be associated to the impact on the business and reputation of the company.

[26] "Cybercrime Reaches New Heights in the Third Quarter," *PandaLabs*, 20 October 2016 at http://www.pandasecurity.com/mediacenter/pandalabs/pandalabs-q3/

In reality, these long-term costs could be much more expensive and damaging than the cyber-attack itself, as they would include among others, a) radical corporate reorganization, b) attribution of liability for negligence to the management, c) third party litigation for clients and injured personnel, d) total or partial reimbursements, e) payment of damages for breach of contract, f) loss of clientele, g) loss of revenue, h) damage to the reputation of the company, i) devaluation of share price, j) loss of product market and k) loss of geographical market. Accordingly, in an extreme scenario, a high-end cyber-attack has the potential of destroying the competitive advantage of even the largest of companies.

Conclusion

The maritime supply routes are the state's lifeline both during peace and war. During peace, they stimulate the economy and keep the population content. During war time, they are an essential, if not indispensable part of the state's defence. In a scenario where the offensive action is located in a different country separated by sea, the maritime supply routes become vital for the transportation of troops, ammunition and heavy military equipment. In a sense, without the maritime supply support, a large-scale war effort overseas would not be feasible or possible. In military scenarios, where the need of a certain number of troops and equipment surpasses the capacity allowed by the military freight and troop transport systems, the merchant navy is called upon to fill the capacity gap. Hence, the merchant navy assumes a military role, although not based on military infrastructure regarding cyber security.

An effective cyber-attack would exploit the network vulnerabilities upon which a state's infrastructure is founded on, such as the ability to resupply itself in economic and military terms. As the transportation and distribution of commodities tend to evolve towards the direction of an unmanned process, it becomes imperative for the state to control its proper functioning.

The civilian and military maritime infrastructures are critical for the survival of the state either during an economic race or a military conflict. As they are interdependent, they should both be included in the definition of critical infrastructures, and the state should equally take all necessary steps to protect them. Currently, the maritime sector is left by the state to shipowners and operators to protect at their discretion but without establishing mandatory minimum requirements to effectively secure it against cyber-attacks. The shipowners and operators on the other hand, are not proactive against cyber threats, either because these attacks are not recognized as such or because protection against them is too expensive and time consuming.

A popular saying states that "the strength of a chain is measured by its weakest link". Hence, the state and its military, is regarded as a chain itself. Its weak points if targeted, result it total cohesion failure and inability for effective management of any situation.

Biographical Note

Dr. Elena (Helene) Mandalenakis obtained a B.A. in Political Science from McGill University in Canada and was awarded with a Masters' degree in European Studies from the Katholieke Universiteit Leuven (KUL) in Belgium. She received her Doctorate in Political Science from McGill University. Her doctorate research was supported by the Research Group on International Security (REGIS) of McGill University and Université de Montréal with scholarships and fellowships from the Greek-Canadian Association and McGill University.

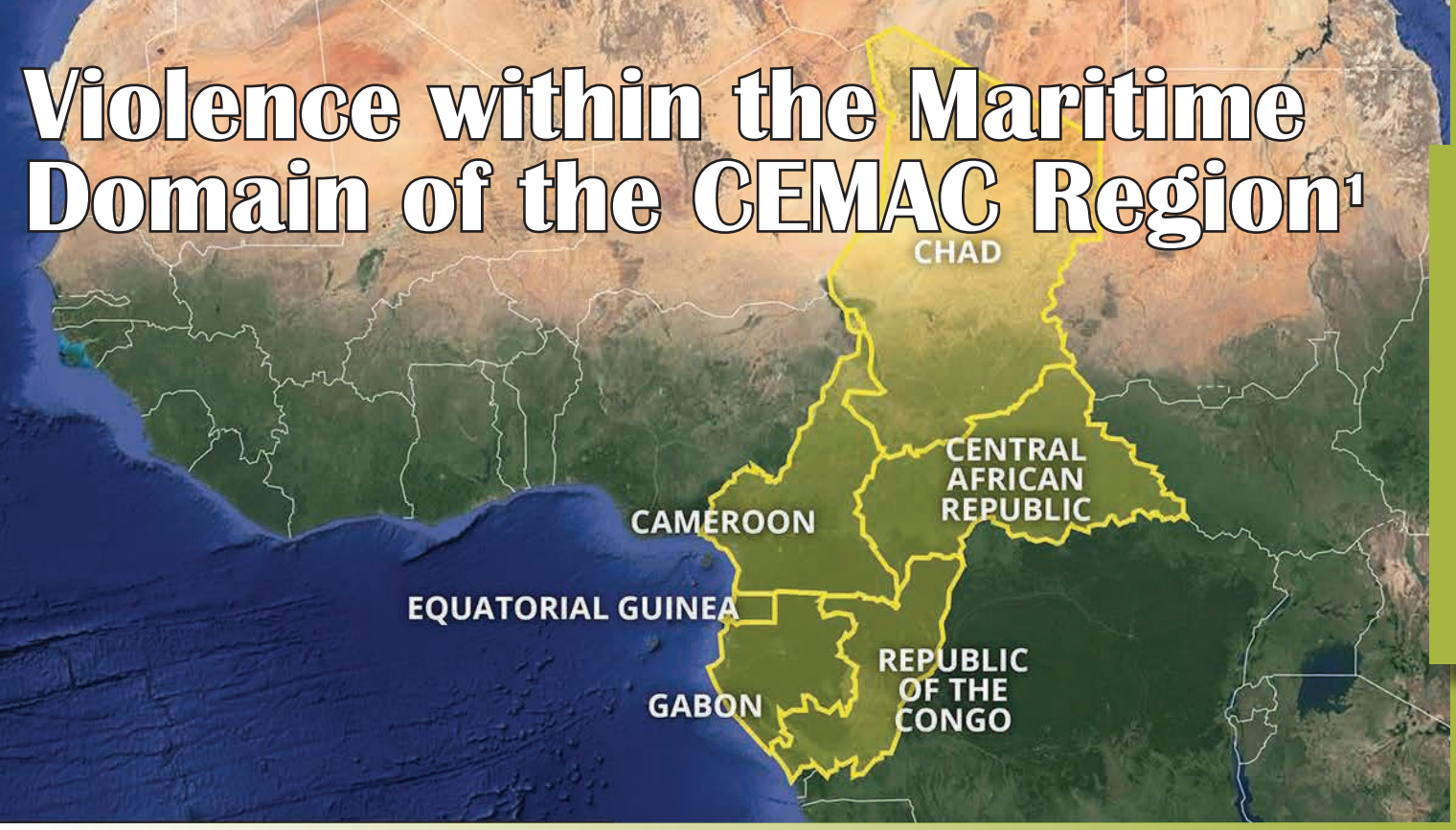
She has been a researcher –Fellow and Associate- at the Institute of International Relations of Panteion University and McGill University.

Dr. Mandalenakis' teaching experience includes courses on foreign policy, international political economy, European and EU politics as well as on minorities at McGill University and the University of Peloponnese.

She has presented her research in international conferences and has published in peer-reviewed academic and policy journals as well as in books on issues of foreign and security policy, cybersecurity, conflict resolution, migration, ethnic relations, state formation and identity, European affairs and resource management. Her current research interests involve international, regional and European security, cybersecurity, European affairs, policy formation, international migration, and identity.

Dr. Mandalenakis is a member of the "Regional Stability in the South Caucasus" Partnership for Peace Consortium Study Group of Defense Academies and Security Studies Institutes (PfPC) and participates in the "Regional Stability in South East Europe" and "Emerging Security Challenges" PfPC Groups

Violence within the Maritime Domain of the CEMAC Region[1]



by Akah Judith Ewo épouse Ndze
Dalaklis Dimitrios

Abstract

A practical consideration of the concept of maritime violence in relation to the Central African Economic and Monetary Community's (CEMAC) maritime space is provided. This is achieved through an examination of the relevant definition under international law, as well as a discussion of the factors accounting for its emergence and growth, including the respective characteristics of manifestation. Acts of maritime violence within the CEMAC maritime areas that have already captured the attention of the international community and the mass media of communication interest include piracy, armed robbery against ships and terrorism. The overall impact of those phenomena is considered, along with both national and international cooperation measures adopted by the countries of the CEMAC region to stem it. The methodology adopted is a literature review of existing primary and secondary sources, realized through traditional library and archival research in Sweden (Malmo) and in Cameroon, including the use of online sources. An important finding is that the causes, effects and challenges of such violence in the countries of the CEMAC region are common in nature and sometimes interrelated. The conclusion and recommendation section points to the need to enhance the current level of cooperation efforts of the countries involved; it also emphasizes the need to explore an additional portfolio of solutions towards stemming maritime violence, working in parallel with the already implemented efforts.

Introduction

Security at sea is challenged by numerous threats. In recent years, there has been global concern for maritime security, considering that an extended number of violent acts are committed at sea, such as armed robbery against ships, maritime terrorism, (maritime) interstate disputes associated with threat and/or use of violence, trafficking of narcotics, people and illicit goods, or arms proliferation. Illegal fishing, various environmental crimes and even maritime accidents associated with disastrous consequences can also negatively impact upon both the safety and security domains (Bueger, 2014, p. 1). The above mentioned un-

[1] The World Maritime University (WMU) in Malmö, Sweden is a postgraduate maritime university founded by the International Maritime Organization (IMO), a specialized agency of the United Nations. The analysis at hand is an adaptation of a Thesis submitted by Ms. Akah in November 2017, to fulfill the requirements of WMU's Master of Science (MSc) in Maritime Affairs degree. The leading author is a diplomat by training and is currently serving at Cameroon's Ministry of External Relations, where she is the Sub-Director in charge of Cameroon's relations with Nigeria. Dr. Dimitrios Dalaklis joined WMU in the summer of 2014, upon completion of a twenty-six years distinguished career with the Hellenic Navy (HN). He is serving as an Associate Professor, focusing on the extended Maritime Education and Training (MET) domain, as well as maritime safety & security issues.

lawful phenomena have steadily been on the forefront of attention, causing enormous damage to human life and property, with great negative impacts on international trade, peace and security.

According to the Oxford Learners' Dictionary, security involves the act of protecting a country, infrastructures/ buildings or persons against attacks, danger, etc. But, beyond this simplistic definition, maritime security can be viewed as measures put forth to respond to collective needs for order and protection from internal and external threats in the oceans and from the oceans (Klein, 2011, p.2). From a maritime perspective, (maritime) security is a recent expression that became prominent after the September 11, 2001 attack; thus, it can be understood as a set of policies, regulations, measures and operations to guard against security threats within the maritime domain (Germond, 2015, p.1).

Maritime safety on the other hand, involves all measures put in place by maritime stakeholders (international maritime community, maritime administrations, insurance companies, ship-owners etc.) to ensure safety, prevent dangers and minimize the effects of any mishap when it occurs. The International Maritime Organization (IMO) addressed the complexity of these two domains under the Maritime Safety Committee by distinguishing appropriately between maritime safety and security. Thus, maritime safety is the act of preventing or minimizing the occurrence of accidents at sea, while security is related to protection against unlawful and deliberate acts (Klein, 2011, p.8). Criminal acts, which remain a reality today, are a major security challenge to the international community, especially in the Gulf of Guinea in terms of prevention and curbing the various manifestations/ management.

The Gulf of Guinea (GoG) covers a vast area (6000km of coastline) from Senegal to Angola with its influence extending upon over 20 sovereign coastal States (and islands), but also a few landlocked ones (Lindskov et al, 2015, p. 7). The region is comprised by the States of West and Central Africa (Angola, Cameroon, Congo Brazzaville, Gabon, Equatorial Guinea, Nigeria, Democratic Republic of Congo, Sao-Tome and Principe). It is of a certain geo-strategic importance, as GoG is the region's major shipping route and is significantly rich in natural resources, with oil/gas and various minerals standing out. In 2012, for example, it was estimated that the region under discussion produced approximately 4% of oil at global level and by 2015 it could supply a quarter of United States' (US) oil needs (IPI, 2014, p.2). This region also supplies significant quantities of petroleum products to Europe and Asia.

Despite, or because of these attributes, the GoG is facing numerous challenges caused by increasing maritime crimes often manifested at sea, but also related to land-based origins. In 2013, for example, the GoG surpassed the Horn of Africa in terms of piracy risk, since it was associated with the highest number of piracy attacks and armed robbery against ships that comprised 1/5 of all recorded maritime incidents globally (Osinowo, 2015, p. 2). This worrying rise in number of attacks off the coast of West and Central Africa resulted in the region being termed as the 'next piracy hot spot' (Dalaklis, 2012, p. 5) It is also indicative that the International Crisis Group (ICG) referred to it as 'The New Danger Zone' (ICG Report, 2012, p.1). Meanwhile, the peculiarity of attacks in this region is that they are more violent when compared with other regions of the world and Nigeria alone accounts for an average of about 87 attacks per year (Steffen, 2017, p.1). This figure is quite high in view of the fact that it moved up from previous years and many more incidents remain usually unreported. The maritime space within the CEMAC sub-region (especially the waters of Cameroon, Gabon, Equatorial Guinea, and Republic of Congo) is a portion of the GoG. Hence, insecurity within this sub-region can be understood against the backdrop of insecurity in the Gulf.

PART 1: MARITIME VIOLENCE IN THE CEMAC SUB-REGION

This part initially provides a geographical presentation of the Central African Economic and Monetary Community's (CEMAC) sub-region and then highlights the issue of maritime violence within the sub-region's maritime space as seen in the creation of a variety of structures aimed at addressing the continuous security challenges. Trend and characteristics of those security threats are also considered.

Section A: The problem

Maritime violence is a worldwide phenomenon and each 'hot spot' around the world has its own history, geography and other characteristics. The CEMAC region in Central Africa is geo-strategically situated in the Gulf of Guinea, at the West Coast of Africa. The maritime space within the CEMAC sub-region (which includes the waters of Cameroon, Gabon, Equatorial Guinea and the Republic of Congo) is an important area at a pivotal position in the Gulf of Guinea - hence insecurity within this sub-region can be understood against the backdrop of insecurity in the Gulf of Guinea. The Gulf of Guinea is an area endowed with valuable resources and it is a strategic transport route for international shipping. The flow of international maritime trade in the CEMAC zone as well as import and export of vital goods are heavily dependent on the specific maritime corridor. This maritime space is faced with numerous threats to peace and security as a result of increasing acts of maritime violence such as piracy, armed robbery against ships and even terrorism.

CEMAC works hand in hand with other regional bodies like the Economic Community for Central African States (ECCAS) to prevent regional crisis, a priority for African Union in the maintenance of peace and security in the

continent. These Central African regional bodies have major security structures established to tackle maritime threats in the sub region. In terms of security structures, the Horn of Africa (Somalia) and the Gulf of Guinea are the main maritime sceneries in Africa that witness numerous and severe acts of violence/ criminality at sea. The waters of the CEMAC region falls within the maritime landscape of the Gulf of Guinea, where attacks are most visible in the maritime zones of Cameroon, Congo, Equatorial Guinea and Gabon (Ingerstad & Lindell, 2015, p.1). It is therefore important for States in the region to ensure security within the maritime space as maritime insecurity has far-reaching socio-economic and political ramifications that transcend national borders.

In the Central African sub-region, CEMAC and ECCAS are the two regional economic communities that address the issues of peace and security (Meyer, 2011, p. 9). Created in 1983, with a special emphasis on enhancing Central Africa`s region Peace and Security, ECCAS works in parallel with CEMAC on maritime safety and security issues; seven (7) member-states of ECCAS have coast in the Gulf of Guinea, with four (4) of them being CEMAC member-states. An inter-regional coordination center (the Regional Centre for Maritime Security in Central Africa (CRESMAC)) was created in Cameroon to link ECCAS and the Economic Community of West African States (ECOWAS). Also, the Africa Law Enforcement Program was initiated by the US Department for Homeland Security and the US Coast Guard, to help build maritime law enforcement and capability to detect and deter illicit activities within the Gulf of Guinea (Shafa, 2011, p.13). Additionally, the Maritime Organization of West and Central Africa (MOWCA) and the Gulf of Guinea Commission are institutions established to ensure integration and coordination of maritime activities (Lindskov et al, 2015, p.28). Meanwhile, IMO in collaboration with MOWCA established a sub-regional Integrated Coast Guard Network for West and Central Africa in order to tackle security challenges within the region.

Therefore, there are two (2) major security institutions that are engaged into tackling maritime security issues in the Central African sub-region: CRESMAC and MOWCA. CRESMAC`s security agenda began in 2009 when it was institutionalized by the International Coordination Centre for Central Africa (ICC) with headquarters in Congo. It is aimed at creating an integrated maritime security strategy needed to effectively respond to emerging security threats (Ujeke et al, 2013, p.24). CRESMAC promotes information sharing, joint patrols/surveillance of maritime space, as well as harmonization of actions at sea. Furthermore, MOWCA`s major objective is to tackle all maritime matters that are regional in character. It has an information communication center to ensure control and flow of information between member-states, as well as an intelligence gathering capacity to help them gain a better understanding of threats and security trends in the region (Shafa, 2011, p.20).

Following the increase of maritime security threats in the CEMAC sub-region, in June 2013, a milestone was achieved when Heads of States of West and Central African States (ECOWAS and ECCAS) as well as the Gulf of Guinea Commission met in Yaounde to adopt the respective Code of Conduct; they also adopted a Memorandum of Understanding (MoU) to prevent and suppress illegal acts perpetrating the GoG states (Michel Luntumbue, GRIP report, 2016). Considering the above, it is safe to point-out that maritime violence is both a reality and a challenge in the CEMAC sub-region; constant efforts made by organizations and involved nations individually testify the need to continue to find ways and means of curbing this continuous challenge.

Section B: Trends and characteristics

During the entire period from the early 1990s to 2008, minor incidents of violent crimes or petty thefts occurred in the coastal waters of the countries of the CEMAC region (Cameroon, Equatorial Guinea, and Congo); more importantly, these types of activities remained at very low levels. Indeed, Professor Ntuda Ebude has already correctly pointed out that piracy and armed robbery against ships actually started along the Cameroon coast during the 2nd half of the 1990s, but remained concentrated around the Bakassi oil exploitation areas (Ebode, 2010, p.82).

Bakassi stands out distinctly from other coastal areas between Cameroon and Nigeria (as well as the CEMAC zone) in terms of piracy and armed robbery against ships, as various armed groups operating within/around this area have often used grievances associated with the Bakassi conflict as a pretext for their actions. A typical example of what these criminal gangs can do is the hostage taking in 2008, when the rebels of the Bakassi Freedom fighters launched an attack on the supply boat SS SAGITTA that resulted into the kidnaping ten (10) persons, seven (7) of whom were French, with two Cameroonians and one Tunisian around Bakassi and within the territorial waters of Cameroon (Ebode, 2010, p.82). This attack was significant, because it marked the beginning of a series of violent attacks that took place in the Cameroonian coastal waters between the period 2008-2009, extending to land with spillover effects to other neighboring states. The nature and frequency of these attacks underscores the fact that by 2009 there were signs of new characteristics of piracy in the GoG as activities of insurgents in the region expanded beyond the southern and western coast of Nigeria, attacking ships off the coast of Cameroon and neighboring coasts of the CEMAC region.

Concerning the specific case of CEMAC coastal states, which is the focus of the current analysis, the total number of actual and attempted attacks amounts to a total of 37 reported cases between 2010 and 2015. Studies demonstrate that the number of attacks during this period saw an overall downward trend with Congo witnessing the highest percentage (7.9%), followed closely by Cameroon with 3.3% and Gabon 1%. This downward trend in the Central African sub-region during that period is all the more significant when compared to West Africa, where Nigeria alone witnessed a 47.4% increase of attacks between 2010 and 2016. Generally speaking, although statistics on incidents of piracy and armed robbery in recent years are readily available based on IMB reports, details of these incidents are hard to cross-check, especially as around 50% of piracy in West and Central Africa remain underreported either because of the victim's desire for discretion, or lack of the necessary supervision (Mohamed & Abdel, 2015, p. 4).

In terms of features, Professor Ntuda Ebode has distinguished four categories of maritime violence occurring within the GoG (specifically in the coastal states of the CEMAC zone): a) those who steal from ships or vessels at ports such as 'petit bandits' roaming the ports in small or less organized groups with their actions generally less violent; b) those who operate on platforms generally at night involving mostly the theft of materials; c) those who target vessels at sea, usually organized groups carrying out well orchestrated actions such as hostage takings and being armed with heavy weaponry such as AK47 etc. and claiming to belong to politically motivated groups whose main objective seems to be to make money through maritime violence; and d) those who carry out unauthorized fishing (Ebode, 2010, p.82-83). However, Nincic has also pointed out that pirates operating close to the shores in the GoG area are generally heavily armed (Nincic, 2009, p. 5). Therefore, their attacks are often more violent there than in other piracy hotspots around the world.

PART II: CAUSES, EFFECTS, AND CONTROL OF MARITIME VIOLENCE

This part is divided into three different sections: section A is dealing with the causes of maritime violence in the CEMAC sub-region; section B is discussing the effects, while section C examines the various efforts being made to address the issue and its negative consequences.

Section A: Causes

The causes of maritime violence in the CEMAC sub-region can be discussed from the geographical, political, economic and social perspectives.

1. Geographical factors

The Gulf of Guinea is a vast area with difficult topography; the coastlines are typified by many creeks and tough highlands. Such difficult geographical features, coupled with the porosity of the area means that the said coastal region inherently provides advantage to pirates and armed robbers who take advantage of the geographical characteristics (numerous small in size islands; existence of the Bakassi Peninsula; mangroves close to the beach and the coastline, which make access difficult). Given that the pirates know the terrain more than anyone else, such features make the area an ideal hiding place for pirates as against those who seek to pursue them; this provides the pirates the opportunity to operate with a very high level of freedom (ICG Report, 2012, p.4). Simply put, these natural features of the area provide numerous hideouts and escape routes, which are very advantageous to pirates.

2. Political factors

Countries of the CEMAC region, like most African Nations, face problems of corruption, mismanagement, and lack of resources etc., which all impact on policy issues. The CEMAC maritime border area has not always

received the attention one would have expected from the governments of the region in terms of security, exploitation of resources and development efforts, among others. In fact, piracy incidents in Africa should not be simply considered as being the outfall of not maintaining good order at sea (Vreÿ, 2009, p. 20). This is the good old problem of bad ocean governance facing most African nations generally, which is often a reflection of bad governance on land as well. Regional instability as a result of state failure and bad governance leads to insecurity; insecurity on land can easily transform into maritime insecurity. It is no coincidence that according to Mohamed (Mohamed, 2015 p. 5): "pirates are not born at sea, but on land" (IPI report, 2014, p.2). For reasons of clarity, the political situation of the Bakassi peninsula crisis between Cameroon and Nigeria, is brought into discussion; armed groups which have been fighting against government forces have often extended their activities towards the sea; the peninsula became a 'safe haven' for pirates throughout the period that the involved countries could not agree on the maritime boundary in the area (Lindskov et al, 2015, p. 16). Noteworthy here is the fact that the porous nature of the CEMAC borders has proven unlikely to prohibit the political instability and militancy off the south-eastern coast of Nigeria from having an effect in CEMAC waters, hence the 'spillover effect' often mentioned by analysts or academics. Other maritime disputes in the CEMAC region include the Cameroon-Equatorial dispute over an island at the mouth of the Ntem River, and the dispute between Equatorial Guinea and Gabon in Corisco Bay (Shafa, 2011, p.12). The one time rebel standoff in Chad, political tension in the Republic of Congo and even claims of a coup d'état attempt in Equatorial Guinea, amongst other political threats, could all be characterized as emerging maritime threats for countries in the region (Vreÿ, 2009, p.23). Such disputes make it difficult to address shared security challenges and it is a self-explanatory fact that they create 'a window of opportunity' for criminals to carry out their activities.

3. Economic factors

It is basic knowledge that if there were no economic resources and maritime traffic was rather scarce within the CEMAC coastal region, criminal gangs would have little or nothing to go after. But, the Gulf of Guinea is very rich in resources. The CEMAC region, has a large population and abundant energy resources typified by the proximity of large oil producers (Nigeria and Angola), maturing oil producers (Congo Brazzaville), mature oil producers showing signs of decline (Cameroon and Gabon) and new oil producers (Equatorial Guinea and Chad); these West and Central African countries border an important sea lane that has vital connectivity with energy commodities (Vreÿ, 2009, p.20). Furthermore, a significant number of vessels are engaged in the necessary oil transport supporting activities.

4. Social factors

It is a very influential factor that difficult living conditions such as unemployment, coupled with a sense of neglect and abandonment could be a recipe for criminality both on land and at sea. Cameroon, for example, finds itself confronted by a threat from the Bakassi Peninsula where local inhabitants have felt excluded, abandoned and unhappy since the Peninsula was handed back to Cameroon (Vrey, 2009, p.23). Meanwhile, livelihoods of local populations are threatened by the continuous degradation of the coastal environment and hampering agriculture-fishing; this can easily explain the 'temptation' of the locals to

engage in illegal activities for survival (ICG, 2012, p.3). Also, growth of maritime crime is as a result of structural problems such as poverty of the great majority of the population alongside the wealthy elite, unequal distribution of wealth, socio-political tension and the grievances of the local communities (ICG, 2012, p.3). One way of understanding the poverty aspect is to recall that, at the local border area, youths that are more frequently involved in acts of piracy and armed robbery come from poor families and, because of their vulnerability, probably undergo some brainwashing before joining the criminal groups they belong to. The promise of reward, comfort and expensive cars, financial gains, luxurious consumer goods and weapons are strong motives; these unemployed youths are lured to engage in piracy, which has become a thriving business (Nincic, 2009, p.100). Furthermore, dense population in the coastal areas, urban disorder, and continuous rural-urban migration are exacerbated by economic disparities and conflict over resources is leading to violent opposition within communities. This existence of discontent is a fertile ground for the recruitment of criminal gangs, pirates and armed robbers (ICG, 2012, p.3). These social problems thus tend to fuel insecurity within the CEMAC maritime space.

Section B: Effects

Given the importance of the sea in terms of international trade and the exploitation of resources, there is no doubt that insecurity within any international route such as the CEMAC maritime space is bound to exercise negative impacts of one form or another, not only locally, but also internationally. These impacts may be political (national or transnational) or socio-economic.

1. Political impact

Maritime violence within the CEMAC maritime space is often perpetrated by armed gangs who advance political grievances as a reason behind their action, particularly with respect to the Cameroon-Nigeria Bakassi conflict. The Bakassi freedom fighters, for example (who operate within the Cameroon-Nigerian maritime space) use deliberate campaigns or attacks at sea to influence political decisions thereby extending their political agenda offshore although their interests are driven by a combination of greed and grievances (Neethling, 2010, p.101-102). While the intention may not be to dwell on the complexities of the Nigerian political situation as it relates to this conflict, suffice is to note that there is a clear interrelation as unfortunately its impact is not limited to the two countries but spills over to other neighboring States in the CEMAC coastal waters.

2. Economic impact

Piracy and armed robbery against ships within the GoG and the CEMAC maritime space in particular obviously have certain socio-economic consequences. Professor Neethling has stated that the best armed groups operating within this region were responsible for attacks on oil pipelines of multinational corporations and also on vessels chattered by oil international exporters; vessels in neighboring states have likewise come under attack for achieving 'an easy and quick profit'. While the cost to the international community of maritime violence may be important in terms of monetary losses and energy or other resources, other costs this phenomenon can impose are less frequently considered (Nincic, 2009, p. 5). The analyst Anna Bowden examined the economic cost associated with maritime piracy and armed robbery against ships in terms of "Direct Economic Cost of Piracy" and "Secondary (Macroeconomics) Costs". The former comprises the cost of ransom payment, insurance cover, re-routing, warning security equipment, navigational force, prosecution of pirates and pre-emption, while the later concerns the cost of regional trade, food price, inflation and foreign revenue (Bowden, 2010, p. 8-19). These costs are most indicative of how costly piracy and armed robbery against ships could be.

3. Social impact

The social impact of maritime violence should be viewed in the context of poverty, political marginalization, and even armed conflict over oil. The plight of the coastal population of the CEMAC states is an important issue

as they rely mostly on fishing for their livelihood. Most of the populations living around the area generally live under difficult social condition due to the factors related to their immediate environment and respective countries. Also, pirate attacks are not limited to oil transport facilities but extend to fishing boats as well, leading to a hike in sea food prices due to scarcity of fish, an important source of protein to the citizens (Nincic, 2009, p.8).

Section C: Measures

This section discusses measures taken to protect the CEMAC maritime zone against on-going maritime violence. Such measures certainly exist at the national level, but also extend well beyond that.

1. National measures

CEMAC coastal states, like other coastal states around the globe, do have within their borders traditional institutions responsible for fighting piracy and armed robbery against ships, although it may be necessary sometimes to adapt these institutions to cope with the new challenges. Governments of these coastal states have different policies on maritime security threats, since they suffer different impacts at different times. For some, this security threat endangers the national economy; but, others consider it a relatively small-scale trans-border crime that does not destabilize the economy (ICG, 2012, p 5). Basically, because security issues transcend national geographical and political boundaries, cooperation between states at the bilateral level is necessary or even imperative.

As a result, Cameroon, Gabon, and Equatorial Guinea (which are the major coastal states in the CEMAC region), have made efforts in recent years to recruit more personnel that will deal with security duties at sea, acquire new equipment and better train their navies/coastguards. These traditional measures in terms of specific institutions include, for example, Cameroon`s Department of Maritime Affairs and Inland Waterways which is the contracting authority of Cameroon in dealing with the IMO over maritime issues while cooperating with other relevant institutions in the country on maritime crimes. There are also institutions like the Ministry of Defense (with the Navy patrolling the coast) and the 'Gendarmerie' also intervenes in certain reported cases (Ebode, 2010, p.83-86).

2. Regional measures

UNCLOS 82, the most instrumental document on ocean governance points out the need for States to cooperate in fighting piracy. Indeed, article 100 of the convention puts forward the following: "All states shall cooperate to the fullest possible extent in the repression of piracy on the high seas or in any other place outside the jurisdiction of any state". Cooperation consists of many actors in the international society, jointly acting or working together for a common purpose. The states of the CEMAC region have traditionally maintained high level summit dialogue to solve problems of insecurity. In fact, the CEMAC states are deeply involved in regional cooperation while remaining committed to international efforts. This sub-regional cooperation in the CEMAC zone could be seen, for example, in the drafting of legislation concerning piracy (the case of the CEMAC Merchant Shipping Code).

Further, as members of the Maritime Organization of West and Central African States (MOWCA), the CEMAC states have been active within the organization in addressing maritime security issues that could be helpful in their own maritime space. For example, in 2008, during a MOWCA meeting held in Abidjan, the creation of an integrated sub regional network of West and Central Africa Coast-Guards was envisaged. This would enable member states to reinforce cooperation among national coast guards and help them to deal more efficiently in their fight against security problems (MWOCA 7th session, 2011, p.3). Meanwhile, as states of the CEMAC region are important African Union (AU) members, they make their voices heard within the AU in terms of addressing issues that have to do with maritime security. It is important to remember that, at the 15th ordinary session of the assembly of the Conference of Maritime Transport Ministers of the AU that held in Kampala, Uganda, 28th July 2010, member states agreed to promote bilateral and multilateral cooperation as well as develop and promote mutual assistance and cooperation between state parties in areas of maritime security and safety (African Union, 2010).

3. International Cooperation

Cooperation of CEMAC states with major countries around the world such as China, various EU members -with France standing out- and the US are relevant with respect to stemming maritime violence within the CEMAC maritime space. The growing role of France and USA for example, to assist and contribute to safety and security in the CEMAC maritime space is becoming more and more visible, as these countries have established permanent naval presence for training and operational purposes that constitute vibrant maritime partnership in the CEMAC region and GoG in particular (Vrey, 2009, p. 26). Furthermore, states of the CEMAC region try to deal with the issue of maritime violence within the context of international organizations like UN and IMO. The fact that CEMAC country members are members of the UN ipso facto implies that the countries participate in efforts made by UN to address issues concerning piracy and armed robbery against ships whenever they may occur within the region. The peculiar case of Somalia illustrates how this may occur (e.g. UN Security Council Resolutions 2018 of October 2011 and 2039 of February 2012 calling on states to take active part in fighting piracy by deploying naval vessels and aircrafts to the Horn of Africa and cooperate with the transitional federal government of Somalia towards this end).

Conclusions and recommendations

a) Conclusions

Maritime violence within the CEMAC maritime space has been a problem since the early 90s. It became rather prominent after the major outbreak of the Bakassi conflict between Cameroon and Nigeria in 1993, as the effects of that war spilled over to the neighboring states. Although there were pre-existing factors conducive to the emergence of the maritime violence phenomenon, such as the geographical configuration of the area, developments such as persistent and protracted conflicts/rebellions in some states of the CEMAC region and the ICJ ruling of 10th October 2002 in favor of Cameroon over the Bakassi conflict also contributed into 'fueling' the armed groups and other criminal gangs operating within the CEMAC maritime space. Such groups used these developments as a pretext to carry out their violent attacks, kidnappings and hostage; negative spillover effects were discussed extensivly.

There is no doubt that most of the acts of violence recorded within the CEMAC maritime space could be classified as piracy and armed robbery against ships (including instances of petty theft, of course). However, many of the acts of maritime violence perpetrated in this region tend to be very peculiar, in the sense that they sometimes involve extreme violence and ruthlessness and are partly carried out on land. Some of them are even perceived to be politically motivated, which means that speculating about terrorism may not be too far-fetched. What this means is that the socio-economic and political ramifications of these activities could be far-reaching indeed. The states of the CEMAC region ought to be cognizant of this fact and particularly within the context of the delicate political atmosphere that reigns between some of the states of the sub-region. The states of the region must therefore be more serious, in terms of enhancing current efforts and adopting more concrete, pervading and effective measures to stem the problem. If the situation is not controlled, the threats may grow to undermine political stability and economic development of the region and further undermine the African maritime reputation.

International cooperation efforts may be good, regional efforts better, but what may be best in this context seems to be situated at the level of national efforts as well as meaningful cooperation between the states of the CEMAC region. One may want to imagine, for example, what would be the situation where Cameroon, with cooperation from Nigeria, succeeded in effectively 'integrating' Bakassi and settling the different populations around the area, while Nigeria on its part, successfully addressed the complexities with the Niger Delta and the other states of the CEMAC region face with persistent conflict strengthen their efforts to address the issues. It is safe to say that this would go a long way towards curbing piracy and armed robbery against ships within the CEMAC maritime space. Meanwhile, CEMAC nations must constantly remind themselves of the importance of each and every legal instrument dealing with maritime security - e.g. relevant provisions of UNCLOS82, SOLAS and the ISPS Code, SUA 88, etc. – hence the need for these nations not only to become party to such instruments but to effectively implement them at the national level and through cooperation with other countries.

Effective bilateral cooperation requires that decision makers in the states concerned come together to 'chart modalities' necessary for achieving their objective. Constant evaluation is also a key imperative, since the maritime sector is dynamic and constantly presents new challenges. Bilateral cooperation is a process that requires a great deal of goodwill on the part of the states concerned as the challenges facing the states of the CEMAC region are numerous and complex reason why the nations must indulge in genuine cooperation with each other and avoid making politically motivated decisions that address internal short-term and immediate priorities as opposed to long term sub- regional goals.

b) Recommendations

As stated by the famous author and clergyman Alphonso R. Bernard, if you don't have a vision for the future, then your future is threatened to be a repeat

of the past. It is therefore important to elaborate on the solution perspective that can be adopted to improve maritime security in the CEMAC maritime space. To effectively deal with maritime violence in the CEMAC region, a number of measures have to be improved, strengthened and reinforced. These include inter alia measures in the legal domain to begin with; the political and socio-economic domains are also important. Needless to point out, regional cooperation is deemed essential, as criminal acts of maritime violence transcends any physical and artificial boundary like states' borders.

1. Regional cooperation plays an important role in solving the problem of piracy and armed robbery against ships. This has already proven successful in the straits of Malacca and Singapore where the Regional Cooperation Agreement on Combating Piracy and Armed Robbery against ships in Asia (ReCAAP) has been an effective example that IMO recommends other states especially in the GoG to emulate (Maximo Q. Meija, 2012, p.37).
2. The states of the CEMAC region in collaboration with ECCAS, ECOWAS and the GoG Commission need to strengthen coordination of legal efforts as stated in the Memorandum of Understanding between member countries of West and Central African states by ensuring a comprehensive review of the legal framework of each member country. This approach will enable states to effectively apprehend, prosecute and trial the arrested maritime criminals. Continuing the discussion of how to strengthen the relevant judicial support, involved states should also work towards the establishment of courts 'tailor-made' to deal with piracy and armed robbery cases cases (Mohamed, 2015, p.8); zonal coordination mechanisms for a common understanding and prosecution of cross border and territorial crimes is also necessary.
3. As an additional solution, states of the sub-region should think of acquire and operate fixed and/or rotatory maritime patrol aircraft(s), further enhancing their capabilities of ship borne patrols and invest in ground and satellite based surveillance asserts for constant observation, monitoring and surveillance to secure the maritime space.
4. Maritime violence originates from land as a result of socio- political lapses in most African states such as poor governance, youth unemployment, unequal distribution of wealth, and accumulated grievances of the local population as a result of neglect, poor coastal and environmental protection. It is therefore important for states of the CEMAC region to ensure good governance; dealing with these 'social deficits' is one of the most effective ways of solving problems and tackle the root cause of the problem.
5. Another pertinent point could be the need of greater awareness and sensitization of the population on maritime issues. This can be done through popularization of research findings on maritime violence by governments via sponsorship of radio and television programs, or even seminars and workshops as well as seek ways and means of sorting out the practical difficulties that go with using military means to curb maritime violence (Ndze, 2015, p. 69)
6. The states of the CEMAC region should ensure optimal implementation of international and regional instruments such as the GoG Code of Conduct, as well as prepare themselves now and in the future to be able to adequately address issues of maritime violence through relevant information sharing and reporting, or implementing joint patrol schemes, amongst others.The states of the CEMAC region should ensure optimal implementation of international and regional instruments such as the GoG Code of Conduct, as well as prepare themselves now and in the future to be able to adequately address issues of maritime violence through relevant information sharing and reporting, or implementing joint patrol schemes, amongst others.

REFERENCES

African Union. (2010). Revised African Maritime Transport Charter, 27. Retrieved from http://www.peaceau.org/uploads/revised-african-maritime-transport-charter-en.pdf

Baldauf, S. (2012). Next pirate hotspot; Gulf of Guinea. The Christain Science Magazine. Retrieved June 18, 2012 from the World Wide Web: http://www.csmonitor.com/World/Africa/2012/0228/Nextpirate-hot-spot-the-Gulf-of-Guinea.

Bowden, A. (2010). The Economic Costs of Maritime Piracy. [Louisville, Colo.]: One Earth Future Foundation.

Bueger, C. (2014). What is maritime security? Marine Policy, 53(Murphy 2010), 159–164. Retrieved from https://doi.org/10.1016/j.marpol.2014.12.005

Chatham House Report. (2013). Maritime Security in the Gulf of Guinea. Report of the Conference Held at Chatham House, London, 6 December 2012. (Rep.). Retrieved https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/Africa/0312confreport_maritimesecurity.pdf

Churchill, R. R., & Lowe, A. V. (1999). The Law of the Sea (3rd ed.). Yonkers, N.Y, Juris: Manchester University Press.

Dalaklis, D., & Chrysochou., G. (2012). Small Arms and Light Weapons (SALWs) Illegal Trafficking: Another Challenge for Global Security. Hellenic Naval Academy. Department of Combat Systems, Naval Operations, Sciences of the Sea,

Navigation, Electronics and Communication Systems., Volume (4/2).

Dalaklis Dimitrios. (2012). Piracy in the Horn of Africa: Some good news, but a lot of work has still to be done…. Maritime Security Review, (9).

Ebode, N. (2010). Piraterie et Terrorisme: De Nouveaux Défis Sécuritaires en Afrique Centrale. B.P. 8106 Yaoundé, Cameroun: Presses Universitaires d'Afrique.

Germond, B. (2015). The geopolitical dimension of maritime security. Marine Policy, (54), 137-142. Retrieved from https://doi.org/10.1016/j.marpol.2014.12.013

Gilpin, R. (2007). Enhancing Maritime Security in the Gulf of Guinea. Retrieved August 20, 2017, from: http://africacenter.org/wp-content/uploads/2007/07/Enhancing-Maritime-Security-in-the-Gulf-ofGuinea.pdf

Ingerstad, G., & Lindell, M. T. (2015). Challenges to Peace and Security in Central Africa : The Role of ECCAS. Swedish Defense Research Agency.

International Chamber of Commerce. (2012). IMB notes increase in piracy off West Africa. Retrieved from http://www.icc-ccs.org/news/753-imb-notes-increase-in-piracy-off-west-africa

International Crisis Group (ICG). (2012). The Gulf of Guinea: The New Danger Zone. (Rep. No. ICG Report, (Africa Report N°195 – 12 December 2012).).

International Maritime Organization, (2010 January 19). Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery against Ships. Resolution A.1025 (26). Retrieved August 20, 2017. http://www.imo.org/OurWork/Security/PiracyArmedRobbery/Guidance/Documents/A.1025.pdf

International Maritime Organization (IMO). (2013). Strengthening Maritime Security in West and Central Africa. Retrieved from http://www.imo.org/en/MediaCentre/HotTopics/piracy/Documents/west africa Maritime Security.pdf

International Maritime Bureau. Annual Report (2010-2016). Piracy and Armed robbery against ships

IPI. (2014). Insecurity in the Gulf of Guinea: Assessing the Threats, Preparing the Response. International Peace Institute Report.

Kamal-Deen, A. (2015). The Anatomy of Gulf of Guinea Piracy. Naval War College Review, 1(68), 93-118. Retrieved from http://search.proquest.com/openview/f0b98e5688d45bd0185614601f823967/1?pq-origsite=gscholar

Klein, N. (2011). Maritime Security and the law of the sea. New York: Oxford University Press.

Kraska, J. (2011). Contemporary Maritime Piracy: International Law, Strategy, and Diplomacy at Sea (1st ed.). Califonia, USA: Praeger Security International.

Leke, S. K. (2012). Chapter 4. In The History and structure of CEMAC. Retrieved from http://wiredspace.wits.ac.za/jspui/bitstream/10539/11740/6/Chapter_4.pdf

Lindskov, J. K., & Riber, N. J. (2015). Maritime Security in the Gulf of Guinea. Retrieved from http://www.fak.dk/publikationer/

Mané, D. O. (2005). Emergence of the Gulf of Guinea in the Global Economy: Prospects and Challenges. 1-22.

Mayer, A. (2011). Peace and security cooperation in central africa Developments, Challenges and Prospects (Discussion Paper 56). Uppsala: Nordiska Afrikainstitutet.

Meija, M. Q. (2002). Defining Maritime Violence and Maritime Security. In Maritime Violence and other security issues at sea. (P. K Mukherjee, M.Q.Mejia & G.M. Gauci (Eds.) ed.). Malmo, Sweden: World Maritime University.

Meija, M. Q. (2012). Maritime Piracy: A Multi-Dimensional Issue: Exploring Linkages Between Economic Development, Political Stability and Maritime Piracy. (S.S Sida).

Michel Luntumbue. (2016). The Long March of African Maritime Safety and Security in the Gulf of Guinea (Rep.). Retrieved https://www.grip.org/en/node/2113

Mohamed, C., & Abdel, M. (2015). Piracy in Gulf of Guinea causes, efforts and solutions. Regional Maritime Security Institute, (AASTMT).

Mukherjee, P. K. (2002). Maritime violence and other security issues at sea: The proceedings of the Symposium on Maritime Violence and other Security Issues at Sea, 26-30 August 2002, Malmö, Sweden (1st ed.). Malmo, Sweden: World Maritime University.

Ndze, B. E. (2015). Effects of Maritime Violence on Cameroon`s Maritime Passenger Transport to Neighboring Countries (Unpublished doctoral dissertation). Regional Maritime University, Accra-Ghana. Retrieved from http://ugspace.ug.edu.gh:8080/xmlui/bitstream/handle/123456789/8213

Neethling, T. (2010). Piracy around Africa's West and East coasts: A comparative political perspective. Scientia Militaria South African Journal of Military Studies, 38(2), 89-108.: https://doi.org/10.5787/38-2-91

Nicoll, A. (2008). The Africa Partnership Station. The International Institute for Strategic Studies, 14(6), 1-2. Retrieved from https://doi.org/10.1080/13567880802390594.

Nincic, D. (2009). Maritime piracy in Africa: The humanitarian dimension. African Security Review, 18(3), 1-16. https://doi.org/10.1080/10246029.2009.9627538

Onuoha, F. C. (2010). "Piracy and Maritime Security off the Horn of Africa: Connections, Causes, and Concerns.". African Security Review, 3(4), 191-215.

Onuoha, F. C. (2012). Piracy and Maritime Security in the Gulf of Guinea: Nigeria as a Microcosm. Retrieved from http://studies.aljazeera.net/en/reports/2012/06/201261212321011333 3.htm

Onuoha, F. C. (2013). Piracy and Maritime Security in the Gulf of Guinea: Trends, Concerns, and Propositions. The Journal of the Middle East and Africa, 4(3), 267-293. Retrieved from https://doi.org/10.1080/21520844.2013.862767.

Osinowo, A. A. (2015). Combating Piracy in the Gulf of Guinea. Africa Security Briefs, 30, 1-8.

Patrick. (2007). Maritime Security in the Gulf of Guinea. JFR Forum, 45, 28-32. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a517524.pdf

Piracy increasing in West Africa, latest report shows. (2017, February 14). Retrieved from https://iccwbo.org/media-wall/news-speeches/piracy-increasing-in-west-africa-latest-report-shows/

Shafa, B. M. (2011). Maritime security in the Gulf of Guinea sub-region: Threats, challenges and solutions. 1-28. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA560829

Shaw, M. R., & Hunter, M. (2014). Comprehensive Assessment of Drug Trafficking and Organised Crime in West and Central Africa. Retrieved from https://www.google.pt/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCYQFjAA&url=http://www.globalinitiative.net/download/drugs/subsaharan-africa/ Organized Crime in West and Central Africa

Starr, S. (2014). Maritime Piracy on the rise in West Africa. Combating Terrorism Centre, Vol.4.

Steven, J. (2013). Maritime Security handbook: Coping with Piracy (M. Freeth ed.). London: The Nautical Institute. Steven, J. (2013). Maritime Security handbook: Coping with Piracy. The Nautical Institute., (M. Freeth, Ed.). Lamberth Road, London:

Talley, W. (2008). Maritime Safety, Security and Piracy (First ed.). London: Informa Law, Mortimer House.

Ukeje, C., & Mvomo Ella. (2013). African Approaches to Maritime Security - The Gulf of Guinea. Friedrich Ebert Stiftung: Peace and Security Series. Retrieved from http://library.fes.de/pdf-files/bueros/nigeria/10398.pdf

United Nations Convention on the Law of the Sea, 1982, Retrieved October 21, 2012 from http://www.un.org/Depts/los/convention_agreements/texts/unclos/unclos_e.pdf

United Nations Security Council Resolution 2018(2011, October 11). Retrieved October 8, 2012 from: http://www.securitycouncilreport.org/atf/cf/%7

United Nations Security Council (2012b, February 27). Gulf of Guinea Piracy 'Clear Threat' To Security, Economic Development of Region. Retrieved September 12, 2012. http://www.un.org/News/Press/docs/2012/sc10558.doc.htm.

United Nations Security Council Resolution 2039(2012c, February 29). Retrieved October 8 2012, from: http://www.un.org/ga/search/view_doc.asp?symbol S/RES/2039%20(2012)

Vreÿ, F. (2009). Bad Order at Sea: From the Gulf of Aden to the Gulf of Guinea. African Security Review, 18(3), 17-30. Retrieved from https://doi.org/10.1080/10246029.2009.9627539.

Wambua, P. M. (2009). Enhancing Regional Maritime Cooperation in Africa: The Planned End State. African Security Review, 18(3), 45-59. Retrieved from https://doi.org/10.1080/10246029.2009.9627541.

The NATO Cybersecurity Generic Reference Curriculum Application to the Maritime Environment

by Dinos Kerigan-Kyrou
Co-Author, NATO Cybersecurity Curriculum
Emerging Security Challenges Working Group, Partnership for Peace Consortium

At a United States Congress Border and Maritime Security hearing, US Coast Guard Rear Admiral Paul F. Thomas was asked his solution to the unique challenges facing the maritime environment arising from rapidly advanced, interconnected technology. RADM Thomas argued for a 'layered cyber protection strategy' incorporating cybersecurity within all aspects of the maritime environment.

The NATO Cybersecurity Generic Reference Curriculum[1] encapsulates this layered approach advocated by the US Coast Guard[2], cybersecurity must be integrated from the very outset, in all aspects of technology and human factors, not as an isolated 'end point' in a process. The NATO Curriculum is a generic reference programme applicable to a wide range of government, military, and commercial activity. It is based around themes crucial to the application of cybersecurity in the maritime environment. The themes include:

+ Cyberspace and the Fundamentals of Cybersecurity.
+ The Risk Vectors of Cybersecurity.
+ Cybersecurity Management.

How can the NATO Cybersecurity Curriculum be applied to the maritime environment?

Cyberspace, the Fundamentals of Cybersecurity and the Maritime Environment

Section one of the NATO Cybersecurity Curriculum examines how the constituent parts (or topology), of cybersecurity are interrelated and arranged. The maritime environment is increasingly dependent on integrated digital systems on-board vessels and within the land-based maritime environment.[3] As Elena Mandalenakis states: "Cyber systems are globalized, inter-connected and highly integrated." This fact exacerbates any disruption in a local system with "unforeseen risks and consequences." The success of maritime operations depend on the security of cyberspace. Dr. Mandalenakis gives the examples of the United States Arleigh Burke-class destroyer, first deployed in 1991 with a crew of 329, and the Zumwalt-class, deployed in 2013 with a crew of only 158, but with a tenfold increase in defence capabilities. The Zumwalt-class is, however, totally reliant on electronic, integrated systems for its military abilities and operational systems.[4] Likewise, civilian vessels are being digitalised and increasingly interconnected.[5]

The internet is the backbone of this interconnection. Contrary to popular belief there is no 'separate' internet for critical infrastructure such as energy, communications, or indeed maritime transport. The topography of cyberspace in the maritime environment consists of increasing dependence on integrated systems, connected online. So what of the possible vulnerabilities?

The Risk Vectors of Cyber

[1] The 'NATO Cybersecurity Curriculum' is part of Allied Command Transformation training. The programme was led by the Canadian Dept of National Defence Canada / Canadian Armed Forces, with the Emerging Security Challenges Working Group at the Partnership for Peace Consortium (PfPC). See: www.nato.int/nato_static_fl2014/.../20161025_1610-cybersecurity-curriculum.pdf

[2] RADM Paul F. Thomas, US Coast Guard. Evidence to: 'Protecting Maritime Facilities in the 21st Century'. Hearing before the Subcommittee on Border and Maritime Security; US House of Representatives, October 8, 2015. Serial No. 114–35, p.43.

[3] United States Coast Guard Cyber Strategy', Washington D.C.

security and the Maritime Environment

Cybersecurity Risk Vectors are identified as the key method of addressing cybersecurity concerns by the NATO Cybersecurity Curriculum. In the maritime environment one of the greatest emerging challenges is the security of the 'Internet of Things' (IoT), operated by Industrial Control Systems.[6]

The IoT consists of internet devices (or 'things'), receiving and transmitting data. These devices contain sensors and actuators able to perform critical functions. Most of these devices are, in effect, computers running software and 'firmware' (a computer program stored within the hardware).

The US and EU have highlighted particular concerns regarding the 'security vulnerability' of these devices.[7] A proposed US Bill ,'The Internet of Things Cybersecurity Improvement Act of 2017' , defines a security vulnerability as a "compromise of the confidentiality, integrity, or availability" of a device or its information.[8]

Due to commercial and legal concerns there is a great reluctance to share knowledge of these vulnerabilities. However, Stefan Lüders at CERN states that while hundreds of their IoT devices control power, security and research, 32% of CERN's IoT devices either crashed or failed when faced with the most basic vulnerability scan.[9] These IoT concerns clearly extend to the maritime environment. April Danos, of Port Fourchon Louisiana and the US National Maritime Security Advisory Committee, and a leading authority on maritime cybersecurity, underscores the challenge: "We are blind, useless and potentially locked out of our own house if we are hacked; and let's face it, it isn't 'if', it's 'when'."[10]

Modern vessel components increasingly comprise the Internet of Things connected to control systems via the internet. For example, the power management, loading and stability, container monitoring, alarms, bridge control console, Electronic Chart Display and Information System (ECDIS), Automatic Identification System, Navigation Decision Support (NAVDEC), Voyage Data recorders, Computerized Automatic Steering, and the Global Maritime Distress and Safety System (GMDSS).

Ports increasingly feature multiple examples of IoT including port security, access control, CCTV, gates, ID cards, automated cargo handling equipment, the Terminal Operating Centre, cranes, and integrated supply chain logistical systems. (Modern ports are rapidly becoming advanced logistical centres incorporating IoT into almost every function).[11]

Moreover, port IoT devices are directly interacting with vessels' IoT including communications, GPS (Global Positioning System), lock operations, maintenance and management, pollution and environmental control systems.[12]

How can cybersecurity vulnerabilities affecting the maritime environment arise?

+ Maritime operations can be deliberately targeted by a hostile military, pirates, and terrorists.

For example, research conducted by the University of Texas at Austin on 'spoofing' a vessel's GPS demonstrates modern navigation systems' vulnerability to hostile actors.[13]

And in 2012 Saudi Aramco and Qatar's RasGas, both of which are significant maritime operators, were victims of the 'Shamoon' and 'Flame' malware causing significant outage. Malicious software has also targeted oil rig stability off Africa and South Korea.[14]

+ A maritime operator can become victim to what the author calls 'Collateral Damage from a Non-Targeted Cyber Attack', where it is affected by malware not specifically targeted at them.

In July 2017 the shipping and logistics company A.P. Moller-Maersk was caught-up in the 'NotPetya' malicious software (or 'malware').[15] Maersk lost about $300m as a direct result of being unable to operate their booking system. (Indeed Maersk employees resorted to using the popular 'WhatsApp' messaging app to process customer bookings until the problem

[4] Dr. Elena Mandalenakis, "Political Implications of Cyber Space on State Power," 'NMIOTC - Maritime Interdiction Operations Journal', 13, no.2 (2016): 15-24; Available at: www.kenap.mil.gr/files/NMIOTCjournal13.pdf

[5] EU ENISA "Analysis of Cyber Security Aspects in the Maritime Sector," 2011 at: www.enisa.europa.eu/publications/cyber-security-aspects-in-the-maritime-sector-1/at_download/fullReport

[6] For further explanation of SCADA (Supervisory Control and Data Acquisition), and Industrial Control Systems see: Robert Radvanovsky & Jacob Brodsky, ed., 'Handbook of SCADA / Control Systems Security' (Boca Raton: CRC Press, 2016).

[7] EU ENISA: 'Security and Liability in the Internet of Things', June 2017, see: www.enisa.europa.eu/publications/ed-speeches/security-and-liability-in-the-internet-of-things

[8] United States Senate. 115th Congress, 1st Session. 'Internet of Things Cybersecurity Improvement Act of 2017'. See also concerns raised about IoT security by Senators Mark R. Warner and Cory Gardner, co-chairs of the Senate Cybersecurity Caucus, at: www.warner.senate.gov/public/index.cfm/pressreleases?id=06A5E941-FBC3-4A63-B9B4-523E18DADB36

[9] Dr. Stefan Lüders, CERN. Presentation at the ITU; available at: www.itu.int/en/ITU-T/studygroups/com17/Documents/tutorials/2012/11-CERNComputerandGridSecurityITU(2012).pdf

[10] Security Industry Association webinar, March 16, 2016 'Keeping Cargo Moving: Maritime Cybersecurity' with Brett Rouzer, US Coast Guard Cyber Command, and April Danos, Port Fourchon; available at: www.youtube.com/watch-v=2naiQd-U_kM

[11] or further information on port security see: April Danos 'Innovative Approaches using Information Technology' (2013), at: aapa.files.cms-plus.com/SeminarPresentations/2013AnnualConvention/Danos%2C%20April.pdf

[12] 'Keeping Cargo Moving' op.cit.

was solved).[16]

Maersk was not specifically targeted; nonetheless a victim of a 'Non-Targeted Cyber Attack' may sustain the same harm as if it were deliberately targeted. + A maritime operator can become an unwilling facilitator of crime via a cybersecurity breach.

In 2013 the EU's Europol police agency announced arrests had been made regarding a cyber attack on the Port of Antwerp. The criminals aimed to use the port's computer systems to facilitate their activities. This access enabled them to monitor the transport of a container holding over 1,000 kg of drugs.[17]

The cybersecurity breach was caused by 'phishing' emails, containing attachments with hidden malware, and also by physically breaking into the port's administration and placing 'keylogging' devices to capture passwords. The passwords were then used for remote access to the port's administration systems. They were able to clone swipe cards to access the quayside and the automated container stacking yard to precisely locate and transport their container before inspection by port authorities.

The Maersk and Antwerp examples demonstrate the interconnectedness of both 'administration' and 'critical function' cybersecurity. Critical infrastructure operators attempt to isolate these systems from one another via a process known as 'air gapping'. However, as these situations demonstrate, air gapping is difficult, perhaps impossible to achieve such is the cross-over between administration and critical functions.

A similar cyber attack could enable criminals or terrorists to utilise maritime facilities for trafficking humans, or for smuggling weapons and Chemical, Biological, Radiological and Nuclear (CBRN) materials.[18]

Cybersecurity Management and the Maritime Environment

The management of cybersecurity is a central part of the NATO Curriculum. Cybersecurity management in the maritime environment requires development of human factors and securing technology. Training and raising all employees' and contractors' cyber awareness is the first necessary step - developing an environment where cybersecurity is seen as each individual's responsibility, whether they are on-board a vessel or within the land-based maritime environment. Indeed, over 70% of cybersecurity breaches are caused by human factors - "people and process" not by the technology, according to Adrian Leppard, Commissioner of the City of London Police.[19]

[13] UT, Austin "UT Austin Researchers Spoof Superyacht at Sea" (2013), www.engr.utexas.edu/features/superyacht-gps-spoofing.

[14] Shamoon and Flame viruses target Windows operating systems. More information: "New wiper malware hits Middle East and Europe", in 'Computer Weekly', at: www.computerweekly.com/news/450414424/New-wiper-malware-hits-Middle-East-and-Europe

[15] See: "New Petya / NotPetya ransomware outbreak", 'Kaspersky Daily': www.kaspersky.com/blog/new-ransomware-epidemics/17314/

[16] "Moller-Maersk puts cost of cyber attack at up to $300m" in, 'Financial Times', August 16, 2017.

[17] 'Europol EC3 'Hackers deployed to facilitate drug smuggling' www.europol.europa.eu/sites/default/files/documents/cyberbits_04_ocean13.pdf

[18] For more information on CBRN see: Brg Gen (ret'd) Galatas Ioannis MD, 'CBRNE Terrorism Newsletter', at: https://www.cbrne-terrorism-newsletter.com

[19] Commissioner of City of London Police, Adrian Leppard, speaking at meeting of CSARN, London, May 2014.

[20] Dinos Kerigan-Kyrou 'Critical Infrastructure: Cybersecurity and Organization'; presented at the 'Critical Infrastructure Resilience conference, UK Security Expo', London, November 2016.

[21] See: RADM Paul F. Thomas, US Coast Guard, op.cit.

It is crucial that all maritime employees are able to identify cybersecurity concerns as early as possible in a 'no blame' environment, so that a problem is identified and dealt with when the problem is 'small' before it becomes 'big'. (Indeed, the maritime and aviation industries already do this in matters concerning operational safety). The IT departments will continue to remain crucial, but identification of a problem is a responsibility concerning every individual; not a single employee or contractor now has a role that can be considered separate from cybersecurity.[20]

Managers and directors may need to further understand that cybersecurity is as integral to successful operations as logistics, fuel supply, or safety. Indeed, incorporating cybersecurity into safety and security, rather than having it perceived as an isolated cost centre, is central to the development of maritime cybersecurity.[21]

As the maritime industry progresses toward an environment consisting of the Internet of Things, the suppliers of components and devices need to play a much greater role in ensuring their products' security.[22] CERN's Stefan Lüders points out that there is presently no device standard or verification system for IoT.[23] Until one is developed the author proposes that the standard for Information Security Management Systems (ISO 27001:2013), is used as a guideline for the maritime industry to verify software, control systems, and the multiple IoT devices that the maritime industry increasingly depends upon.[24] The maritime industry, possibly in close collaboration with EU ENISA (the EU's cybersecurity agency based in Heraklion, Crete), and the US Dept of Homeland Security may wish to develop a testing programme for maritime interconnected devices. While 100% security can never be guaranteed, the industry may need to exert greater influence on device suppliers to ensure the robustness and resilience of components.

Finally, improving cybersecurity information sharing across the maritime environment may greatly help. Indeed, the US has developed an excellent platform for industry to share cybersecurity threats and challenges, US-CERT.[25] Likewise, the EU's 'Network and Information Systems Directive' will compel critical infrastructure operators to share cybersecurity breach information.[26] Further engagement by the maritime industry with EU Europol's EC3 Cybercrime Centre and ENISA will help both minimise the occurrence of cybersecurity problems and limit the damage when they do occur.

Summary

The NATO Cybersecurity Generic Reference Curriculum makes clear that achieving the highest standards of cybersecurity is a multifaceted task, requiring a layered approach concerning human and technological factors. It requires an understanding of the fundamentals of cybersecurity, its risk vectors, and the management of these risks. As Major General Stefano Vito Salamida states on behalf of Supreme Allied Commander Transformation: "I am convinced that it can serve as a reference for partner countries in the design and development of course models and programmes for professional Cybersecurity military education. It will also serve as an enhancement of military interoperability between NATO and its partners and strengthen the collaboration on a responsive education and training system. It is my pleasure to support the PfPC Emerging Security Challenges Working Group through publishing this Cybersecurity Reference Curriculum as a NATO document." The NATO Curriculum is a training programme that is fully adaptable to the maritime environment

[22] Freely available software through the Open Vulnerability Assessment System (OpenVAS), include 'Metasploit' vulnerability scanning and 'Kali Linux' penetration testing software to test the robustness and resilience of IoT products.
[23] Lüders, op.cit.
[24] This is known as a Second Party audit, or 'an audit on suppliers'. See: International Standards Organization, ISO 27001:2013.
[25] See: www.us-cert.gov
[26] EU 'Directive on Network and Information Systems, 2016' See: www.ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

Dr. Dinos Kerigan-Kyrou CMILT
Co-Author, NATO Cybersecurity Curriculum
Emerging Security Challenges Working Group of the Partnership for Peace Consortium

Dinos is a member of the Emerging Security Challenges Working Group, an external consultative body to NATO's Emerging Security Challenges Division, based at the Partnership for Peace Consortium in Garmisch, Germany. He is a visiting lecturer at the University of Greenwich and is responsible for the cybersecurity division of the Senior Command & Staff Course at Defence Forces Ireland. Dinos holds the ISO 27001 lead auditor certificate for Information Security Management Systems, and is a Chartered Member of the Institute of Logistics and Transport. For several years he conducted training at the NATO School Oberammergau to NATO and Partnership for Peace military and civilian staff on subjects including cybersecurity, energy security, and critical infrastructure resilience. He previously worked for many years in aviation law and policy at British Regional Airlines, and then as Communications Director for CANSO, the organisation representing Air Traffic Management providers. Dinos is on the editorial board of 'Connections', the Journal of the Partnership for Peace Consortium. Dinos has a PhD in European Union law. He is an active member of the Hellenic Community of Ireland.

Biometrics in Support of Naval Units to fight Piracy and Terrorism

by Lieutenant Commander Ioannis Argyriou GRC (CG)

Introduction

The maritime environment that NATO faces today is complex and often comprised of unconventional, irregular, and hybrid elements. This human-centric environment contains terrorists, insurgents, influential leaders and clandestine state-sponsored groups hidden among civilian populations and is complicated by multiple levels of associations and complex human factors. The security environment is likely to contain a broad and dynamic set of challenges where adversaries and other actors alike compete with each other across a broad range of environments. Commanders should seek a deeper understanding of these challenges. Intelligence is crucial to develop this understanding by providing the insight and foresight commanders need to make decisions.

Maritime shipping is an integral component of the global economy, and is inextricably linked to both national prosperity and international cohesion. In order to take all the necessary measures to ensure the safe transportation of people and goods in the marine environment, we must first be aware of illegal activities and threats that occur at sea. Such prohibited activities include acts of terrorism, piracy, armed robbery, acts of violence against maritime navigation, potential quarantine situations, drug trafficking, migrant smuggling, unsafe transport of migrants, transport of wanted felons and/or terrorists, arms trafficking, unresolved radiation alarms, and illegal fishing. The legal implications of these actions depend on the maritime area in which the illegal act is committed.

Terrorists and pirates consistently use the maritime environment to achieve their goals. Cooperation of all stakeholders in the field of security is essential in order to reduce piracy and terrorism.

These maritime challenges are often interrelated and require governments to develop multi-national solutions rooted in International cooperation. Cooperation amongst nations and international entities is not always easy, with economical, political, and social constraints impacting the willingness and ability to act. Improving cooperation within NATO on maritime security concerns is a vital issue. NATO needs cooperation in all areas to strengthen its response to threats to maritime security.

Piracy and terrorism

Piracy

The issue of piracy has affected the the merchant community throughout history and continues today. The causes, consequences, and methods of addressing piracy are of primary concern to the international community, shipping companies, and organizations such as the International Maritime Organisation (IMO).

Piracy is an international crime. Traditionally, a state can exercise jurisdiction only within its territorial waters. However, the 1982 United Nations Convention on the Law of the Sea

(UNCLOS) specifies three distinct cases in which warships or ships under public authority may apply jurisdiction outside their maritime sovereignty zones. These are boarding, hot pursuit, and piracy. Here we will focus on the latter.
According to Article 101 of UNCLOS, piracy is defined as:

a. any illegal act of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:
   (i) On the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;
   (ii) Against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;
b. Any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

Any act of inciting or of intentionally facilitating an act described in subparagraph (a) or (b).

Terrorism

Terrorism is the unlawful use or threatened use of force or violence with the goal of instilling fear and terror, in order to coerce or intimidate governments or societies, to achieve political, religious or ideological objectives.
Terrorism can be seen as a violent act specifically designed to attract attention and spread fear to a large audience. Terrorists aim to use violence to gain the maximum degree of leverage needed in order to achieve desired change. Through their actions, terrorists seek to sway public attention to issues they consider important and pass across their message.
Various terrorist groups differ considerably based on their motivation. They differ in the nature of their ideology and their political goals. They differ in their relationship with religion, as well as the level of support they receive from their communities. They also differ in their use of force.
Terrorism is a concept with multiple causes, consequences and manifestations and therefore not easily defined. In essence, it is a broad ideology aimed at provoking terror with the purpose of destabilizing political life, expressing a reaction to government policy and carrying out an extreme form of protest. Terrorist attacks can be perpetrated by one or more individuals. Moreover, they are aimed at injuring or destroying as many people and assets as possible. Additionally, terrorist attacks may be perpetrated by people who are not born in the same country and are being carried out to avenge citizens of another country for political or religious motives.

What is Biometrics

Biometrics is the automated recognition of individuals based on their behavioural and biological characteristics. Today there are many types of biometric data can be collected to identify a person, such as fingerprint, face, iris, DNA, gait analysis and hand geometry. Some of those commonly used by biometric data capture devices are analyzed in more details below.

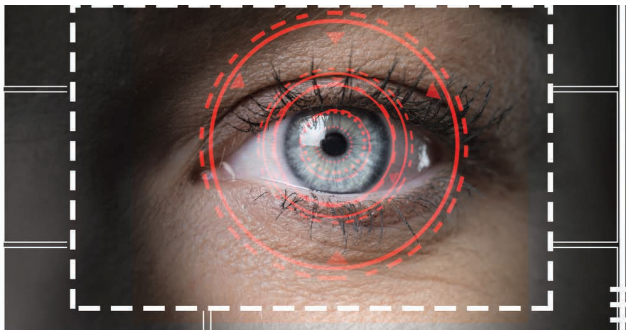
Fingerprints

Fingerprint collection is critical to catching explosives manufacturers, identifying who handled weapons and explosives in a cache, and who was present a safe house other than the people that were found. Fingerprint recognition has been around for over 100 years and can be extremely accurate in positively identifying a person from a visible or latent fingerprints. Because of its extensive use worldwide, technologies for capturing standardized fingerprints are widely available.
While not as accurate as Iris recognition, fingerprint recognition tools have the ability work in concert with collected forensics from a crime scene or taken from an object. These latent fingerprints can then be loaded into the system and checked against the database. Fingerprints can lead you to

the bomb maker, the person that loaded the weapons into the cache, and the individuals who were at the safe house.

Face

Recognizing a person using face geometry is a technology that has evolved significantly in recent years. These systems are increasingly being developed on a wider scale of applications making this technology promising for the future. The facial recognition process consists of capturing many images of the face then extracting unique facial features as well as distances from or between the nose, ears, mouth, eyes and cheeks



Iris

Iris recognition is the process of recognizing a person by analyzing the random pattern of the iris. The iris is a muscle within the eye that regulates the size of the pupil, controlling the amount of light that enters the eye. It is the colored portion of the eye with coloring based on the amount of melatonin pigment within the muscle. Due to its uniqueness, universality, reliability and stability, Iris patterns serve a major role in several recognition and authentication applications.

Why we use biometrics

- To catch IED makers and members of the networks
- To confirm or refute identity
- To give the population a way to identify each other
- To identify, track, locate and deal with the population
- To deny the enemy the ability to hide within the population, eliminate local support

These key reasons show why we use biometrics for the protection of our own forces as well as for the local populace. The capability to positively identify an individual enhances the overall mission success. When you can identify, track and locate members of the populace, you can help control what happens and when it happens rather than being in a reactive mode.

Biometrics is needed not only in force protection and security missions, but is also used to achieve an advantage over an enemy in such operations as conventional warfare, combating terrorism, forcible entry, strikes, raids and operations with multinational partners.

Biometrics can be used to link people to times, locations, groups, and activities, while simultaneously providing a means to detect and identify them in the future. Whether a biometric match links a new record with a latent fingerprint from an IED, or a previous record captured for base access, these links offer potential value that can be realized through specialized analysis.

Advantages

The greatest advantage to using biometrics is to remove the power of anonymity at its most basic level, answer the question of who is standing in front of you at the gate. Every individual can be considered a package of distinctive, if not unique, biometric identifiers, from palm prints to iris and from handwriting to gait.

Any human characteristic, either biological or behavioral can (in theory at least) be used as a biometric modality.

The listed characteristics are currently some of the biometrics that can be used to recognize a person with a certain degree of accuracy. No single modality should be considered perfect for all applications.

Limitations

- Applicable Laws and Policies must be considered when developing operational and intelligence functions for capturing biometric data.
- Cultural Considerations for the population from which biometric data is being captured must be made when planning and carrying out biometric activities. Because of cultural differences, biometric capture must be conducted in accordance with acceptable local customs. For this reason, commanders or those directing biometric capture must be familiar with, and sensitive to, the local culture.
- Security is required for Biometric Capture as it takes the time and attention of personnel. Biometric Capture must not risk the safety of the personnel or the individual being enrolled.

Environment can limit Biometric Capture as weather and operational factors can influence the quality of data, which has subsequent impacts on the entire Biometric Cycle.

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

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

E-mail: argirioui@nmiotc.nato.int - johnarg00@yahoo.gr Mobile: (0030) 6974014100

Visit of The Chief of Italian Fleet, Vice Admiral Donato Marzano and The Chief of the Hellenic Fleet, Vice Admiral Ioannis Pavlopoulos, June 2017

Visit of The American Hellenic Institute, July 2017

Visit of SEEBRIG, July 2017

Visit of World Hellenic Inter-Parliamentary Association, July 2017

Visit of the Chief of Defence of Norway, Admiral Haakon Bruun-Hanssen and the Cfief of Defence of Hellenic Armed Forces, Admiral Evangelos Apostolakis, September 2017

2nd NMIOTC Cyber Security and Cyber Defence in the Maritime Environment Conference, September 2017

Visit of Hellenic National Defence College, September 2017

Visit of the Minister of Defence of the Slovak Republic, Mr Peter Gajdos, September 2017

NMIOTC Commandant, Commodore Georgios Tsogkas, cutting the "birthday" cake for the Centre's 9th anniversary, with senior Staff Officer, October 2017

The Commander of the Naval Base in Alexandria, Rear Admiral Iham Mohamed Sobhy Aly visited training ship ARIS, in the context of the multinational excercise MEDUSA 2017, October 2017

Visit of the Deputy Assistant Secretary of the US Navy, Mr. Jim Balocki and Senior Director for Policy and Strategy Deputy under Secretary of the Navy for Policy, Ms. Mindy Montgomery, November 2017

Visit of Cfief of Defence of Hellenic Armed Forces, Admiral Evangelos Apostolakis with Chief of Cyber Defence & Information of Armed Forces of Norway, Odd Pedersen, during the Military Partnership Directorate Meeting,November 2017

European Defence Agency Conference, with the presence of the Cfief of Defence of Hellenic Armed Forces, Admiral Evangelos Apostolakis and the Chief of the Hellenic Fleet, Vice Admiral Ioannis Pavlopoulos, November 2017

Exercise NIRIIS 2017 Pre-Sail Conference, November 2017

Interview of NMIOTC Commandant, Commodore Georgios Tsogkas, December 2017

Visit of Hellenic Navy Naval Cadets,December 2017

Exercise Sea Breeze, July 2017

Course "5000", August 2017

Joint Training of Dutch and Swedish Armed Forces, September 2017

Joint Training of Dutch and Swedish Armed Forces, September 2017

Course "8000", September 2017

Training of Qatari Special Forces, September 2017

Training of German Forces for Boarding Deployment, October 2017

Training of ROS REGELE FERDINAND Command and Boarding Teams, October 2017

Training of Polish Special Forces Team NSWU FORMOZA, October 2017

Course "12000", October 2017

Pilot Course "21000", October 2017

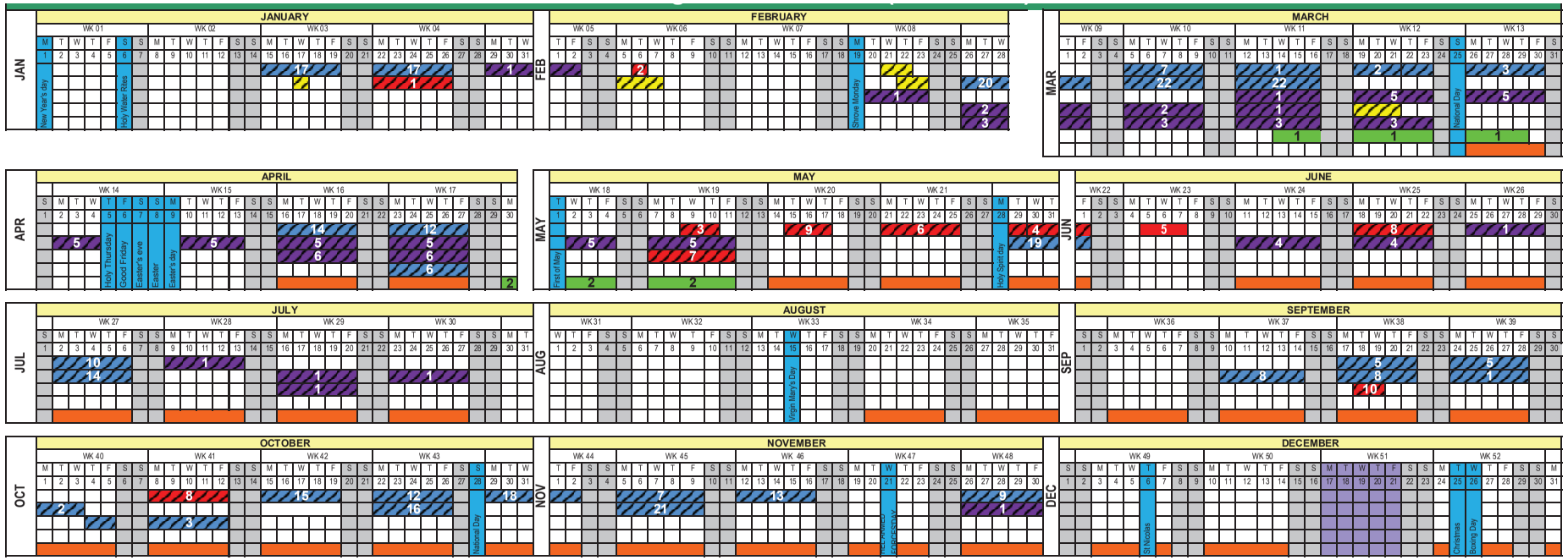
Training of GRC Special Forces Team, October 2017

Training of Egyptian Boardind Team, during Exercise MEDUSA 2017, October 2017

Training of Ghanaian Special Forces Team, November 2017

Course "18000", December 2017

Training of NMIOTC personnel at the firing range, December 2017



COURSES (ETOC ID.)

1. Course 1000 - Command Team MIO Issues (MOP-MO-51201)
2. Course 2000 - Boarding Team Theoretical Issues (MOP-MO-51203)
3. Course 3000 - Boarding Team Practical Issues (MOP-MO-41205)
5. Course 5000 - Maritime Operational Terminology Course (MOP-MO-11208)
6. Course 6000 - Weapons of Mass Destruction in MIO (MOP-MO-31209)
7. Course 7000 - MIO in support of Counter Piracy Ops (MOP-MO-41210)
8. Course 8000 - C-IED Considerations in Maritime Force Protection (IED-ED-31679)
9. Course 9000 - Legal Issues in MIO (LGL-LE-31613)
10. Course 10000 - MIO in Support of Countering Illicit Trafficking at Sea (MOP-MO-32012)
11. Course 11000 - AVPD Course (on demand) (MOP-MO-32011)
12. Course 12000 - MIO in a C-IED (AtN) Maritime Environment (IED-ED-31904)
13. Course 13000 -MIO in Support of International Efforts to Counter Migrant Smuggling Activities at Sea - Command Team Issues (MOP-MO-32015)
14. Course 14000 - Maritime IED Disposal (IED-ED-32008)
15. Course 15000 - MIO in Support of International Efforts to Counter Migrant Smuggling Activities at Sea - Practical Issues
16. Course 16000 -Maritime Aspects of Joint Operations (MOP-MO-22078)
17. Course 17000 - Train the Trainers Technical Instructor
18. Course 18000 -Maritime Biometrics Collection and Tactical Forensic Site Exploitetion
19. Course 19000 - Cyber Security Aspects in Maritime Operations (COP-CD-22104)
20. Course 20000 - Protection of Critical Maritime Infrastructure [C(M)I]
21. Course 21000 -Medical Combat Care in MIO

ACTIVITIES

1. ADL BIOMETRICS WS
2. NAB (NMIOTC)
3. NCB (HNGS)
4. NATO Maritime Operations Law Seminar
5. NMIOTC Annual Conference
6. NATO Shipping WG
7. Adoption of non-NATO standards and development of new dual use and other standards in collaboration with civil SDOs (pilot)
8. Drafting, Production and Maintenance
9. SPS WMD WS
10. Cyber Security Conference

EXERCISES / METTs

1. NOBLE DINA
2. PHOENIX EXPRESS

TAILORED TRAININGS

1. GRC SOF team (Army, Navy, Air Force, Coast Guard, Police, etc)
2. DEU team
3. MEU team
4. NLD team
5. LBY team
6. LTU team

TRIAL COURSES

► **Updated 12 Dec. 2017**

NMIOTC

ΝΜΙΟΤC/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

www.facebook.com/nmiotc

www.instagram.com/nmiotc

Hellenic Army's Printing Office