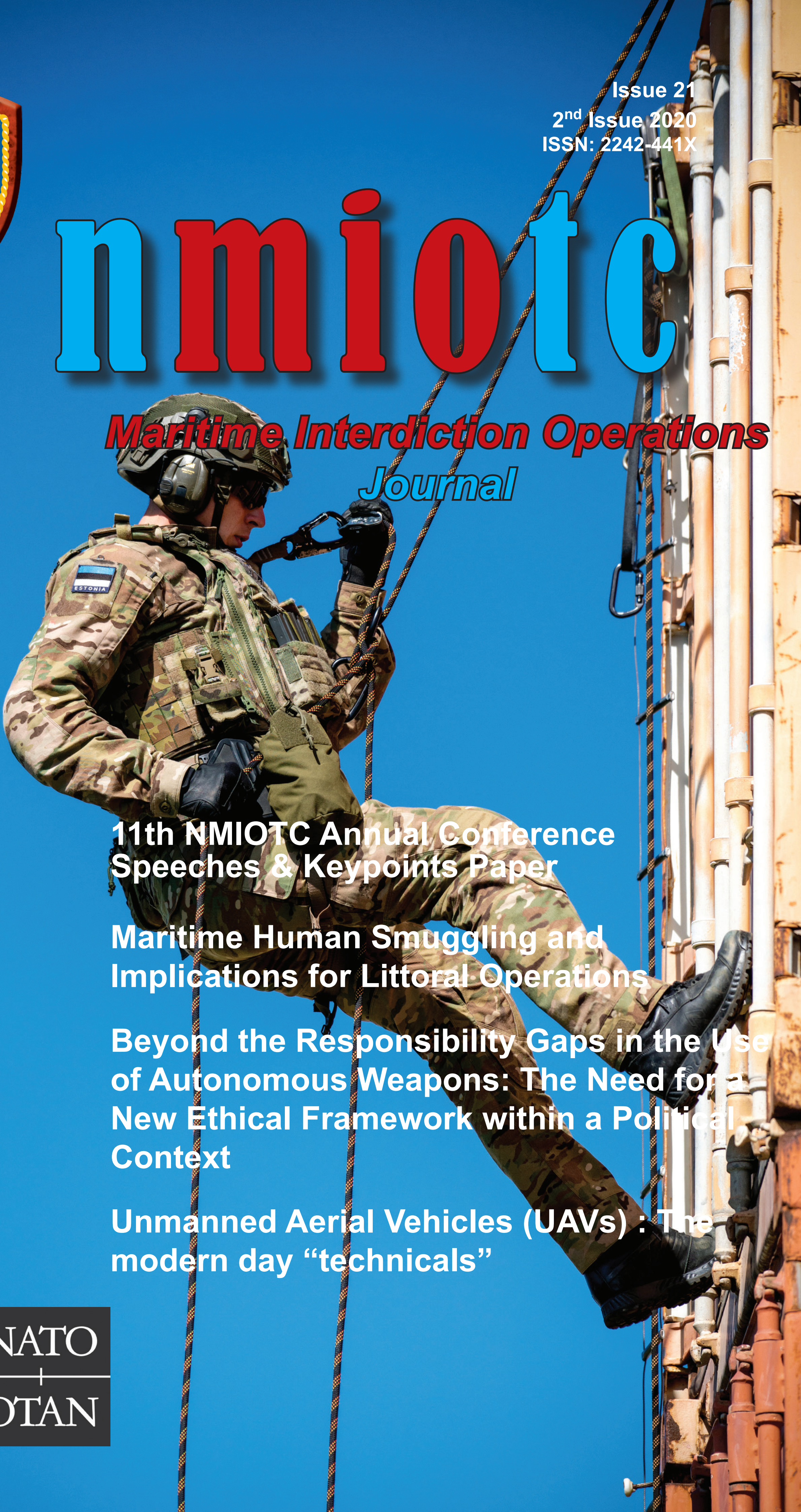
Issue 21
2nd Issue 2020
ISSN: 2242-441X

nmiotc

Maritime Interdiction Operations Journal



NATO MARITIME INTERDICTION OPERATIONAL TRAINING CENTRE

11th NMIOTC Annual Conference Speeches & Keypoints Paper

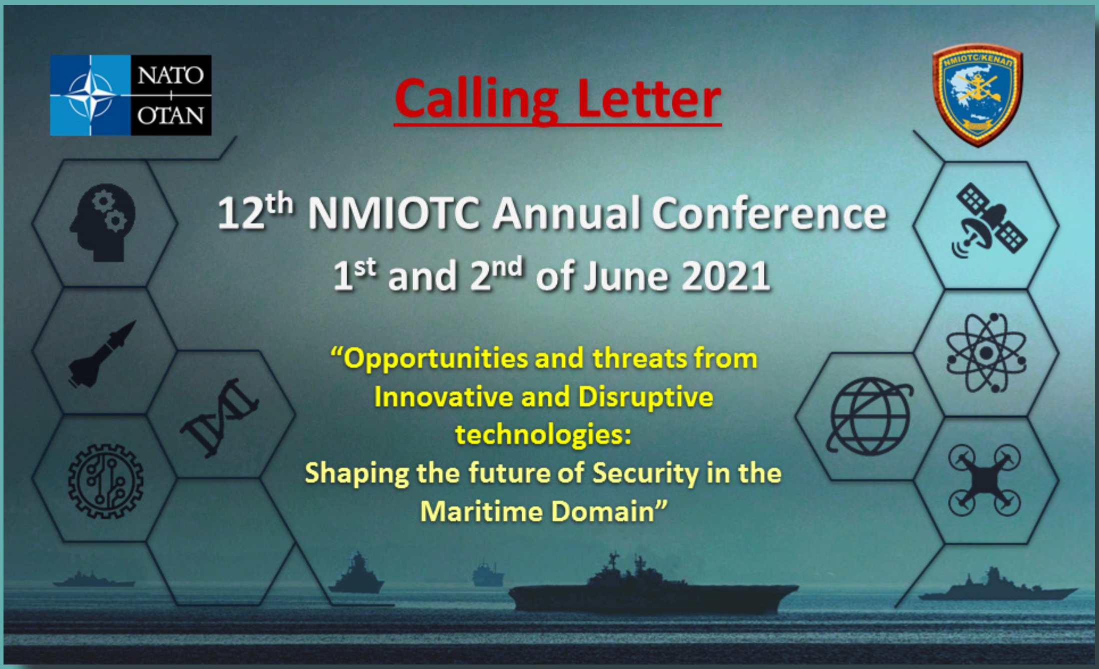
Maritime Human Smuggling and Implications for Littoral Operations

Beyond the Responsibility Gaps in the Use of Autonomous Weapons: The Need for a New Ethical Framework within a Political Context

Unmanned Aerial Vehicles (UAVs) : The modern day “technicals”

NATO OTAN

NATO
Maritime Interdiction Operational Training Centre



Calling Letter

12th NMIOTC Annual Conference

1st and 2nd of June 2021

"Opportunities and threats from Innovative and Disruptive technologies: Shaping the future of Security in the Maritime Domain"

Save The Date

"Gender Perspectives in Maritime Security" Seminar

3rd to 4th of June 2021

CONTENTS

COMMANDANT'S EDITORIAL

MARITIME SECURITY

NMIOTC COURSES AND ACTIVITIES

HIGH VISIBILITY EVENTS

NMIOTC TRAINING

nmiotc

MARITIME INTERDICTION
OPERATIONS
JOURNAL

Director
Commodore P. Papanikolaou GRC (N)
Commandant NMIOTC

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

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

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

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

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

NMIOTC
Commandant's Editorial

Modern maritime environment is characterized, as we all know, by complexity and diversity. By its very nature it offers abundant freedom to seafarers, being at the same time vulnerable to activities threatening Nation's interests and the free flow of world commerce. Illicit trafficking, pollution, terrorist activities or support to them and piracy are just few examples of illegal activities conducted from or through the sea. Threats to peace and stability emanating from the sea have, more than ever before, a global reach and the response to them is a challenge for NATO nations and the global community to meet.

Global security challenges have led to the need for new training requirements. NMIOTC being the only NATO accredited Educational and Training Facility focused in the maritime domain responds to these needs by training naval units and specialized teams in MIO, and also by providing proposals for new doctrines, tactics, methods and equipment that will address a wide range of maritime security challenges. Our aim is to develop diverse and highly effective Maritime Security capabilities, and to enhance integration and interoperability for the Allied and partner nations, while forging a law enforcement culture, through proper training on international law.

In that context, and in addition to the training that NMIOTC provides, we also organize conferences, seminars and workshops in order to establish relationships, cooperation and common understanding, to exchange views and ideas, and to discuss solutions to these challenges.

This year, considering that peace, security and prosperity relies more than ever before upon the close correspondence and collaboration of all stakeholders, particularly in the maritime domain, we addressed the issue of a whole of society approach to current and emerging challenges. Thus, this year's conference theme was "Interagency and whole of society solutions to maritime security challenges". That event was an open forum getting together nations through their naval forces and law enforcement agencies, as well the shipping industry, International organizations, and NGOs in order to promote awareness and common understanding and investigate means of further cooperation, necessary to meet the challenges of the future. I cannot avoid mentioning, that the current unprecedented situation that we all face with the COVID-19 pandemic, has even furthermore demonstrated this paramount need for a whole of society, international and interagency approach to large scale challenges.

During the works of the conference we couldn't stress more the so many aspects of illegal activities emanating from the sea that are seriously threatening peace, stability and prosperity globally. Nationally or locally, and at a whole of government approach, two tools should be applied, in order to provide to us the opportunity to respond:

- Reliable and persistent Maritime Domain Awareness – Maritime Situational Awareness (MDA-MSA)
- Thorough decision making process.

Both could and should be enhanced by disruptive technologies and always taking into account the existence of cyber threats, so that we retain the technological advantage over our potential adversaries.

Operating globally though has one and only prerequisite: Cooperation between all stakeholders. From the presentations and the discussions of the conference, it was tangible that we all (military/ law enforcement/ civil and private sector) working on that but we should start cooperate without barriers, or if you like, HOLISTIC COOPERATION is necessary in order to deter, be able to defend (if necessary) and (at the end of the day) project stability globally.

Panagiotis Papanikolaou
Commodore GRC (N)
Commadant NMIOTC

Admiral Karl L.Schultz
Commandant US Coast Guard
Keynote speech - 11th Annual Conference

Good Morning! It's my distinct privilege to represent the United States here in Souda Bay, Crete, at the NATO Marine Interdiction Operations Training Center!

Thank you, Commodore Papanikolaou, for the invitation to speak at this year's 11th annual conference; I know that our Secretary of State has been in Greece these past two days as well.

This year's conference theme, "Inter-agency and whole of society solutions to maritime security challenges" is near and dear to my heart. Many—probably characterized as most of the U.S. Coast Guard's successes—stem from the power of partnerships and the related cooperation and collaboration found in those partnerships.
What many do not realize (even in America) is that the Coast Guard, while an Armed Force, is not a member of the Department of Defense. Our Service falls under the Department of Homeland Security and this structure allows the U.S. Coast Guard to possess unique authorities and capabilities as a military service, and both a regulatory and a law enforcement agency.

Our fellow sea services—the U.S. Navy and the U.S. Marine Corps focus on lethality—on winning wars. In times of war, the U.S. Coast Guard will assist in such effort. And I am excited to announce in the weeks ahead, our three naval services will launch a new tri-service maritime strategy that will outline our respective U.S. Naval roles. That strategy shows that the U.S. Coast Guard, while an armed force, serves as a "bridge" between Department of Defense "lethality" and State Department "diplomacy." We thrive operating in this space and we fully recognize that our borders begin well beyond our coastline, and that threats to our National interests and security originate far from our homeland.

Hence, we cooperate with partner nations to prevent those threats from reaching our shores. We strive to "value" our partners as we synchronize efforts and operate jointly to shape and stymie trans-national criminal organizations, non-state actors, and nations with ambitions to coerce and dominate in the maritime domain. If left unchecked, such threats undermine regional stability and security and the "rules based international order" that underpins the NATO alliance. And we do this work globally as our U.S. Coast Guard cutters and aircrafts, mobile training teams, and marine and facility inspectors deploy world-wide.

One such maritime threat is the transport of illicit narcotics.
For years we've trained, equipped and coordinated with dozens of countries across South and Central America, and the Caribbean, as well as with Allied partners such as the French, Dutch, Canadians, and the United Kingdom, to help stop the flow of illicit drugs. These efforts are paying off.

This summer, a U.S. Coast Guard Cutter conducted an at-sea boarding of 75-ft cargo vessel in the Caribbean and turned the vessel over to the Colombian Navy for a follow-on dockside boarding spanning a period of more than seven days.
This case resulted in the discovery of over 7,500 kilograms of cocaine concealed within hundreds of bags of fertilizer, and highlights the robust cooperation with partner nations, and the continued advancement of concealment tactics used by trans-criminal organizations.

These Western Hemisphere partner nations now coordinate and lead their own counter narcotics operations, and participate in approximately 50% of all the cases led by Joint Interagency Task Force-South, our United States lead agency for maritime drug interdiction detection and monitoring.
Colombia led "CAMPAIGN ORION"—a 45-Day Multinational campaign, with 26 participating nations, is underway in its 6th iteration. In the last, or 5th iteration, partner nations removed 50 metric tons of illicit narcotics.

I am incredibly grateful for the increasing contributions of our Latin American counterdrug partners, and our allied shipmates, in this fight to save lives.
Thanks to the power of partnerships, the U.S. Coast Guard has interdicted more than 1.8 million pounds of cocaine in the last four years...

Let's not forget that each of these interdictions also spark the process for legal prosecution… we present about 600 smugglers before the U.S. criminal justice system annually.
Depending on the location of the interdiction, the United States likely needs to secure a waiver of jurisdiction from the flag state—informing where in the United States we can prosecute the case, and therefore transport the suspects, secure the evidence, and take witness statements. Each of these actions within the process require different inter-agency engagements, and to make it work, we must all work in concert, in real time.

In the United States, our interagency, "whole-of-government" maritime threat response decision-making process is called MOTR—or the "Maritime Operational Threat Response Plan." We use the MOTR plan daily to ensure we speak as one voice, move forward in alignment, and share information.

MOTR was presidentially signed and it works well for our inter-agency coordinating needs. It works because we have built trust among agencies, which takes time and patience.
The plan is inclusive, flexible, adaptable, straight-forward, and consistent, or repeatable. This MOTR plan has forged a community amidst government officials who operate in separate departments, with separate chains of commands, and separate authorities.

Many countries have some version of this plan, a maritime response decision-making process. I share ours with you as it may provide insight and possible inspiration to continue strengthening ties and forging partnerships in our collective efforts for maritime security.

We see MOTR work effectively to support our counter-drug efforts. Yet, the counter-drug effort is just one of the Coast Guard's 11 statutorily assigned missions. We exercise MOTR in support of over 60 active bilateral agreements with nations around the globe to counter threats and challenges, ranging from counterdrug and search-and-rescue to Illegal, Unreported, and Unregulated—or IUU—fishing enforcement activities, to cyber threats at sea.

I continue to hear from international partners regarding the challenges they face with illegal fishing in their EEZs. IUU fishing prevents these partners' ability to have stable control over their economies and natural resources, as well as security of their food supply.

Fish may not, at first, appear to be a maritime or National security issue. However, fish is an essential protein source to over 40 percent of the global population. Fisheries around the world are critical to many nations' sovereignty, to their economic security and their maritime governance.
And there's currently a "fight for fish" in the Pacific, off South America, and off the African coasts.

"Distant Water Fleets" are a growing national security concern when they violate the sovereign rights and jurisdiction of coastal states, fish without permission, and over-fish license agreements. The work itself by distant water fleets is not transparent.
China has the largest "distant water fleet" in the world—with a reported armada of over 4,600 vessels that operate in the Exclusive Economic Zones of 42 countries; some reports suggest they have over 16,000 "distant water fishing" vessels, operating internationally under different flag states.

To support this fleet, China has published an Ocean Fishery Development Plan which lays out a network of "fishing bases" throughout the globe to service these vessels—and to build maritime power—without ever firing a shot.

Many are familiar with Beijing's destructive fishing operations in the South China Sea and Western Pacific. However, we also see similar activity in Africa's Gulf of Guinea and off the coast of South America, including recent reports of China's "Distant Water Fleet" operating near Ecuador's Galapagos Islands.

I imagine the Arctic is next as climatological changes push migratory species further North in the decades to come, and the region becomes more accessible…

Keep in mind, China's "Distant Water Fleet," while by far the largest, is just one of many fishing fleets venturing far from home to harvest other nations' resources.
Local fishers stand no chance against competing modern "Distant Water Fleets" with industrial capacity, which ship catch far from harvest location. In these local and oftentimes developingstate economies, shore-side demand for fish increases as supply dwindles, driving prices skyward and putting local fishermen out of work.

In this light, IUU fishing has replaced piracy as the leading global maritime security threat. As demand for fish increases and maritime resources diminish, skirmishes over this natural resource – fish/protein - become more likely due to more frequent clashes at sea.

What is the U.S. Coast Guard doing about this threat? Well, we are leveraging our existing partnerships across the globe, within the U.S. government, and in academia, too.

Earlier this month, we released the "Illegal, Unreported, and Unregulated Fishing Strategic Outlook" which details the Service's vision for addressing the IUU fishing threat--through targeted, intelligence-driven enforcement, and by countering irresponsible predatory state behavior.

But, most importantly, the Strategic Outlook reinforces the importance of our multilateral, multinational cooperation.
We know we cannot be successful alone. To disrupt IUU fishing across the globe, we must work together! Our success hinges on leveraging partnerships, both existing and new, to create a unified front to combat IUU fishing in every ocean.

Together, we will confront this coercive and antagonistic activity head-on by promoting transparency, starting by increasing maritime domain awareness. In the process, we will strengthen global maritime security, regional stability, and economic prosperity—both for the U.S. and for our "like-minded" partners worldwide.

We know international cooperation works: for 25 years, the six nations which contribute to the enforcement efforts of the "Operation North Pacific Guard" have confronted "distant water fishing fleets" that fail to adhere to international rules and regulations. Our collective efforts have been overwhelmingly successful and together, we have practically eliminated Illegal

High Seas Driftnet Fishing in the North Pacific Ocean.

Bottom line: in the maritime domain, presence equals influence.
That's why in recent weeks we had two Coast Guard cutters participate in Operation Nanook and Search-and-Rescue Exercise Argus off the coast of Greenland with the Canadians, Danes, U.S. Navy and French Forces, as well as local, federal, state and tribal agencies. These peaceful international exercises with fellow Arctic Nations are opportunities to enhance operational capability in a dynamic environment, while strengthening rules-based order.

For two years in a row, we've sent U.S. Coast Guard cutters to Africa's Gulf of Guinea to carry out the living marine resource mission, anti-piracy operations, and search and rescue with partner nations such as Nigeria, Sao Tome and Principe, Senegal, and Cabo Verde.

And we sent a sea-going buoy tender to the Pacific island nation of Palau, where our U.S. Coast Guard crew re-built over 50 aids to navigation. Navigational aids are important as they enable "trade at scale"–ships carrying commodities—to frequent a port.
We've also sent our largest cutters, our Flagship National Security Cutters, to enforce sanctions and build partnerships in the Indo-Pacific.
And we are currently building new heavy ice breakers, Polar Security Cutters, to have an enduring presence in the Arctic and Antarctic.
I say this with both confidence and humility: Our U.S. Coast Guard presence in areas of the world matters.
I believe U.S. Coast Guard cutters model the way Coast Guards should act.

Coast Guards support sustainable fishing practices and prevent Illegal, Unreported, and Unregulated fishing in order to protect their nation's natural renewable resources.

Coast Guards promote the "transfer of knowledge" and "capabilities across agencies" to enhance each other's maritime domain awareness.

Coast Guards respond when mariners are in distress.

Coast Guards facilitate maritime commerce as today's consumer depends on "Just-in-Time" shipments of international goods by sea.

And Coast Guards influence others, not by a domineering spirit, but rather by re-enforcing a "rules-based system" that promotes peace, security, prosperity and sovereignty of all nations.

The U.S. Coast Guard seeks to demonstrate that our Nation offers transparent partnership and a clear alternative to predatory and duplicitous behaviors.

We all share multiple maritime challenges.

Each of these challenges offer opportunities to cultivate partnerships, build trust, and participate in multi-lateral and multinational forums.

The U.S. Coast Guard has been, and will continue to be, a committed partner to nations and organizations that are dedicated to a "transparent, rules based order." My team and I look forward to engaging with you on how we can work together to protect our global commons.

I look forward to learning and talking with you on this important issue.

Semper Paratus!

VADM Keith Blount CB OBE Royal Navy Commander, Allied Maritime Command

Keynote speech - 11th Annual Conference

I want to extend my sincere thanks and appreciation to NMIOTC, not only for the opportunity to speak here today, but for your many years of support to the maritime community. We are grateful for the tremendous efforts you have championed for maritime interdiction operations -- everything from research, training, and doctrine to the successful employment of that knowledge through your effective fostering of interoperability and cooperation among naval units. In more recent years, your leadership and contribution to the field of cyber security have positioned us all to remain much more cognisant of the relevance and significance of this ever-evolving threat. For those of us operating across the maritime domain, the enduring value of your proficiency and expertise in these most essential arenas cannot be overstated.

1. COVID

The world is a much different place that it was just a year ago. The impact of COVID-19 to our nations, our economies, and our people is a new reality that we have all become acutely aware of. The pandemic's impact has not stopped there, however. It has transformed the manner in which we carry out the day-to-day operations of our organisations.

COVID-19 is the greatest example of an inter-agency problem one could think of. The challenge is primarily medical, not military, but it can have a major impact on military readiness and the strategic balance. Responding to it required an expert mix of medical, scientific, government, economic and military advice. Seldom has the Medical Advisor been more important in a maritime headquarters than now.

Responding effectively to COVID-19 includes such aspects as the facilitation of our workforce, the restructuring of our procedures and processes to adapt to teleworking, and the safe and calculated approach to bringing everyone back together in a safe new working environment as we are permitted to do so. The difference between us and those we protect is that when the world is placed on pause -- when major corporations, schools, government organisations, and local communities take a pause – we cannot. Even as we acknowledge the devastating impact of COVID around the world, we also know our competitors might look for even the slightest glitch in our posture, or smallest window of opportunity to exploit such a gap. So our mission continues, even in the face of unprecedented challenges.

On the maritime front, I am very proud of the resilience our forces have shown during these challenging times. On the surface, it may seem that there is an inherent advantage to being in the maritime domain during a pandemic in that we have the ability to closely control where and when we go places and who we interact with and how closely we interact with them. But in reality, that advantage only gets you so far, when you consider things like crew rotations, necessary port visits, and maintenance requirements. For us, and I am sure for many of you, this was a process that we had to learn from and refine as we went along, but there were a few tactics that I think set us up for success from the onset.

We established our AIM early and gave clear direction on how we were going to monitor, assess, and adapt to COVID guidance as it came out, balancing safety and operational effectiveness. We communicated with our Allies and their leadership to ensure we were staying apprised of the individual country restrictions and its impact on their personnel. Finally, we made sure that we were maintaining an ongoing dialogue with our headquarters and standing naval force crews. The result was that – in September 2020 and nine months after news of the pandemic broke – MARCOM and the SNF had not had a single confirmed case.

Communication is the common theme you will notice there. As we all know, communication within our organisations is a critical component of success, especially now. Our ability to do so effectively, whether across the sea or through teleworking, is a testament to our collective resilience. Equally important, though—especially in these times—is our ability to communicate that resilience and persistence strategically to the rest of the world. As I mentioned earlier, our competitors will look for opportunities in our posture to pursue interests contradictory to our own. It is therefore imperative that we continue to press forward in these critical times.

Operationally, we have done so. DYNAMIC MONGOOSE in the High North, BALTOPS in the Baltic Sea Region, BREEZE and SEA BREEZE in the Black Sea, and Operation Sea Guardian in the Mediterranean have all continued to showcase our commitment to the Alliance and reassured those who rely on the deterrence we provide. I thank all of you who have helped lead on that front.

2. Operation Sea Guardian

I cannot think of a better example that speaks to the relevance of inter-agency cooperation than Operation Sea Guardian. Our obligation to ensure maritime security in the Mediterranean requires a multitude of actions, in collaboration with our Allies and Partners, and represents the full spectrum of capabilities that we possess. Today, I will highlight just three of those areas – Commitment, Cooperation, and Forward Thinking.

Our mission is not one-dimensional. We operate on, above, and below the sea. To do so effectively, and provide an accurate maritime picture requires the commitment of us all. And with each pledge for support – with each commitment – that picture of our environment gets clearer. Last year through direct and associated support, we had the contribution of more than 260 ships and submarines, amassing more than 7,500 collective days at sea. Beyond that, we had more than 5,500 flight hours of support above. While those numbers may seem remarkable, they are necessary. That is exactly the kind of commitment it will take, consistently and collectively, each year as we move forward.

Second comes cooperation. This goes beyond simply working alongside one another. It is about shaping our maritime situational awareness through collectively enhancing our ability to do so. Information sharing is at the top of that endeavour. And this is not just information about military matters, but terrorism, trafficking and even organised crime. It is an inherently comprehensive and inter-agency mission. Success requires deepening the operational relationships between Allies, as well as more deliberate interactions and dialogue with those stakeholders who can best contribute to a comprehensive MSA picture—Governments, Military and Law Enforcement, the Shipping Community, Academics, and others, to discern and preserve ground truth on the threats to the maritime environment, their pattern, and their trends. This includes more interagency cooperation, more IO cooperation, and a collective understanding of the vital importance of the NATO-EU relationship with regards to our mutual interest of maritime security. We will continue to do some of this through the NATO Shipping Centre, proactive engagements through our ship hailings, the Maritime Information Exchange program, key leader engagements, but ultimately, through fruitful cooperation with those who have a true vested interest in maintaining a safe maritime environment.

Finally, there is Forward Thinking. COVID-19 gave us an unpredicted assessment of our courage, our determination, and ultimately, our priorities. What it also did was require us to become more agile in our thinking, and swifter in our execution of that thought. That same logic can be applied to the manner in which we look at warfighting today. The landscape is continually evolving with the technology becoming more compact, and the operator becoming more autonomous. Our challenge is to become more anticipatory in our operations and more conversant with those technologies operating within

our knowledge gaps.
The NATO Warfighting Capstone Concept is laying the long-range groundwork to do just that. Its focus on the future of warfighting enables us to look ahead toward the potential battlespace we may face over the next 20 years. This is one area, where if we spend too much time learning from the past, we will be inadequately prepared for the future. Maintaining our competitive advantage against emerging threats requires that we make continual efforts to advance our integration of artificial intelligence and autonomous instruments of power into our sphere of responsibility. This is a direction we intend to head. Ultimately, Operation Sea Guardian represents the best of who we are jointly and underscores our greatest responsibility to the Alliance of collective security and defence. This effort will continue to demand the most from us all, and I thank those who have contributed so much time, effort, personnel, and resources to achieve all that we have so far.

3. Autonomy and Experimentation

There is critical need for NATO to master all-domain operations at sea, incorporating space ISR, cyber defence and AI data fusion into future operations. It is imperative for Allied Navies to not only leverage these growing MSA resources, but also to confront how to mitigate their risk to their own forces. As militaries around the world invest in advanced technology, we recognize that an important part of maritime situational awareness is unmanned systems and their application into the tactical picture.

The exploitation of Maritime Unmanned Systems in the maritime domain as the “long arms” of our ships and maritime assets is in motion and is going to be even more so in the future, a powerful force multiplier, notwithstanding their ability to deliver stand-alone effects when operated from shore-based control stations. With an ability to provide kinetic and at times precise surgical effects, they have the potential to enlarge our MSA in a very efficient and effective manner. It will be a key factor in ensuring Alliance superiority in the maritime domain.

There remain several challenges to be addressed. We need to improve MUS autonomy as this will increase their resilience to cyber warfare and electronic warfare threats to work autonomously with greater resilience and reliability when engaged in persistent and discrete operations. Our capacity to deal with big data needs to be improved, going from a requirement for high speed communications to the capacity to process, fuse and analyse big data, transforming it into MSA by better leveraging artificial intelligence.

Heading into 2021 and beyond, we will look at ways to advance our understanding of these technologies from basic-level knowledge to a relevant part of our daily naval operations. DYNAMIC MESSENGER in 2022 will focus a great deal on large-scale operational experimentation, both with robotics and maritime unmanned systems. By then, the technology will be different than it is now, so we must continue to pursue our collaborations with industry and academia if we are to remain ahead of the pace in this most vital area of future warfare.

4. Conclusion

Allow me to conclude with a word about our greatest maritime asset - our cohesion. Collective Defence is the founding principle of NATO. Our commitment to Alliance cohesion in the maritime domain ensures we remain able to thoroughly and effectively deter, defend, and project stability while supporting the three primary functions area of our activities: Strategic, security and warfighting. Our awareness of tensions within the Alliance underpins our need to continually strive to preserve that cohesion as it remains our strongest asset against emerging global threats. I am grateful for all efforts to maintain that solidarity and cohesion in difficult times.

Mr Dirk Dubois
Director, European Security Defense College
Keynote speech - 4th NMIOTC Cyber Security Conference in the Maritime Domain

Dear Commodore Papanikolaou, honoured guests, dear ladies and gentlemen.

Those of you that know me, not so many in this group, know that I'm not a very active person on social media. Not that I am against modernisation or against computers, open communication or sharing information. I just never felt the need to promote my own person on the WWW or to give away much of my personal information on the internet. Actually, I was even quite proud when I Googled myself in 2008, that I only found one relevant hit. Now please, don't go and Google me right now to check. Finally, when I became Head of the ESDC in 2015, I allowed myself to be persuaded to create a LinkedIn profile. One of the first contacts worked for NMIOTC. She promised that she would try to persuade her hierarchy to join the ESDC network. I didn't think much more about it, until last year, the Centre approach me officially to become an Associate Network Member a status which the EU Member states granted with pleasure and which explains in part the reason why I am standing here.

Before I go further, I would like to take the opportunity to very briefly tell you about the ESDC, who we are and what we do.

- The ESDC is a civilian-military network of 189 training institutes training from the EU Member States and from third countries, all providing training on CSDP.
- The College has a separate legal entity, but is embedded in EEAS.
- In the last few years, we run approximately 100 training activities per year and trained 5000 persons in the academic year 2019-2020, despite being closed for 4 months.
- In terms of Organisation, the college consists of the following bodies
  - Steering Committee, where Member States provide the overall political guidance.

- Executive Academic Board, providing academic advice by the representatives of the training institutes. Currently it has 7 task-oriented configurations.

o We have a portfolio consisting of over 50 different courses.

Of course, there were many more good reasons for NMIOTC and ESDC to be interested in co-operating and all of them are linked to what we will discuss over the coming days. For me, the reasons fall in a threefold of categories:

- Maritime security
- Cyber security
- EU-NATO cooperation

Let me through each of these categories in due time and tell you how we are active in the area Maritime security.

For the EU, the maritime dimension is of paramount importance. Approximately 70% of our internal and external trade travels over the seas. Freedom of navigation is therefore very high on our agenda. Secondly, the seabed is the one place where so-far unexploited resources can still be found in abundance. One example: the newly discovered hydro-carbon fuel reserves found in the Eastern Mediterranean. Another example: where can you still place large wind energy parks in a built-up, overpopulated country like Belgium? The seabed is also extensively used for things like cables, pipelines … As grandson of two fishermen, I shouldn't forget one of the hot issues in the discussions between EU Member States on many occasions and more particularly nowadays in the negotiations on Brexit: fishing rights!

On 24 June 2014 General Affairs Council adopted the EU Maritime Security Strategy. provides a set of common principles on which the European Union and its Member States can now develop their specific policies and action plans. The EU Maritime Security Strategy (EU MSS) covers both the internal and external aspects of the Union's maritime security.

In this strategy, the EU defines its interests and values as regards the maritime dimension. What do we do to protect or naval interests, our territories and our citizens? But also, and just as importantly, the EU underlines also here that it is a champion, perhaps one of the very few left in the world, of a rules-based international order. On the seas, this means respecting the UNCLOS and in case of diverging interpretation, the primacy of the UN and of international tribunals and courts to solve these issues, rather than resorting to blunt violence and intimidation.

Over the years, the EU has put in place a number of maritime operations to protect our interests. The oldest EUNAVFOR Atalanta, to protect the SLOC of the Horn of Africa and the youngest EUNAVFOR MED Irini, with has as part of its mandate to help ensure the weapons embargo against Libya. However, these operations can only help fight the symptoms. To really reduce piracy, more effort was needed on land to train and mentor Somali security forces and to help build-up local capacities.

In the ESDC course offer, we have a course dedicated to the maritime security strategy in particular, but the naval operations and other CSDP mission and operations are regularly addressed in many of our courses.

The maritime strategy also touches on internal security. I live in Antwerp. Before I go any further: any Dutch in the room? No? Ok, then I can safely say it is the biggest port in Europe. Actually, depending on what statistics you look at, you could just as well claim that that should be Rotterdam, but OK, allow me for once to be just a little bit nationalistic. As the two biggest harbours in Europe, they also share the dubious honour of being the main ports of entry for drugs traffic especially from South-America. Linked to that traffic, both in the Netherlands and in Belgium, drugs clans are recently fighting a gang war, resulting in hand grenade attacks and drive-by shooting incidents on the streets. Luckily, so far the damage has remained mostly material, but I'm not sure it will stay that way.

This brings me to the second reason for the involvement of NMIOTC in the ESDC network: cyber security. Living in Antwerp, I have often wondered how you would be able to find the one specific container in which you hid a few hundred kilo of cocaine among the thousands of containers that arrive daily in our ports. Well, obviously each container has its unique code, sitting in a database, where its exact position in a ship or on the harbour docks are stored. If you want to retrieve your container, you need that code. Certainly, that database is a target for hackers? However, let's assume for now that that database is well protected. The code still needs to be sent to the owner, the shipping company, the truck driver who will pick up the container…

Studying the agenda, I found another very interesting title in session 3 later today: ‘We hacked a ship’. It reminded me immediately of two stories: one is about two students from the university of Texas, who were able to take control of the $80 million luxury yacht White Rose in international waters of the coast of Italy in June 2013, using GPS spoofing. The other story, perhaps even more serious, is about the allegations that US warships, involved in serious collisions, in South-East Asia were hacked as well. In 2017, the guided-missile destroyers USS John S. McCain and USS Fitzgerald, were involved in such incidents. Official reports afterwards identified other causes for the two otherwise unrelated collisions in which the vessels were involved, but just the idea of that being possible…

In 2018, the ESDC got an additional tasking from the Member States to create a Cyber Education, Training, Exercise and Evaluation platform. During the built-up phase, our small team analysed the ‘cyber ecosystem’ in the EU. We quickly realised how stove-piped the approach in the EU was: some dealing with network security, other dealing with cybercrime, yet others dealing with cyber defence and finally the EEAS dealing with cyber diplomacy. It is our conviction that to train effectively and efficiently on cyber, you need to break through these stove piped approaches, so that at the very least there is a common understanding and a holistic, integrated approach to the problem. Moreover, you need to address different target audiences at different levels: awareness, technical, operational/tactical and legal. This platform reached its full operational capacity by the summer of 2019. Together with the training institutes in its network and with partner agencies such as ENISA, EDA and EUROPOL, we currently count 7 so-called ‘regular courses’ and plan to run an additional 4 pilot-activities. The platform is also actively involved in promoting research in the domain of cyber security and defence and supports through its expertise the planning, conduct and evaluation of exercises at the HQ of the EEAS.

Well, as the saying goes: all good things come in three! In 2018, the EU and NATO in a joint statement agreed on a number of action points. One of them is the closer cooperation in the field of education and training. In particular, the cooperation between centres of excellence was promoted. Since then, three NATO CoEs have joined our network either as full members or as associated partners. This helps the two organisations in reaching a better understanding and in increasing the interoperability between both organisations on the one side and between Member States and allies on the other side. On a number of topics, the traditional military ones, that interoperability is already far evolved and NATO standards and procedures are generally applied also by the EU and its MS. This should not come as a surprise when 21 countries are in both organisations. In other, less traditional fields - and cyber is such an example – the standardisation and interoperability are still far from being achieved. At the ESDC we hope, with the support of the network members such as NMIOTC, to contribute to this interoperability and better understanding through our training and education, through research and through exercises.

I’m looking very much forward to listening to all the high-level speakers in the coming two days and I wish you all an excellent and virus-free cyber conference!

11th NMIOTC Annual Conference 2020 "Interagency and Whole os Society Solutions to Maritime Security Challenges

by Ms Wendi Brown, Lieutenant Colonel U.S. Army Reserve

The 11th NMIOTC Annual Conference was held on September 29th, 2020 at the NMIOTC premises in Souda Bay, Crete, Greece. This year was unique because COVID-19 kept many of the speakers and participants from attending the conference. However, the conference still featured a wide variety of speakers who delivered valuable knowledge and information about maritime overall security challenges. Wendi O. Brown, Lieutenant Colonel U.S. Army Reserve, provided this article; her email is 1wendibrown@gmail.com

The Conference had four keynote speakers:
The first keynote speaker was Admiral Karl L. Schultz, the Commandant U.S. Coast Guard. You can find Admiral's speech in this issue on page 6. In his speech he emphasized the US Coast Guard's role in the U.S. Department of Homeland Security and its responsibility to respond to maritime partners in distress. The US Coast Guard values partners and strives to continue joint operations, their efforts resulting in 600 smugglers brought to US justice system. It handles state actors and works on a global basis, addressing the immigration problem as well as various drug campaigns. Finally, ADM Schultz highlighted the fact that the US Coast Guard is not global police for fishing or drugs but instead aims to create partnerships to promote transparency including partnering with African maritime ships.

The second keynote speaker was Vice Admiral Keith Blount CB OBE RN, Commandant of NATO's Allied Maritime Command. You can also find the Admiral's speech in this issue on page 10. His speech highlighted the major impact of COVID on military activities and explored ways in which competitors are looking for opportunities exploit military vulnerabilities caused by the pandemic. Admiral Blount discussed a particularly successful NATO operation, "Operation Sea Garden", focusing on three achievements:

a. Commitment to excellence and getting the job done right
b. Cooperation among interagency missions and international organizations
c. Forward thinking: Understand the need for cyber security, development and use of AI, and analysis of big data.

The third Keynote speaker was Rear Admiral Jean-Michel Martinet, Deputy Operations Commander European Naval

Force Mediterranean. Admiral Martinet discussed the Force's Core task, the arms embargo of Libya (CIAT), and the specific authorizing UN Security Council Resolutions which established the Arms embargo, authorized boarding and diversions, and extended the UNSCR 2292 mandate to 5 June 2021. He also highlighted the secondary effects of the embargo: the contribution to the disruption of human trafficking business model, the training and monitoring Libyan Coast Guard & Navy, and the gathering of information on oil smuggling.

The fourth Keynote speaker was Mr. Wayne Raabe, Director of Interagency Partnering – U.S. European Command. In his speech "Threats to European Maritime Security must be countered through a Whole of Government Approach," Mr. Raabe discussed the effects of transnational maritime threats:

a. The Territorial Disputes and Armed Conflicts (South China Sea disputes cost 4.74 Trillion annually in maritime trade)

b. The Proliferation of Weapons (497% increase in explosive-precursor liquid chemicals seized in international customs from 2011-2014)

c. Piracy and the Armed Robbery (1690 actual and attempted armed attacks at sea 2010-2014)

d. Natural Disasters and Climate Change (50 cm sea-level rise)

e. Pollution and the Environmental Impact (11.6 billion/year damage to marine ecosystems from plastic waste, 50% of the last 22 major oil spills have occurred in EU waters)

f. The Terrorism and Other Intentional Unlawful Acts (201 completed, failed and foiled terrorist attacks in the EU in 2014)

g. The Organized Crime and Trafficking (1.9 trillion/year estimated value of organized crime activities)

The solution to handle the above issues and concerns is the U.S. doing collaboration or joint alliance with Allies and Partners. It is far more effective to work through partnerships than independent thinkers.

The Conference had twelve speakers:

1st Lecture: EU Coordinated Maritime Presences (CMP) by Captain Efstathios Kyriakidis, BR Chief Operation Coordination European Union Military Staff. He discussed the main goals of CMP (Enhanced Maritime situational awareness, Naval presence and outreach, A maritime security enabler), the Gulf of Guinea (GoG) Pilot Case (Support and strengthen the EU Strategy on the GoG, Support the Yaoundé Code of Conduct) and the CMP GoG Task Force Responsibilities. These responsibilities include: ensuring overall coordination, coordinating EU and MS actions to implement the CMP GoG, completing maritime security analysis with POL/STRAT assessments, share the results with all MS and relevant partners, monitoring the implementation plan of the CMP in GoG, reporting to PSC on the implementation of the plan, and holding strategic meetings with maritime industry.

2nd Lecture: Beyond Great Power Competition? Maritime Security and the Shifting Paradigm of Global Challenges by Professor James Henry Bergeron, Political Advisor to the Commander Allied Maritime Command. Professor Bergeron noted that great power competition is based on being transactional (conducting business buying/selling). With great power competition it is essential to focus on global cyber threats. A New Organizing Paradigm may be coming, meaning that being competitive will not be business as usual; all must adjust and adapt to global needs and challenges.

3rd Lecture: Maritime Security Challenges in the South by Colonel Ghislain Lancrenon, Deputy Director of NSD-S Hub. He mentioned that the NATO Strategic Direction-South Hub (NSD-S) will assemble, analyze, and promote information sharing that contributes to NATO comprehensive regional understanding, situational awareness and decision making. His speech focused on these points: explanation and description of piracy in the Gulf of Guinea and the dynamics in the Horn of Africa, the importance of understanding the environment and having awareness of the variety and heterogeneity of international actors, enhancing force interoperability by taking advantage of NATO expertise on education and centers of excellence, capacity building and information sharing, the criticality of regional diplomacy to the enhancement of cooperation, the collaboration and coordination necessary to increase maritime security, and finally that a more holistic approach in close cooperation and coordination between stakeholders is paramount in mitigating maritime threats and vital to national, regional and global approaches, especially in a pandemic situation.

4th Lecture: EU Navies Capability Challenges by Mr. Eric Girard, Head of Unit Maritime Domain at the Capability, Armament and Planning Directorate, EDA. The EU Capabilities Development Priorities include the enabling capability for cyber responsive operation, information superiority, space-based information and communication services, ground combat capabilities, enhanced logistics and medical supporting capabilities, under water control contributing to resilience at sea, and air mobility.

5th Lecture: Maritime Security and Inter-Agencies Italian Navy Initiatives by Commander Francesco Loiero, Head of Doctrine & Standardization Office of the Italian Navy General Staff. His point was that the virtual regional maritime traffic center is a model to create virtual networks that provide, through an internet portal, unclassified information on regional and trans-regional maritime traffic by connecting operational centers of adhering navies.

6th Lecture: Security Environment out to 2035 from the Central Eastern Europe perspective by Major Radoslaw Zielinski, Doctrine and Training Centre of the Polish Armed Forces. He explained the three phases toward training the Polish Armed Forces: Phase 1: Analysis of the Security Environment (Geopolitics, Economy, Society, Urbanization, Technology, and Natural Environment); Phase 2: Analysis of the Operational Environment; and Phase 3: The Use of Polish Armed Forces.

7th Lecture: Working in the Three Levels of Cooperation to Counter Maritime Security Threats by Mr. Christopher Kremidas-Courtney, Adjunct Lecturer, Institute for Security Governance (ISG), Principal, Hybrid Threat Solutions LLC. During his speech, Mr Kremidas stated that the interoperability consists of the following three factors:
a. The Whole of Government: agencies and ministries from national to local level work together and share information
b. The Whole of Society: valuable for its ability to provide unique capabilities and information sources in addition to building support among the population for the effort
c. The Comprehension Approach: actors work together with a shared sense of responsibility and openness, taking into account and respecting each other's strengths, mandates, roles, and decision-making autonomy

8th Lecture: An Update in Maritime Security Threats the Maritime Risk Management Approach by Mr. Nick Georgopoulos, Chief Business Development Officer, Diaplous. The Global Maritime Ecosystem consists of the following systems: Maritime Logistics Chains, Ship systems, port systems, and application of technology, Shipowners, port operators, authorities, financing, technology companies, shipyards, and ship managers are the primary stakeholders in the Global Maritime Ecosystem. Maritime Threats in the 21st century consist of piracy, armed robbery, terrorism, cyber, refugees, and illegal activities such as trafficking, drugs, and smuggling.

9th Lecture: Exploring the Legal Framework for the Enhancement of Interagency and Whole Society Solutions to Maritime Security Challenges: Transboundary Cooperation on Natural Resource Management of Marine Areas Affected by Sea-Dumped Chemical Weapons by Mr. Grant Dawson, Lawyer/diplomat, Legal Adviser (Acting) Prohibition of Chemical Weapons. He stated that there are several current legal frameworks that states must take advantage of in order to prevent, reduce, and control pollution of the marine environment. Remedial Legal strategies include making adjustments to amendments and protocols, modifying practices, and customizing international law.

10th Lecture: SAURON Multidimensional situational awareness-based solution to port security challenges: The Port of Piraeus (PPA) pilot demonstration by Ms. Eleni-Maria Kalogeraki PhDc, University of Piraeus, Dept of Informatics and Mr. Ioannis Papagiannopoulos PhDc, PFSO-DPSO – DManager of Security and Environmental Protection Dept Piraeus Port Authority. Ms. Kalogeraki discussed the key role that PPA plays in Europe and Greece. SAURON responds to how port operators can identify cyber, physical or combined threats in their infrastructure, the goal of SAURON being to provide a multidimensional yet installation-specific Situational Awareness platform to help port operators anticipate and withstand potential cyber, physical or combined threats to their freight and cargo business and to the safety of their employees, visitors, passengers and citizens in the vicinity. The SAURON project uses the SAURON Holistic Situation Awareness concept – Physical, Hybrid, and Cyber Situational Awareness.

11th Lecture: Stakeholders Management in Maritime Security by Dr. Nikitas Nikitakos, Professor, Dept. of Shipping Trade and Transport, University of the Aegean. Dr. Nikitakos presented the five major steps in the stakeholder management process: Identify the Stakeholder, Analyze Stakeholder, Plan Stakeholder Management, Manage Stakeholder Engagement, and Control Stakeholder Engagement. Stakeholders (external and internal) include port, terminal, legal, crew, labor, incident management, education, training, and more.

12th Lecture: Maritime security threats in the Western Indian Ocean: Threat Escalation and Whole of Government Approaches by Professor Francois Very PhD, Research Coordinator Security Institute for Governance and Leadership in Africa (SIGLA). Whole-of-Government public services, agencies, and organizations must collaborate to achieve shared goals. Integrated government responses to critical and challenging issues are achieved through policy development, program management, and service delivery. Threats range from “soft” to “hard,” which include terrorism, insurgency, and hybrid threats. Finally, the Maritime Security in the Western Indian Ocean uses in the matrix approach, which consist of four categories: Marine Environment, Economic Development, National Security, and Human Security.

CLOSING REMARKS

To sum up we can say that with four keynote speakers and twelve powerful lectures from established maritime global experts and academic professionals, the conference covered every critical maritime security area.

As a young captain in the U.S. Army Reserves, Lieutenant Colonel Brown was called up to work at the Pentagon on the Crisis Action Team after 9/11. For her outstanding efforts, she received Army Staff Identification Badge and Global War on Terrorism Service Medal. As a major, Wendi Brown completed two consecutive combat tours in Afghanistan, which lasted for 18 long months. For her exceptional efforts in combat, she received the Bronze Star Medal, Defense Meritorious Service Medal, Non-Article 5 NATO Medal, Global War on Terrorism Expeditionary Medal, Afghanistan Campaign Medal, and NATO Afghanistan Service Medal (ISAF-International Security Assistance Force). As a lieutenant colonel, she worked at the U.S. European Command in Germany, joint operations environment, to monitor terrorist activities for 51 countries and territories including Europe, Russia, Ukraine, Turkey, and Israel to ensure stability throughout NATO and European Union. Also, Lieutenant Colonel Brown, completed logistical support to a global NATO communication network contingency operation to ensure computer and internet interoperability among NATO countries in case of terrorist or enemy network attacks against critical infrastructure. In the following assignment, Lieutenant Colonel Wendi Brown worked at the U.S. Africa Command, another joint operations environment, to monitor terrorist activities on the African continent. While working full-time, Lieutenant Colonel Brown earned her first Master of Science in Cybersecurity, graduating summa cum laude; an educational curriculum coordinated and endorsed by the U.S. Department of Defense. Four years later, she earned her second Master of Science in Cybersecurity. The graduate degree was Master of Science in Cybersecurity with Specialization in Cyber Intelligence, graduating summa cum laude; an educational curriculum coordinated and endorsed by the U.S. National Security Agency and U.S. Homeland Defense.

Maritime Human Smuggling and Implications for Littoral Operations

by Cdr Peter THOMSSON
Royal Swedish Navy

Thomsson is Chief of Staff of the 4th Naval Warfare Flotilla in Berga. He holds Masters' degrees in War Science and in Economics and Business. He has also worked in finance and in the defence industry and is a fellow of the Royal Swedish Society of Naval Sciences.

This article is based on a contribution to the OpTech East Med conference at the NATO Maritime Interdiction Operational Training Centre in Souda Bay, Crete, in November 2019. It was organised by the Littoral Operations Center at the U.S. Naval Postgraduate School. The article is a updated and revised from a previous version was published in the journal of the Royal Swedish Academy of War Sciences. It incorporates an elaboration that could not be accommodated under the time constraints at the podium Although based on professional experience, all views and opinions are the author's own.

1 Introduction

I would like to express my gratitude to the NATO Maritime Interdiction Operational Training Centre (NMIOTC) and the Littoral Operations Centre at the U.S. Naval Postgraduate School for the invitation to participate in the conference OpTech East Med. I believe that the combination of venue, topic and hosting organisations was optimal for the conference, in order to appreciate complexities but also to look at the maritime responses required.

This article provides a brief outline of human smuggling across the Mediterranean in general and the Libyan example in particular. It is based on my understanding of the subject from my time in the Operational Headquarters of European Naval Force Mediterranean Operation SOPHIA in Rome as well as from operations in Afghanistan and off Somalia. Building from these experiences I would like to develop my thoughts on the implications of these types of missions for current and future littoral operations.

2 Human smuggling

Starting in 2013, several deadly accidents involving migrants occurred in the Central Mediterranean. On 18 April 2015 a small vessel capsized off the Libyan coast on its way to Lampedusa. Of the assessed 700 migrants on board only 28 survivors were eventually pulled from the sea. As far as I am aware, this remains the single deadliest event during a migrant crossing to Europe. The incident caused an international uproar and sparked several EU initiatives to stop ruthless smugglers. A ten-point

"Source: Guardia Costiera"

action plan was decided upon by an extraordinary session of the European Council, of which Operation SOPHIA was one[1]. Other items included reinforcing FRONTEX operations, increasing coordination between concerned EU bodies and engaging key countries in the region.

With a fast track process, planning for Operation SOPHIA was initiated in May 2015 with Initial Operating Capability reached only a few weeks later when a multinational force set to sea, supported by aerial and other assets[2]. This is an unparalleled accomplishment among EU operations and a sign of the resolve to swiftly address a very challenging situation despite its many complexities. Despite the wide range of efforts and progress made, human smuggling and casualties keep occurring, albeit at a lower level. Operation SOPHIA ended in March 2020, being succeeded by Operation IRINI that has the aim of enforcing the arms embargo to Libya[3].

2.1 Smuggling

The problematic of smuggling dates back a long time, as part of a greater challenge in the Mediterranean crossroads that since the earliest days of civilisation have been a central hub of human activities and trade. There are numerous smuggling routes towards and across the Mediterranean. There is substantial overlap between the different kinds of flows as smugglers employ established networks but alternate between the types of merchandise according to changes in demand, perceived risk and profitability. Migrant smuggling and trafficking appear to offer relatively low risk for high returns.

In this article, migrant smuggling refers to persons who travel by their own subjective will, at least to some extent, while trafficking refers to persons who are traded and transported as objects, with little or no influence over their situation. For both categories there seems to be an excess in demand for smuggling, which will maintain criminal activities and cause smugglers to innovatively adapt and seek new ways and means to achieve their ends, if they are countered.

2.2 Migrants, asylum seekers and trafficking victims

Turning to migration there are a number of factors influencing migration in the region. The International Organization for Migration, IOM, points to demographic and socioeconomic trends, climate change and conflict as being the main causes for migration[4].

Armed conflict is certainly a case in point with regard to Libyan smuggling, where transiting migrants and refugees originate from a wide area from Central Asia and the Middle East to Africa. According to the United Nations High Commissioner for Refugees, UNHCR, in 2020 there were almost 80 million forcibly displaced people in the world. Many of these are in the Middle East or Northern Africa.

Globalisation has opened trade flows between poorer and richer regions. In the wake of this, information about the standard of living and employment opportunities have become accessible for disenchanted individuals who seek to travel to what is perceived as the land of plenty. The ease of access to and opportunities at the destination are often strongly exaggerated by smugglers, as marketing, as well as by those who have travelled before, who seek to justify the costs that often leave families indebted to smugglers for years. In operation SOPHIA we saw the smuggling routes being employed for escaping war as well as of seeking better ways to provide for their families, many with combinations of these and ambiguous grounds for determining their right as asylum seekers or other status. It should be borne in mind that not only asylum rights but also the general standard of living makes Europe attractive. This is true even for those who are limited to an irregular status in the

[1] European Commission: Press release Joint Foreign and Home Affairs Council: Ten point action plan on migration, European Union, 20 April 2015.

[2] Council of the EU: Press Release 482/15: Council launches EU naval operation to disrupt human smugglers and traffickers in the Mediterranean, European Union, 22 May 2015.

[3] Council of the European Union, "Council Decision 6414/20 on a European Union military operation in the Mediterranean (EUNAVFOR MED IRINI)" (European Union, 25 mars 2020), https://data.consilium.europa.eu/doc/document/ST-6414-2020-INIT/en/pdf.

[4] World Migration Report 2018, International Organization for Migration, Geneva 2017.

European Union and the grey or even black labour market, where many are cynically exploited.

Some migrants, especially those with a relative level of wealth, make a single payment at the point of origin to purchase a passage by several transportation means all the way to the destination. Others are repeatedly pressed for additional payments at each stage of the journey, despite having been promised a package deal. This leads to extortion where families are pressed for ransom payments, to abuse and mutilation or even to migrants being sold as slave labourers or trafficking victims. Some, especially young women, are trafficked from the outset, most often for prostitution. Others fall victim to trafficking along the way as they are snared by criminals.

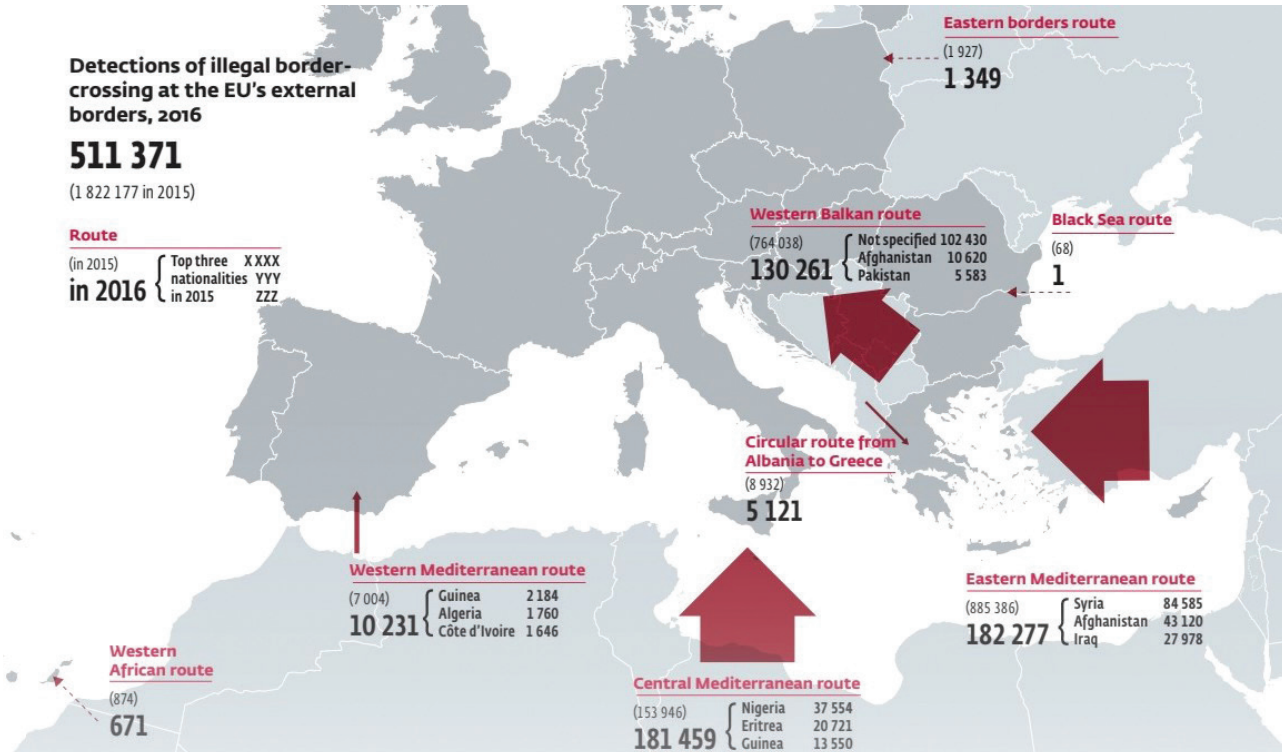
Crossing the land continent is challenging; across barren deserts, regions with contested control and national borders where passage may or may not be permitted. Having reached the coastline migrants and trafficking victims are crammed together in so called safe houses for days or weeks before departure. This naturally poses great risks for the spread of contagious diseases, in itself a concern when migrants originate from regions stricken by Ebola or other epidemic diseases. There have also been cases where competing smuggling bands have intercepted boats after they have set off, to press the migrants for their last possessions.

2.3 The crossing

The graphic below from FRONTEX shows illegal border-crossings into the European Union in 2016, with 2015 in parentheses. Those were the two years with the greatest total number of arrivals in modern time. Cross Mediterranean human smuggling and migration has, however, been present as a phenomenon for a long time, shifting between different routes and means over time, as well as in quantity.

The fluctuation is mainly attributed to changes in push factors, such as armed conflict, and the availability of a transit corridor through which to arrive at the coastline and set out across the sea. The latter occurs when law enforcement is insufficient to stem migrant flows. The most significant impact recently was the conflict in Syria, occurring at the same time as governmental control decreased in the post-Ghaddafi turmoil. This opened up Libya as a transit channel and smugglers were quick to establish their networks. The business idea is to provide access for asylum seekers and economic migrants into Europe, preferably into the Schengen area.

According to the Missing Migrants project, in the period from January 2014 to September 2020, about 20,500 migrants died during their journey crossing the Mediterranean[5]. Not only do smugglers abuse, extort and sometimes kill migrants, there are furthermore indications that the business model is based on a ruthless understanding of a fatality tolerance of a percent or more. During my time in Operation SOPHIA it seemed that following mass drownings, smugglers took measures to reduce risks and the number of fatalities



"Source: FRONTEX, Risk Analysis for 2017."

[5] IOM Missing Migrants Projects: "Spotlight on the Mediterranean", https://missingmigrants.iom.int/region/mediterranean (29 September 2020).

“Source: Guardia Costiera”

decreased. That effect was often temporary as greed soon again took precedence over caution. But as long as migrants, in one miserable way or another, are landed in Europe, there is little disincentive for others against trying. Consequently, yet more are encouraged to undertake the journey, in turn exposing themselves to the risk of atrocious abuse while at the same time financing large scale organised crime[6].

Looking closer at the Libyan example, Libyan smugglers long ago abandoned any intention to ensure that the migrant vessels reach all the way across to the European mainland or even the European islands closest to the African coast. Instead, they rely on the legal and binding obligation for mariners to save lives. Thus, they cause each crossing to become a Safety of Lives at Sea (SOLAS) event. Thereby ships of all kinds are forced to render assistance, if they are capable, as prescribed by article 98 of the United Nations Convention on the Law of the Sea. Smuggling vessels, rubber or wooden boats, are rarely in shape to put to sea and are furthermore crowded and heavily overloaded. There are accounts that on occasion, migrants reluctant to board unseaworthy vessels have been killed on the beach to coerce others to board for the perilous journey. The rubber boats, often imported from less scrupulous exporters in the Far East, may even be of substandard components and construction that will start to disintegrate after a few hours at sea. While wooden boats may appear safer, they can be so crowded that smugglers put migrants in locked compartments below deck for stability reasons, which has caused death by suffocation.

This deliberate and coldblooded business practice on the part of smugglers causes difficult dilemmas. Just as an example, in 2015 several non-governmental organisations (NGOs) started operating closer to the Libyan coast, seeking to reduce risks for migrants. But in doing so, they became an instrumental part of the business model, as smugglers adapted to the changed conditions this implied. During my time in the operation, I saw the average distance from coast to SOLAS event slashed from 80 nautical miles (NM) to around 20NM. At the same time, boats were launched from the coast ever more overloaded, in poorer state and in harsher weather conditions. Thus, with the honourable intention of saving lives, NGOs were exploited to allow smugglers greater profits. It is possible that the decreased smuggling from Libya to a great extent is an effect of the re-establishment of the Libyan Coast Guard. Here it might be worth to point out that it may be both unhealthy and unprofitable for a coast guard officer to counter smugglers. However, the decrease may to some extent also be an effect of the reduced presence of NGO vessels close to the coast, since

[6] Desperate Journeys - Refugees and migrants arriving in Europe and at Europe’s borders, UNHCR The UN Refugee Agency, Geneva 2018, pp. 21–27.

SOLAS events in late 2018 occurred in excess of 100NM from the coast.

2.4 Large scale rescue operations

The subsequent large-scale rescue operation entails substantial risks for all parties involved. If not already shipwrecked, the migrants upon seeing a rescue vessel may cause their own to capsize as they rally to the side of the vessel facing the rescue. The process of taking hundreds of persons on board is difficult, exacerbated by their being weakened by starvation, dehydration and abuse. Modern merchant and naval vessels often have high freeboards and few access points for rescue operations. Once on board, the shipwrecked must be tended to, with food and water as well as sanitary and resting possibilities. But neither naval, nor merchant, vessels are adapted for mass rescue of this kind. Indeed, the Mediterranean situation caused the International Chamber of Shipping (ICS) to issue guidance on the subject of large-scale rescue operations at sea, in 2014 with a revised second edition issued in 2015[7].

Furthermore modern merchant vessels have small crews, which risks causing new problems as the sheer number of people taken on board and their needs to be tended to may compromise the security provisions of the ship and invalidate measures in the Ship Security Plan that are required under the International Ship and Port Facility (ISPS) Code, Chapter XI-2 of the SOLAS Convention[8]. The small crews and sometimes insufficient possibilities of isolating restricted areas pose a risk for hijacking. In March 2019, a group of shipwrecked migrants hijacked the ship that had rescued them, when they learned that it was bound for Libya. This was contrary to the promises made by smugglers and so they demanded instead to be taken to Europe. The situation had to be resolved by a military Hostage Rescue Operation.

From time to time, smugglers seek to recover the vessels, after the SOLAS event, in order to reuse them for yet another launching of migrants. Despite normally being in poor state, the smuggling boats represent a value both from a financial standpoint but also from the fact that boats are hard to come by. Some have been destroyed by conflict, others have been seized at sea and rubber boats may even be seized as they are imported. At first they maintain distance, posing as fishermen or any other innocuous activity meant to keep them from being compromised and to avoid undesired attention from patrols. Once the migrants are transhipped to a rescuing vessel, smugglers sweep in to try to recover the boat. In some cases, smugglers have even fired upon rescuers.

“Source: Guardia Costiera”

2.5 Additional risks and threats

Unfortunately, the hardships endured by the migrants and the consequent increased risk of contracting contagious diseases poses a risk also to the rescuers, especially with large numbers of people within the limited space available.

Other concerns are those of the risk of terrorists infiltrating migrant groups. They could do so either to strike ships or to carry out attacks on targets ashore, the main threat feared being that of suicide bombers or bomb-laden vessels. There have been several instances of suspected foreign terrorist fighters being encountered on the Mediterranean routes. Between July and September 2019, INTERPOL conducted Operation Neptune II, detecting more than a dozen suspects in ports of debarkation in southern Europe[9].

Yet another type of threat is that of military weapons systems, employed either by regular or irregular armed groups or even terrorists. Naval irregular warfare has not attracted

[7] Large Scale Rescue Operations at Sea - Guidance on Ensuring the Safety and Security of Seafarers and Rescued Persons. Second edition. International Chamber of Shipping, London 2015.

[8] International Convention for the Safety of Life at Sea (SOLAS), International Maritime Organization, London 1 November 1974; Thomsson, Peter and Widlund, Mattias, Sjöfartsskydd & ISPS-koden, Third edition, Jure Förlag AB, Stockholm 2017, p. 14.

[9] Foreign terrorist fighters detected during INTERPOL maritime border operation, INTERPOL, Lyon 19 September 2019, https://www.interpol.int/News-and-Events/News/2019/Foreign-terrorist-fighters-detected-during-INTERPOL-maritime-border-operation (29 September 2020).

as much attention as that on land but represents a substantial threat to be reckoned with. Indeed, force protection or the capability to mitigate this kind of threat are part of the reasons for deploying naval vessels and other military assets for a mission that primarily would be a civilian mission. Another concern is the law enforcement part of the mission that requires efforts to collect evidence and to identify smugglers. This can be risky but is a necessary component in the full range of efforts to combat this criminal activity. Fortunately, law enforcement authorities can contribute training and second officers to the ships.

2.6 Assets employed

Widening the perspective to include another mission primarily of a policing character, that of counter piracy, it is perhaps no surprise to see that the capabilities are similar. Consequently, the assets requested in the Combined Joint Statement of Requirements (CJSOR) and in Force Generation Conferences, show a high degree of correspondence. In EUNAVFOR Operation ATALANTA, off Somalia, participating nations have contributed vessels for off-shore patrolling, ranging from corvettes to destroyers and even LHDs (Landing Helicopter Dock ships); reconnaissance aircraft either of sophisticated military types, coast guard or even civilian aircraft; as well as specialized teams for boarding and interviewing. To this can be added general ISR (Intelligence Surveillance and Reconnaissance) assets and systems that tend to be the same for supporting any military mission.

While counter-smuggling, just like counter-piracy, may seem to make suboptimal use of military assets like those listed, they are nonetheless two types of challenging missions. Being better equipped than most other law enforcement vessels to respond to military threats, naval vessels may be the only choice for these types of missions. Furthermore, due to their mobility, dexterity and versatility, naval vessels are likely to remain politicians' preferred instrument for operations in littoral environments. They can be employed in the full spectrum from counter-smuggling, counter-piracy and counter-terrorism to low- and high-intensity conflict. This width of operational types naturally poses a challenge to ensure that ships, equipment, doctrine and training provide adequate support to build the required situational awareness and the capability to operate in an environment that is expected to be cluttered, contested and constrained[10]. For this, I am sure that the NMIOTC is an excellent organisation to hone the skills for a key part of the operational spectrum.

3 Implications for future operations in the littorals

Some of the solutions that may be forwarded to address migrant smuggling have already been implemented. Information campaigns in countries of origin counter the exaggerated marketing of smugglers. Embargoes and other ways to intercept weapons and rubber boats in transit to launching areas have been enacted. There are also capability development efforts in supporting Libyan authorities in countering the smugglers.

Looking further, I would like to finish by offering some thoughts on future operations. I find it unlikely that the ambiguous nature of conflicts will decrease. With an increase of hybrid threats and grey zone activities, the threat may not be the high-intensity and clear-cut type. Rather the requirement to be capable of addressing a low-tech threat and of discriminating between legitimate and illegitimate targets remains. This is of particular importance in the busy littoral waters with a plethora of activities and actors. It is further compounded by the increased practice of employing sophisticated efforts to deceive and confuse as well as working through proxies or other non-attributable measures. However, it is also complicated by the necessity to cope with peer or near-peer state adversaries, employing state-of-the-art technologies.
At this time, Anti-Access, Area-Denial (A2/AD) are very pertinent subjects. This extends far out to sea but naturally also has consequences for operations in the littoral area. Since this has attracted strong interest and been analysed upon by experts in the field, I will abstain from elaborating on the subject in this article.

Photo: Melina Westerberg, Swedish Armed Forces"

[10] Development, Concepts and Doctrine Centre (DCDC): Strategic Trends Programme - Future Operating Environment 2035, Ministry of Defence, London 2015), pp. 33–34.

3.1 The littorals

The littorals have substantial concentrations of human population as well as resources and are also the cross-roads for trade and other exchange, a fact which may not be widely known but is uncontroversial and central for naval officers. It is even suggested that for future conflict, the littorals may be designated as strategic centres of gravity. The increased importance of the littorals has been recognised since the end of the 20th century.

With the vast majority of all maritime activity being located in, or at some point passing through the littorals, it may be wise to ensure capability to operate in this type of environment. Shallow waters, narrow passages and choke points or other navigational constraints make of the littorals an operating environment that possesses other opportunities and limitations than the open sea. This implies a difference in what types of weapons and sensor systems as well as tactics that can be employed. Despite technological advances, it remains challenging to detect, acquire and engage surface and subsurface targets close to the coastline, especially in archipelagic areas and waters busy with merchant and fishing vessels[11]. The coastal state, or potentially a coastal non-state actor, also benefits from the shorter ranges and protected waters that enable the use of small vessels. These can be used for swarming tactics, as have been employed by Iran in the Strait of Hormuz. Naturally, the coastal state also enjoys the home-field advantage of being able to bring land and air systems to bear. By exploiting technological gains, autonomous vehicles can be used for various purposes by an attacker. Unmanned systems, in particular in the lower cost range such as COTS (Commercials off the shelf) that are adapted for military use may well be more frequent in coastal areas where there is a lesser need for speed and endurance.

Shallow and constrained waters provide ample opportunities for both offensive and defensive mining as well as other means of modern undersea warfare. Covertly delivered, such systems have a capability of wreaking havoc on an enemy's freedom of movement at sea. However, a deliberately conspicuous emplacement will also represent a threat to sea lines of communication and cause time consuming mine clearance, where time is traded for probability of clearing all mines, or rerouting. This is a powerful tool for coercion and for shaping the battlespace. The spectre of sea mines and maritime IEDs has reappeared with an increasing number of mine incidents and detections in the Red Sea and off Syria since 2015[12]. Creating ambiguity and sowing doubt may have equal or potentially stronger effect than a successful attack. For example, the unclaimed explosions on tankers off Fujairah in May 2019 and in the Strait of Hormuz in July 2019 immediately affected oil prices and brought the world's attention to the region while retaining some deniability for the alleged perpetrator, even if Iran is strongly suspected for direct or indirect involvement. Since the end of the Cold War, mine countermeasures (MCM) have seen little priority globally. Some navies have disbanded their MCM vessels without replacement. Others are trying to rebuild neglected MCM capability. This may be hazardous, given the increase in maritime IEDs and the growing importance of the littoral waters.

The problematic of developing naval strategy has been exacerbated by new challenges from grey zone activities and hybrid threats[13]. Contributing directly or indirectly, naval forces are critical to secure shipping but priorities are difficult to make as the limited number of units cannot balance the numerous and vast trade activities. The renewed interest in container based weapons systems to arm civilian vessels is ambiguous[14]. Containerised weapons systems onboard can offer offensive as well as defensive capabilities, see for instance the Russian Club-K, Israeli LORA or Australian EOS R400 systems. These reinforce the connection to civil-military relations to ensure proper appreciation of potentially hostile activities within the full strategic context, especially under the density of activities that characterises the littorals.

3.2 Scouting and Antiscouting

With the Eastern Mediterranean being a very busy maritime region, obtaining sufficiently detailed situational understanding to make decisions and conduct operations was a challenge in Operation SOPHIA. Every technological gain, be it in sensor range and detection capability or in weapons range, speed or hit probability, in itself also represents an imperative for the adversary to counter it, which naturally applies also to an irregular actor. The latter was blatantly

[11] Hughes, Wayne P: Fleet Tactics and Coastal Combat, Second edition, Naval Institute Press, Annapolis, MD 2000, p. 167.

[12] Heubl, Ben: ”How a growing naval mine threat upsets the Royal Navy”, E&T Engineering and Technology, London 2 November, 2020, https://eandt.theiet.org/content/articles/2020/11/an-ageing-mine-hunting-fleet-puts-pressure-on-royal-navy-s-defence-capabilities/ (9 November 2020)

[13] Granholm, Niklas: “Small Navies and Naval Warfare in the Baltic Sea Region” in McCabe, Robert C, Sanders, Deborah and Speller, Ian (eds) Europe, Small Navies and Maritime Security: Balancing Traditional Roles and Emergent Threats in the 21st Century, Routledge, Oxon 2019, pp. 73–85.

[14] Norbert Doerry: ”Institutionalizing Modular Adaptable Ship Technologies”, Journal of Ship Production and Design, 2014, pp. 5–9.

obvious in Operation SOPHIA where smugglers made efforts to avoid detection and deceive sensors by hiding among commercial and fishing vessels. Sophisticated actors can employ signature reducing measures in multiple dimensions, which, when combined with adequate tactics, may negate technological advances in sensor and sensor integration. This may render extended ranges and higher speeds practically irrelevant. At least it may reduce the effective engagement distance to such a degree that it forces the attacker to operate in less advantageous ways or at shorter range than preferred.

Given that a firing solution starts with locating and acquiring target data, scouting and anti-scouting measures represent a competition in itself with the objective being to deny the opponent the ability to "fire effectively first". To a great extent, this echoes the findings of the late Wayne P. Hughes. In 2000 he pointed to trends towards defence by cover, deception and dispersion, towards unmanned and autonomous systems and integrated cooperative engagement technologies. Cover, deception and dispersion could potentially be mitigated by multi-disciplinary sensor fusing and by big data analysis, the downside of which is that it is dependent on technology and communications. Particularly with reference to the capabilities that sophisticated command and control systems offer, Hughes reminds us of the concurrent vulnerability of such systems if and when we become excessively reliant upon them. Indeed, an opponent may well exploit this by employing technological asymmetries by creating an electronic warfare (EW) environment in which his systems and doctrine enjoy a comparative advantage. Naturally, this renders the already challenging concept for cooperative engagement even more difficult[15]. There is thus a risk that an exaggerated dependence on technology and on a close command and control loop will hamper or even paralyse modern naval forces, particularly in littoral waters which are challenging for many kinds of sensors.

Particularly in the archipelagic waters, operating close to the coast or behind islands can deny the use of extended sensor and weapon ranges, potentially even the use of hypersonic weapons if terminal phase manoeuvring cannot be executed at sufficient distance to strike the target. Hence, within the final miles to shore the effective striking power of small and stealthy vessels with light and shorter range weapons systems may be bigger than that of larger vessels with heavier and longer range weapons systems. Naturally, this is under the condition that the small vessel has the capability to adequately manage close range and cluttered combat environments. Strands of this reasoning can be seen in a recent report, which suggests changing the force composition of the U.S. Navy by increasing the number of small manned and unmanned surface vessels at the expense of large vessels; in an effort to increase capability, reduce costs and improve tactical decision-making[16].

In some cases, less sophisticated technology has its advantages. In Operation SOPHIA a civilian aircraft with a couple of standard civilian instruments allowed crude sensor fusing by an operator on board. This enabled detection, location and classification of vessels at sea. It was a relatively unsophisticated platform that successfully provided actionable intelligence for the operation at low cost. Similarly, the civilian maritime patrol aircraft of the Swedish Coast Guard were some of the most capable in Operation ATALANTA off Somalia. While this may not translate into high-intensity conflict it does serve as an example of affordable sensors that can provide valuable situational awareness in lower conflict ranges. The use of unmanned sensors already in practice also represents a lower cost, if not in money then at least in lives at risk.

3.3 Situational understanding or situational misunderstanding

Other means an adversary could employ to gain an advantage would be to target cognitive processes, in order to degrade the ability of operators and decision-makers to properly assess the situation and implement the necessary actions. There is a requirement for a joint and detailed situational understanding to be able to react in time. Furthermore, this must be adequately balanced; neither over- nor under-reacting, and doing so in time so as not to be presented with a hard to reverse fait accompli. Modern western armed forces are to a high degree reliant on technology and may have become complacent from low-intensity conflict, which represents a known vulnerability. The advantage may well lie with the challenger, for whom degrading the use of technology may be sufficient. However, even when actions can be observed and

[15] Dalsjö, Robert, Berglund, Christofer, and Jonsson, Michael: Bursting the Bubble - Russian A2/AD in the Baltic Sea Region: Capabilities, Countermeasures, and Implications, Försvarets forskningsinstitut, Stockholm 2019, pp. 73–75, 85–93.

[16] Clark, Bryan and Walton, Timothy A.: Taking Back the Seas - Transforming the U.S. Surface Fleet for Decision-Centric Warfare, Center for Strategic and Budgetary Assessments, Washington, D.C. 2019, pp. 21–26, 64–78, 84–87.

attributed to an adversary, there remains a risk of failing to understand the meaning, since 'seeing is not necessarily believing'. This has been shown by numerous military surprises throughout history. One way to mitigate this is by extensively adopting mission command, supporting the commander on scene with the requisite means and mandate[17]. However, this requires fundamental doctrinal cohesion and application throughout the command chain to be practicable. The same applies for force integration in joint and combined operations. As advanced during OpTech East Med, technical interoperability is a necessary but insufficient requirement for effective force integration. Both of these may be more difficult to implement in practice than to express in guiding documents.

Due to the strategic repercussions from complex situations it has been argued that the freedom of action for tactical commanders should be limited, for the benefit of more holistic and coordinated decision making in higher commands. Recognising the concerns, I nonetheless disagree, since in my mind the complexity and limited time for decision making are instead precisely the reasons to entrust skilled tactical commanders present in the situation the mandate required to execute timely and adequately balanced actions. Such extensive responsibility of the commander at the scene to take the necessary measures, even challenging higher command when the situation so dictates, dates back more than a hundred years in the idea of *Verantwortungsfreudigkeit*[18]. Granted, this places high requirements on the commander for gauging consequences and making decisions, but this is facilitated by technological and organisational advances onboard along with the continuous training. The capability for this may well have benefited from the international security operations of the past 20-30 years and the awareness of far reaching ramifications of actions – or inaction – as with the so called 'strategic corporal' [19]. As an example, persistent underwater incursions through the 1980s forced Sweden to elaborate robust standing rules of engagement. By these the commanding officer has the mandate to use deadly force against a foreign submarine within Swedish internal waters, already in peacetime[20].

Mission command may be more challenging at lower conflict levels, where the error margin is smaller as even minor tactical actions may have far reaching consequences. The German Auftragstaktik that is often advanced as a model is not always implemented in the way originally conceived, due to differences in strategic culture and other factors. For mission command to function effectively it has to be nurtured within an allowing culture. The mandated subordinate must enjoy a high level of trust[21]. Furthermore, the subordinate must also have an advanced understanding of the mission's purpose and the superior commander's reasoning so as to act in line with the commander's intent. Small, peripheral nations by sheer necessity need to be agile and respond to surprise, implying a high level of trust for subordinates. Technological developments with Network Centric Warfare and operations with lower tolerance for deviation or failure may have hampered the conditions for mission command. Furthermore, in addition to a mandate, the commander on-scene must be furnished with units possessing the capability and agility to adapt to the situation at hand. This needs to be possible at short notice and as the situation evolves, so as not to be overtaken when the adversary increases tempo. With all due respect for the shortcomings of human cognition, I am sceptical that artificial intelligence will within the foreseeable future be able to replace a human being in factoring in and weighing all aspects and making necessary decisions.

3.4 Learning from the less obvious

How does all this tie in with the human smuggling this article started out from? According to the UK Development, Concepts and Doctrine Centre, the future operating environment is expected to be characterised by 5 Cs in being: congested, cluttered, contested, connected and constrained. This description is fitting for littorals in general and probably even more so for the littorals of conflict areas where refugees, trafficking victims or migrants may well be encountered both in the coastal areas and offshore. While the problematic of human smuggling and trafficking is a tragic phenomenon in itself and primarily a policing mission, it also represents one end of the wide spectrum of naval operations in the increasingly congested littoral zone. Furthermore, as has been advanced under the label of "weaponization of migration", it is a potential tool for an adversary to employ along with contracting organised crime and other covert means within a greater scheme to influence the target state.

It is possible for an antagonist to covertly mine a fairway by making use

[17] Vego, Milan: "On Littoral Warfare", Naval War College Review, Spring 2015, Vol. 68, No. 2, pp. 60-62.

[18] Exerzier-Reglement für die Infanterie, Kriegsministerium, München 1906, pp. 90-91.

[19] Charles C. Krulak, "The Strategic Corporal: Leadership in the Three Block War", Marine Corps Gazette 83, No. 1 (1999), pp. 20–22.

[20] Handbok IKFN Hävdande av vårt lands suveränitet och territoriella integritet (H IKFN 2016) Stockholm: Försvarsmakten, 2016, sect. 69.

[21] Doktrin Gemensamma operationer Stockholm, Försvarsmakten, 2020, p. 31.

of an inconspicuous merchant vessel, where a single mine may cause enough uncertainty and disruption to achieve desired ends[22]. Such a tactic was tried by Libya in the Red Sea to disrupt Saudi trade. Even if these types of operations may appear different from high-intensity conflict between peers or near-peers, it would be unwise to envisage such conflict, even in a worst case large scale war, as something of the like of World War II. Rather, a skilled adversary should be expected to make use of any and all ways to deceive and confuse where difficulties faced in the lower conflict range or even in policing missions may be created. The example of the Swedish Coast Guard aircraft also serves as an example of the benefits from closer integration between governmental authorities, something that is also crucial for addressing grey zone threats in national defence operations.

The future operating environment is expected to exhibit more convoluted civil and military aspects in warfare, as is taken into account in descriptions of hybrid threats and grey zone activities. Indeed, on this there is agreement across the divide since references are often made to a speech by the Russian Chief of the General Staff, General Valery Gerasimov, that is often used to designate the contested term of Gerasimov doctrine[23]. Knowingly employing the terminology for these terms, for which final agreement on definition remains to be seen, I see them as indirect strategies and ways either to obtain objectives without escalation to armed conflict, or to shape the battlespace, should armed conflict be unavoidable. Conditions are expected to be more obfuscated as an adversary when possible will employ a wider range of instruments of power, fomenting dissent and divide to obtain his objectives or at least to shape the battlespace for potential armed conflict. This may perhaps be easier on land where there are human activities of greater scale and diversity, bearing in mind that the object of war remains on land. Nonetheless, the littorals are expected to grow in importance and consequently so will the risk for conflict. Naval operations today are an even more indispensable component of a comprehensive strategy. Naturally, this is already recognised by leading professionals, as for instance by the former SACEUR, Admiral Stavridis[24].

3.5 Flexibility is of the essence

The key take-away I offer is that unfortunately we will not revert back to a clear-cut conflict situation but find challenges aggregated or even compounded. This adds to the complex operational environment, about which I have developed my thoughts above, drawing on the expertise of other theorists, practitioners and analysts. Thus, learning to master convoluted operational environments such as the littorals of Libya – with migrants, smugglers, terrorists, platforms and maritime traffic – reduces the risk of being overwhelmed by the 5C-operational environment and a deliberately caused chaos that an adversary may attempt to use. In that vein, while employing sophisticated, high value assets like modern warships in policing missions remains somewhat unsatisfactory, I strongly believe that there is a learning opportunity from which to benefit, which will allow for honing crucial skills for mastering a future, more complex, operating environment.

State-of-the-art technology can be exploited to improve situational understanding but such use must not become a reliance that presents a critical vulnerability. Ability to sustain low-tech operations or to operate in a challenging environment must be maintained as well as flexibility to quickly adapt as the situation evolves. The example of the civilian airplane serves to show that in the daily operations as well as at lower conflict levels low-cost solutions may bring substantial benefit that may complement – but never replace – the sophisticated units built for high-intensity conflict. From sheer economic rationality, in the lower conflict range we cannot do without sensor systems that are affordable in procurement or operating costs, even if they lack robustness for wartime conditions. Nonetheless, the challenge is to strike a balance between these and more costly but robust systems required for high-intensity conflict.

To be able to cope with the surprise that an aggressor will seek to achieve, Finkel develops a strong argument for flexibility in several strata: doctrinal and conceptual; organisational and technological; cognitive and command and control; and lessons learning and rapid dissemination. He postulates that these are required for a military organisation to successfully overcome surprise[25]. After all, it would be unwise to expect the enemy to follow a script and role that we have written, or more succinctly expressed in the quote “The enemy gets a vote”, ascribed to former the former US Secretary of Defence, James Mattis. The experiences of recent security assistance operations

[22] Murphy, Martin and Schaub, Gary Jr.: ”’Sea of Peace’ or Sea of War - Russian Maritime Hybrid Warfare in the Baltic Sea”, Naval War College Review vol. 71, no. 2 2018: p. 17; Stavridis, James: ”VI. The United States, the North Atlantic and Maritime Hybrid Warfare”, Whitehall Papers vol. 87, no. 1 2016, p. 96.

[23] Jonsson, Oscar: The Russian Understanding of War - Blurring the Lines between War and Peace, Georgetown University Press, Washington, D.C. 2019, pp. 19, 73.

[24] Stavridis, James: ”Maritime Hybrid Warfare is Coming”, United States Naval Institute. Proceedings vol. 142, no. 12 2016.

[25] Finkel, Meir: On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield, Stanford Security Studies, Stanford CA 2011, pp. 224–225.

have been ambiguous. Overwhelming technological and organisational superiority has allowed for elaborating complicated plans with lines of operation stretching across several phases on a great time scale. Despite this, events in the battlespace have forced frequent minor and major alterations to the plan. This fits well with the adage that "plans are nothing, planning is everything", often attributed to US General Dwight D. Eisenhower. Assessing and adjusting the plan provides strategic and operational flexibility. Mission command, as discussed above, offers the possibility to parry unexpected developments and exploit opportunities, to an extent that cannot be planned ahead. In essence, I argue that mission command when well implemented is crucial for successful operations in modern, rapidly developing conflicts of all levels of intensity.

4 Final remarks

I hope that with this article, based on my contribution to the OpTech East Med conference, I have conveyed some of my understanding of a complicated web where human smuggling interacts with large scale organised crime and potentially also with terrorism and war. To this I have added some thoughts of implications for littoral operations. Naturally, my thoughts are not altogether unique as I have tried to show by the referencing. Of particular mention is the late Capt. Wayne P. Hughes whose Fleet Tactics and Coastal Combat is a recommended read for anyone with an interest in the littorals and in which the fictional battle incidentally is situated just off Crete, in the Aegean. The subject remains current, only in December 2019 an article at the U.S. Naval Institute made a similar argument[26].

Since this article is based on experiences from the counter-smuggling operation off Libya it builds from a low-intensity littoral operation to argue for the lessons that can be learned from these and similar operations. What is suggested in this article is in no way meant to infringe upon the core mission of modern navies: the capability to successfully engage in high-intensity conflict at sea. Rather, I argue for how recent experiences in the lower range of conflict can contribute to being capable of addressing a wider range of challenges as the conflict spectrum is broadened to include activities such as hybrid or grey zone operations.

While I fear to have delivered more questions than answers, I hope at least to have contributed to the understanding of the challenges ahead. I am looking forward to learning of current and future ways and means to overcome whatever challenges we must face. As Rear Admiral Drimousis pointed out in his opening remarks at the OpTech East Med conference, in the modern day the littorals are an operating area of utmost importance.

Commander Thomsson, Royal Swedish Navy, is Chief of Staff of the 4th Naval Warfare Flotilla in Berga. Prior to this he was posted in the Swedish Defence Staff and in the Maritime Component Command. He has served internationally in NATO ISAF in Afghanistan, in EUNAVFOR Operation ATALANTA and in EUNAVFOR MED Operation SOPHIA. Thomsson holds Master's degrees in War Sciences as well as in Economics and Business. He is also a fellow of the Swedish Royal Society of Naval Sciences.

[26] Colin Barnard: "Baltic and Black Sea Navies Must Invest in Littoral Warfare", United States Naval Institute. Proceedings vol. 145, no. 12 2019.

Beyond the Responsibility Gaps in the Use of Autonomous Weapons: The Need for a New Ethical Framework within a Political Context

by George Kiourktsoglou

Introduction

Starting two decades ago, the dawn of the 21st century saw the emergence of the fourth industrial revolution with disruptive innovation as its poster child. New technologies came to the fore, with applications ranging from fracking, 3D printing and robotics, to quantum computing, the internet of things, artificial intelligence (A.I.) and its crown jewel, deep learning. War, as described by Carl von Clausewitz (Clausewitz, 1873), slowly but steadily joined the rising number of human activities incorporating the latest technological breakthroughs in their DNA, causing – or about to cause – numerous irreversible mutations.

The tectonic shift in modern warfare's nature, from human-centric to machine-centric via the use of unmanned – or more accurately, human uninhabited (Leveringhaus, 2016, p. 49) – weapons, like aerial vehicles (U.A.Vs.) and robots, has triggered a lively and ongoing global debate among scholars of war-ethics. At the very epicentre of this debate lie the so-called responsibility gaps introduced via the use of autonomous weapons (A.Ws.) lacking moral agency, or according to Sparrow, 'the prospect of intelligent actors without moral responsibility' (Sparrow, 2007, p. 74). Within this context, on the one side of the spectrum, there is a school of thought that is highly critical and eventually dismissive of A.Ws., evangelising that 'unless or until the responsibility question can be resolved, there must be a presumptive prohibition against the deployment of armed autonomous weapons', (Enemark, 2014, p. 108). On the opposite side of the spectrum lies Ronald Arkin, who considers his 'ethical robotic warfighter', (Arkin, 2009), as the manifestation of the early first steps 'towards the construction of an autonomous robotic system architecture capable of the ethical use of lethal force'.

In between the two previous polar-opposite approaches, Alex Leveringhaus, (Leveringhaus, 2016, p. 123) takes 'the middle path in dealing with the conceptual issues in the debate on autonomous weapons', by adopting a risk-based approach to complement the existing three principles of jus in bello, meaning distinction, proportionality and necessity (Walzer, 1977).

The present article is an effort to underline the dire need for a coherent ethical framework that on the one hand would evolve beyond the wholesale dismissal of A.Ws. due to responsibility gaps and 'the insidious danger of moral hazards', (Scharre, 2018, p. 263), while at the same time, it will avoid the pitfall of shrinking ethics into science, (Schwarz, 2018, p. 294), via the adoption of a technological answer to a nagging philosophical question.

Autonomous versus Unmanned versus Human-Uninhabited

At this point, a clear line of distinction has to be drawn among autonomous, unmanned and human-uninhabited weapons. A drone is a characteristic case.

People frequently use the term 'unmanned drone' and at the same time imply autonomy. This is not necessarily right. Drones are always human-uninhabited but not necessarily unmanned. This is because there is usually a human operator, who can be either 'on the loop' - able to intervene on a need-to basis – or 'in the loop', meaning actively flying the drone. Only in the case of an absolute human absence can a drone be fully autonomous and at the same time unmanned. The analysis that comes immediately below refers to fully autonomous weapons – unmanned drones included.

Useful disambiguation: Cognitive Systems and Artificial/Machine Agents

A system can be characterised cognitive if it has the ability to 'perceive' its environment and translate it into awareness. If the system is fully autonomous – meaning with human operators out of the loop – then it may also act autonomously on the received information. This is a typical case of machine/artificial agency, which is a sub-group to the family of cognitive systems. More specifically, artificial agents are systems that not only receive information from their surroundings, but they can also act on it. As such, they have the ability to establish interaction of sorts with their environment.

Literature Review

At present, war-ethics are codified in the United Nations Charter of 1945 (Charter of the United Nations, 1945), the Geneva Conventions of 12 August 1949 (International Committee of the Red Cross, 1949) for the protection of war victims (civilians, prisoners of war, e.t.c.) and the two additional protocols that were adopted in 1977 (International Committee of the Red Cross, 1977). The scholarship epitomised in the above three documents has served humanity in the aftermath of the 2nd world war and a series of regional ones, like for instance in Vietnam and the first Gulf War. However, particularly in the years since 9/11, war as humanity has known it for millennia, has been changing mainly through the weaponization of disruptive innovation. The introduction of autonomous weapons has laid bare the inadequacy of the existing legal and particularly the ethical framework underpinning armed conflict. In this vein, Lloyd Axworthy and Walter Dorn elaborate on the urgent need to have an updated humanitarian law in face of all the latest developments in military technology (Axworthy and Dorn, 2016). Fairly recently, Walzer also elaborated on targeted killings using drones and the collapsing equilibrium between the ease of launching an attack and the substantially reduced military risks and political costs on calling the same attack (Walzer, 2016).

Rodin researched the new ethics in the emerging landscape of warfare and 'experienced serious difficulties in interpreting and applying standard judgements of just war theory' (Rodin, 2006, p. 153), whenever the condition of reciprocity was put to test due to the asymmetry of warfare. He believed that when at war, reciprocity should take precedence over the three principles of jus in bello, meaning necessity, discrimination and proportionality. This approach has been based on the view of war as a contest (Enemark, 2014, p. 65) and the proposition that remote control killing – for instance using drones – heaps doubt on traditional sociological and ethical notions of what it means to be a combatant or 'warrior' within the military profession (Enemark, 2014, , p. 77). Similarly to Walzer and Rodin, Kahn postulates that 'riskless warfare may take the destructive power of war outside of the boundaries of [democratic] legitimacy…' (Kahn, 2002). This is also consistent with the view expressed by Singer who elaborates on the removal of risk and its impact on drone operators (Singer, 2009). Taking it a step further, Martin van Creveld doubts the very nature of war fought with machines, believing that 'war does not begin when some people kill others: instead it starts at the point where they themselves risk being killed in return' (van Creveld via Singer, 2009, p. 432). In this vein, but years ahead of the current global debate on autonomous weapons and the ethics that attach to them, Luttwak coined and analysed the term 'post heroic-war' (Luttwark, 1995) and likewise, Pepperell elaborated on the concept of 'post-human war' (Pepperell, 1995).

Zeroing in more on the ethical challenges emanating from the use of A.Ws., the notion of the so-called responsibility gap has put the scholarly debate on steroids – at times blurring the line between science and philosophy. The definition of a responsibility gap was given by Matthias as 'a class of machine actions, where the traditional ways of responsibility ascription are not compatible with our sense of justice and the moral framework of society, because nobody has enough control over the machine's actions to be able to assume the responsibility for them' (Matthias, 2004, p. 175). Similarly, Horowitz was one of those who elaborated on the issue of human (non-)responsibility whenever 'smart machines take over from human soldiers on the battlefield' (Horowitz, 2016). Peter Asaro warned against weapons' autonomy, because of the likelihood of an accidental war. He believed that autonomous weapons may get close to, but they will never achieve Kantian moral agency (Asaro, 2008).

The gist of the debate about responsibility gaps lies in the nagging question of who will be responsible in a case of malfunction of a smart weapon, which as such, causes unjustified death and destruction. Broadly speaking, the international scholarship is split in two schools of thought, with each one offering its own answers. It is at this point that the author of the present proposal believes that there is a gap in the existing knowledge, which could be further researched and as such be the springboard for a doctoral project.

More specifically, on the one side of the spectrum, Sparrow sets the pace believing 'it is a necessary condition for fighting a just war, under the principle of just in bellum, that someone can be justly held responsible for deaths that occur in the course of the war. As this condition cannot be met in relation to deaths caused by an autonomous weapon system it would be therefore unethical to deploy such systems in warfare' (Sparrow, 2007, p. 62). Evidently, he rejects altogether the use of A.Ws. as unethical, on the grounds of the accompanying responsibility gap.

Similarly, Enemark believes that although drone technology makes violence easier and less risky, it does not count as moral permission. He is also clear that '[…] the moral case for introducing mechanical warriors in war depends, first, on their improving the conduct of war from a jus in bello perspective. Second, justice in war requires the responsibility for any misconduct that does occur can be fairly attributed and punishment meted out accordingly' and 'unless or until the responsibility question can be resolved, there must be a presumptive prohibition against the deployment of armed autonomous drones' (Enemark, 2014, p. 102).

Likewise, Scharre cites Bonnie Docherty, a lecturer at Harvard Law School, raising concerns that 'autonomous weapons could create an accountability gap' which would 'disallow for retributive justice for victims or their families and for deterring future actions', (Docherty via Scharre, 2018, pp. 261-2).

The Human Rights Watch (H.R.W, 2015) elaborates on the potential accountability of a fully autonomous weapon. It draws a line of distinction between personal, criminal and civil liability and comes to the conclusion that gaps in accountability are inevitable as the use of autonomous weapons becomes progressively broader and more pervasive. The H.R.W. report elaborates on the twin legal concepts of actus reus and mens rea within the context of weapons' autonomy and highlights the obvious collapse of mens rea in the case of a crime perpetrated by a machine. The report also develops a more hands-on approach to situations faced by commanding officers in the line of fire and investigates the so-called causal responsibility in the use of an autonomous weapon. It delves into the concepts of direct and indirect responsibility – or command responsibility. Eventually, it produces evidence to support the argument that the widespread use of autonomous weapons will represent a step backward for international criminal law.

In the same vein, but assuming a slightly different approach, the International Committee of the Red Cross in its latest report of April 2018 (International Committee of the Red Cross, 2018) argues in favour of the retention of human agency in decisions to use force and against autonomous weapons. The main arguments against machine agency are the lack of moral responsibility, the lack of accountability and the preservation of human dignity. For the ICRC 'the fundamental question at the heart of the ethical discussion is whether, irrespective of compliance with international law, the principles of humanity and the dictates of public conscience can allow human decision-making on the use of force to be effectively substituted with computer-controlled processes…'.

Assuming a more technical approach, Neil Davidson believes that 'as all of the obligations under international law, legal obligations and accountability for them cannot be transferred to a machine…', (Davidson, 2018). He also argues in favour of the I.H.L. principles of distinction, proportionality and unnecessary suffering in attack. He gives as main reasons for the rejection of autonomous weapons the lack of both predictability and reliability. In sum, the type and degree of human control over and autonomous weapon should be based on the robust verification of technical performance, the manipulation of operational parameters and the ability for humans to intervene should the need arise.

On the opposite side of the spectrum lies a less populated school of thought, which tries to fill the responsibility gaps using technology. The chief-apostle of this school of thought is Ronald Arkin who sets his mark with the goal 'to provide robots with an ethical code that has been already established by humanity as encoded in the Laws of War and the Rules of Engagement' (Arkin, 2009). According to Enemark, 'this is a project to engineer a robot warrior, or an ethical governor component, without human frailties and possessing ethically superior warfighting abilities…' (Enemark, 2014, p. 110).

Schwarz believes that this is a 'strategic fallacy: an attempt to eliminate all and every possible danger using a mode of technologically informed warfare that by necessity produces ever-new categories of risk and danger…' (Schwarz, 2018, p. 190). As such, it is also a manifestation of the 'phenomenon of automation bias that occurs in decision-making, because humans have a tendency to disregard or not search for contradictory information in light of a computer-generated solution that is accepted as correct' (Miller via Schwarz, 2018, p. 290).

Last but not least, Alex Leveringhaus chooses to take the 'middle path' and tries to bridge the gap between ethicists and technologists by introducing the element of risk in the debate about A.Ws.. He believes that 'the role of risk in warfare has not been discussed in much detail by those working on the ethics of war' and he proposes the introduction of a fourth principle of 'reasonable risk' to complement the existing three of jus in bello, meaning distinction proportionality and necessity (Leveringhaus, 2016, p. 121).

Framing new Research via the Identification of Gaps in the existing Scholarship

As elaborated in the previous section of Literature Review, the debate on the responsibility gaps introduced via the use of A.Ws. has been almost – with the exception of Alex Leveringhaus – monopolised by two schools of thoughts. On the one side of the argument, the Ethicists, represented mainly by Sparrow and Enemark, dismiss smart weapons altogether on the grounds of the inability for Kantian attribution whenever machines replace humans as moral agents. On the other side, the Technologists, represented by Arkin, have until now responded to the quandary with the injection of more technology.

If one though takes a step back and above, he will easily come to realise that this is not the first time in human history that techno-pessimism comes to the fore. 'Concerns that humanity has taken a technological wrong turn, or that particular technologies might be doing more harm than good, have arisen before' (Economist, 2019). In an only slightly different twist, Strawser believes that remotely controlled weapons are 'merely an extension of a long historical trajectory of removing a warrior ever father from his foe for the warrior's better protection'. In his view the 'fair fight' threshold was crossed long ago (Strawser, 2010, p. 343).

Upon identification of similar quandaries, the winning recipe traveling throughout history has been that if technological shortcomings are to be successfully addressed, this can only happen via more technology. Such a historical fact would undeniably place Arkin and his roboticised 'moral governor' ahead of the Ethicists. However, there is a problem with such a line of thinking. This has been clearly framed by Schwarz writing that 'moral reasoning that relies on analytic abstractions and technologically streamlined understandings of war, does not have the capacity to address those morally significant factors that fall beyond the domain of what can be ascertained numerically'. Put simply, technology cannot contain ethics because 'the idea of ethics as science is highly contested' (Schwarz, 2018, p. 294). Such an approach would give Sparrow and Enemark precedence over the Technologists. However, if there is one thing that both sides agree is that A.Ws. are here to stay. The progressively 'post-human' nature of war, manifested via the use of autonomous weapons, is a clear and present ground-reality and it is becoming more prevalent as time goes by. As such, it demands a proper ethical footing that until now has proven to be elusive.

Schwarz believes that 'if we want to rethink ethics, we ought to consider it in the context of politics' and in the same vein, 'both the ethical and the political are descriptions of the context in which we find ourselves; compelling and irreconcilable obligations can and do happen in a forceful way, without foundations. Understood as an action, ethics becomes much more closely tied with politics as action and the two share essential aspects' (Madeleine Fagan via Schwarz, 2018, p. 198).

The Aim of Research in the field of Ethics of Autonomous Weapons and Potential Methodology

The aim of such a research should be to develop a new ethical framework – within a political context – that would be able to address convincingly the current lack of 'ethical underpinnings of a fully technologized conception of warfare and armed interventions' (Schwarz, 2018, p. 201). Such research could push the barriers of knowledge and as an additional benefit, it could also bridge the gap between Ethicists and Technologists.

The main research problematic should be, whether ethics can evolve past the responsibility gaps, to support a fully technologized conception of warfare and armed interventions.

This could be done by leveraging ethnographic methods to identify what Martin calls 'UPOs' or 'Unidentified Political Objects' (objets politiques non-identifiés) (Martin, 2002). These are political relations and political sites that are generally unseen, or unidentified by political scientists (Joudre, 2009, p. 201). However, whereas a mainstream scientific method goes cheek-by-jowl with a clean research hypothesis, which is developed ahead of the analysis of evidence, this is not the case with ethnography. In the latter case, the researcher incessantly asks 'why', while groping in the dark among otherwise bewildering, unimaginable, or seemingly irrational practices. This is the process that Clifford describes as 'making the familiar strange, the exotic quotidian' (Clifford, 1986). For this reason, new research should skip at the early stage the formulation of a solid research hypothesis. Unlike the proverbial drunk who searches in vain for his keys only in the light of the streetlamp, the researcher should aim to move the barriers of knowledge and shed ethnographic light beyond what is currently illuminated (Schatz, 2009, p. 305).

Potential Sources of Knowledge and further Thoughts on the Research Methodology

The research in ethics of autonomous weapons would have unavoidably to tap into the knowledge (both tacit and explicit), as well as the views and the mindsets of professionals who are directly involved in the development and subsequent use of autonomous weapons. These professionals are expected to be familiar with the ethical challenges posed by the responsibility gaps. This is a direct hint to:

- Information technology scientists and technologists, who develop the various platforms of artificial intelligence / machine learning underpinning the function of A.I. weapons;
- Executives of firms / industrial manufacturers of A.I. weapons;
- Politicians tasked with the approval – or not – of A.I. weapons in military operations;
- Senior military officers and field operators of A.I. weapons;

These are the so called 'professional elites' that McDowell defines as 'highly skilled, professionally competent and class specific' (McDowell, 1998, p. 2135). Parry uses the term 'hybrid elites', because the critical knowledge sought for instance in the present research, does not exist in traditional institutions 'but rather within increasingly informal, hybridised, spatially fragmented and hence largely invisible networks of elite actors', (Parry, 1998, p. 2148).

It is becoming evident that the proposed research would require a high degree of 'participant observation or immersion in the field' of ethics of A.I. weapons, as defined by Aronoff (Schatz, 2009, p. xi). Even more, with the stated aim 'to develop a new ethical framework within a political context', the research methodology to be adopted would have to 'peel the onion skin of reality – to get closer to its essence' (Grass, 2007) and to hold out the 'the promise of epistemological innovation' by 'challenging existing, often hegemonic, categories of practice and analysis' (Schatz, 2009, pp. 11, 15).

In this vein, researchers view ethnography 'not just a tool that social scientists interested in meaning-making processes can use to study public opinion, but actually as a mainstay of current political practice' (Cramer Walsh, 2009, p. 171). As such, the proposed research should be conducted by someone who 'is enough of a participant who has access to the people he wishes to study and is allowed to remain in the setting in which they meet, while he is mainly an observer' (Cramer Walsh, 2009, p. 178).

On the issue of data collection and analysis, a structured and well regimented ethnographic approach, would introduce a research protocol similar with the one suggested by Beamer (2002, p. 1994) for interview coding and analysis.

Epilogue

Weapons featuring various degrees of autonomy have been for too long a ground reality in the military field, and as such they have given rise to ethical considerations that cannot be moped under the carpet anymore. The existing framework of international law that governs warfare worldwide, although entrenched, cannot cope with the wave of disruptive innovation that progressively permeates the military field. The need for a coherent new set of ethical rules and regulations that will both come to terms with new reality and at the same time bring some order in a developing chaotic landscape is now more than ever direly needed.

References

Books

Arkin R. (2009). 'Governing Lethal Behavior in Autonomous Robots'. Chapman-Hall (Taylor & Francis), New York

Clifford J. and George E. M., (eds. 1986). 'Writing Culture: The Poetics and Politics of Ethnography'. University of California Press, Berkeley

Cramer Walsh K. 'Scholars as Citizens: Studying Public Opinion through Ethnography' via Schwatz E. (2009). 'Political Ethnography : What Immersion Contributes to the Study of Power'. University of Chicago Press, Chicago, pp. 171, 178

Enemark C. (2014). 'Armed Drones and the Ethics of War. Military Virtue in a post-heroic age'. Routledge, Oxfordshire and New York, p. 62, 65, 77, 102, 108, 110, 113

Grass G. (2007). 'Peeling the Onion'. Random House, London

Joudre C. 'The Ethnographic Sensibility: Overlooked Authoritarian Dynamics and Islamic Ambivalences in West Africa' via Schwatz E. (2009). 'Political Ethnography : What Immersion Contributes to the Study of Power'. University of Chicago Press, Chicago, p. 201

Leveringhaus A. (2016). 'Ethics and Autonomous Weapons'. Palgrave Macmillan, London, p. 9, 49, pp. 121-122

Martin, D.C. (2002). 'A la recherche des OPNI'. Karthala, Paris

Pepperell R (1995). 'The Post-Human Condition', Exeter: Intellect, p.1

Rodin D., (2006). 'The Ethics of asymmetric Warfare'. In Richard Sorabji and David Rodin (eds), 'The Ethics of War: Shared Problems in Different Traditions'. Aldershot: Ashgate, 2006, p. 153

Scharre P. (2018). ‘Army of None’. W.W. Norton & Company, New York, p. 251, pp. 261-2

Schwarz E. (2018). ‘Death Machines’. Manchester University Press, Manchester, p. 120, 165, 182, 190, 198, 201

Schwatz E. (2009). ‘Political Ethnography : What Immersion Contributes to the Study of Power’. University of Chicago Press, Chicago, pp. xi, 11, 305

Singer P. W. (2009). ‘Wired for war’: The Robotics Revolution and Conflict in the Twenty-First Century’. Penguin, New York, p. 432

Von Clausewitz C. (1873). ‘On War’. Enhanced Media Publishing, New York, 2017

Walzer M. (1977). ‘Just and Unjust Wars: A Moral Argument with Historical Illustrations’. 5th Edition, Basic Books, New York, 2015

Essays / Articles

Arkin R., (2009). ‘Ethical Robots in Warfare’. Technology and Society Magazine, IEEE. 28. 30 - 33. 10.1109/ MTS.2009.931858, accessed via t.ly/r8MlX

Axworthy L. and Dorn A.W., (2016). ‘New Technology for Peace & Protection: Expanding the R2P Toolbox’. American Academy of Arts and Sciences, Journal Dædalus (Ethics, Technology & War), MIT Press, Cambridge, MA, 2016, accessed via https://goo.gl/PXiLRV

Asaro P. (2008). ‘How just could a robot war be?’, accessed via https://is.gd/Koyhdy

Beamer G. (2002). ‘Elite Interviews and State Politics Research’: p. 94, accessed via t.ly/nZYw8

Davidson N., (2018). ‘A legal perspective: Autonomous Weapon Systems under International Humanitarian Law’. accessed via https://is.gd/reQGMf

Economist, (2019). ‘Pessimism v progress’, published online on the 21st December 2019, p. 13, accessed via t.ly/v8dxp

Horowitz M. C., (2016). ‘The Ethics & Morality of Robotic Warfare: Assessing the Debate over Autonomous Weapons’. American Academy of Arts and Sciences, Journal Dædalus (Ethics, Technology & War), MIT Press, Cambridge, MA, 2016, accessed via https://goo.gl/PXiLRV

Kahn P. (2002). ‘The Paradox of Riskless Warfare’, Philosophy and Public Policy Quarterly 22, no 3, 2-8, p. 4

Luttwak E.N. (1995). ‘Toward Post-Heroic Warfare’, Foreign Affaires 74, no. 3, 109-22, p. 115

Matthias A. (2004). ‘The responsibility gap: Ascribing responsibility for the actions of learning automata’, Ethics Information Technology 6, p. 175, accessed via t.ly/GrRnX

McDowell L. (1998). ‘Elites in the city of London: some methodological considerations. Environment and Planning A 30’: p. 2135, accessed via t.ly/7R9K2

Parry B. (1998). ‘Hunting the gene-hunters: the role of hybrid networks, status, and chance in conceptualising and accessing corporate elites. Environment and Planning A 30’: p. 2148, accessed via t.ly/xZgpq

Sparrow R. (2007). ‘Killer Robots’, Journal of Applied Philosophy, 24(1), pp 62-67, p. 74

Schwarz E. (2018). ‘Technology and Moral Vacuums in just war theorising’, Journal of International Political Theory, 14(3), pp. 280-298, p. 290, 294

Strawser B. (2010). ‘Moral Predators: The Duty to Employ Uninhabited Aerial Vehicles’, Journal of Military Ethics 9, no. 4, 342-68, p. 343

Walzer M., (2016). ‘Just & Unjust Targeted Killing & Drone Warfare’. American Academy of Arts and Sciences, Journal Dædalus (Ethics, Technology & War), MIT Press, Cambridge, MA, 2016, accessed via https://goo.gl/PXiLRV

George Kiourktsoglou obtained his B.Sc. in Mechanical Engineering in 1992 from the Aristotelian Technical University in Greece. As an intern, he worked for the Israeli Public Corporation of Electricity. Having concluded his military service he went to the U.S.A. to study Nuclear Engineering at Cornell University. From the latter he graduated in 1996 with an M.Sc.. From 1996 until 2009 he worked for Royal Dutch Shell both in Greece and the Far East. Sponsored by Shell, he graduated in 2006 from Alba in Athens with a Diploma in Management and two years later with an M.B.A. in Shipping. George is a fellow of the British Higher Education Academy and a member of the American Nuclear Society, the Chartered Management Institute and the Institute of Marine Engineering, Science and Technology in London. He speaks Greek, English, German, Japanese and French.

Unmanned Aerial Vehicles (UAVs) : The modern day "technicals"

by Evangrelos Mantas
& Constantinos Patsakis

This is a part of The Sky is Falling Down: Unmanned Aerial Vehicles as Emerging & Disruptive Technology Threat Assessment, research presented at 14th NATO Operations Research and Analysis Conference.

INTRODUCTION

"The more the world changes, the more it stays the same". As technology moves forward day by day, more challenges on the battlefield rise as well and new more sophisticated systems appear. The constant in this change is always the same: Gain tactical advantage over the adversary. A few years ago, advanced weapon systems were only available on a handful of military organisations. Today guerrilla or radical forces have access to market products that with a few modifications can prove quite efficient and equalize the advantage gap. Commercially available drones have been the platform of choice due to the tactical advantage they provide, their relatively low cost and flexibility to change the payload of the drone (e.g. cameras, weapons, sensors) depending on the mission. Hence the term "modern-day technicals", a term[1] that goes back to the Somali civil conflict in the early 1990s where armed pick-up trucks relied on their speed and agility to launch assaults against enemy combatants, giving the rebel forces a tactical advantage by simply modifying already existing. Modern-day armies already operate Medium-Altitude Long-Endurance[2] (MALE) drones (e.g. MQ-9 Reaper[3]), and High-Altitude, Long-Endurance (HALE) drones (e.g. RQ-4 Global Hawk[4]) that inarguably offer a tactical superiority on the operational field.

Nonetheless, nowadays conflicts may take place in urban areas where warfare logistics are far more complex, take advantage of Small Unmanned Aerial Vehicles (sUAV) that can be easily and quickly deployed by guerilla/insurgents fighters and counter the technological superiority in the open battlefield through asymmetric capabilities[5] in this restricted battlespace. Those sUAV's operate ISR (Intelligence, surveillance and reconnaissance) or strike missions and pose a new threat for the ground troops safety and operational success.

Over the past few years, the Islamic State (ISIS) developed its own drone program without any financial aid from a state actor, modifying already existing off-the-shelf commercial drones or making makeshift flying machines, providing detailed instructions and recommendations using social media to spread them online[6] widely. Those drones have been modified to carry and deliver explosives to targets acting like flying Improvised Explosive Devices (IEDs). Since the beginning of the conflicts, the Islamic State fighters have increased their combat capabilities and experience in conducting drone missions and use social media to release propaganda material associated with the drone program. An International Center for the Study of Violent Extremism (ICSVE) research[7] related to ISIS' drone activities within its territories in Syria, reveals that ISIS drone operations started during mid-January 2017 having established a training centre for the militants by March 2017 in the city of Raqqa. A modification and maintenance headquarters for drones and other digital equipment was set to a nearby location where the weaponization of drones took place

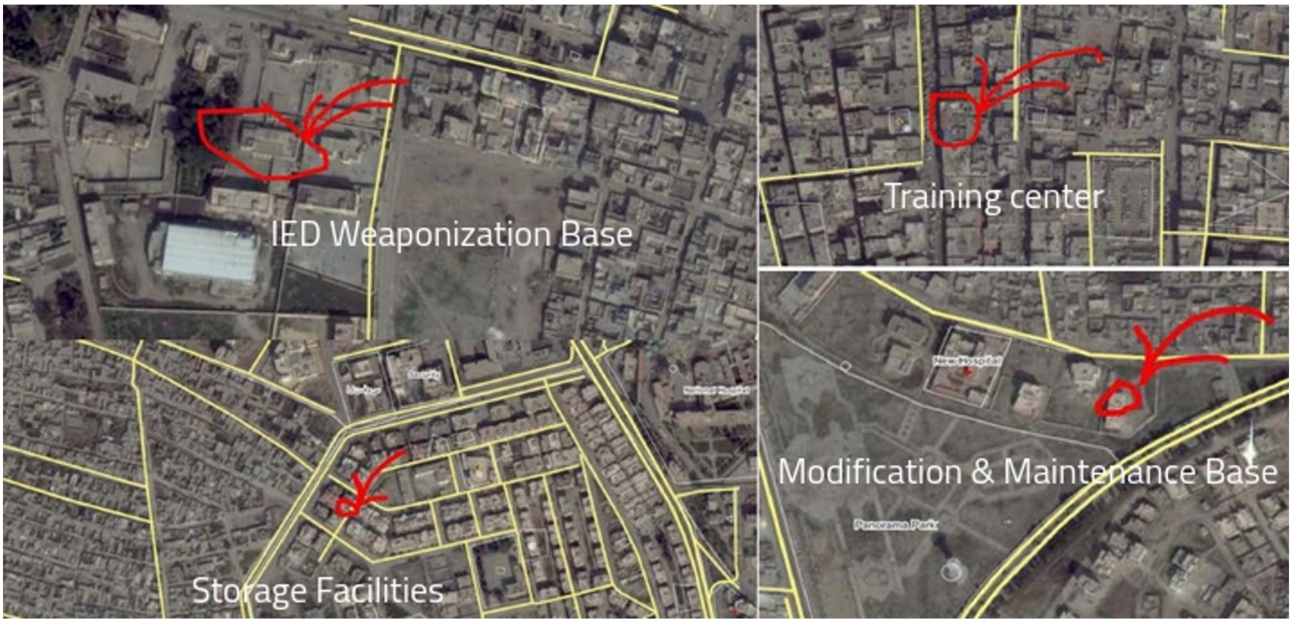


Image : ISIS drone weaponization logistics centers in Raqqa, circa 2017 (Image sources: Almohammad, Asaad & Speckhard, Anne. (2017). ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics. ICSVE Research Reports.)

and later shipped them to a storage and distribution centre. Evidently, an adversary with a fully working logistics supply chain of weaponized drones is an immediate threat that endangers personnel, vehicles, infrastructure and the success of an operation.

THREAT IDENTIFICATION

To this extent civilian and military ships are exposed to this threat.In this section, we identify the threats that UAVs pose against vessels and naval bases, used as an attack vector in accordance with their operation.

Intelligence, Surveillance and Reconnaissance (ISR)

Intelligence is arguably one of the most critical components on the modern-day battlefield. Real-time information on the vessel's location ,either docked either sailing, can provide the adversary with a tactical advantage. Drones equipped with high-resolution cameras can identify the number of personnel on board, existing attack capabilities and defence countermeasures or onboard equipment and provide this information for a later attack using drones or other conventional strike methods (e.g. artillery/airstrike). Since a small drone can fly relatively quietly and fast, it is hard for the vessel's defence counter measures to detect it and therefore neutralize it.

Drone Bombing

The technological advancement of drone technology has enhanced the operational capabilities of drones to carry a significant amount of payload from a range of sensors to explosive ordnance. For this reason, drones have emerged as a complex threat that is getting harder and harder to neutralise. Terrorist organisations give extensive publicity to its use of armed drones, in a way that is probably meant as a demonstration for their tactical capabilities[8] over the bigger and more sophisticated western drones. Over the last few years, numerous incidents have been reported of suicide drones used from rogue groups. On May 2009, four ships, including three oil tankers, were damaged in mysterious "sabotage attacks" carried out by drones[9]. Naval bases are no exception whether they are located in conflict zones or in the domestic urban area of peacetime countries where the consequences of a drone attack on the personnel and the military logistics cycle would be dire. Armed drones could replace mortar installations due to their precision and effectiveness to deliver a hit against crew members and vessels. The threat of explosive-carrying drones is equal or even more severe to IEDs since the combination of IEDs and UAVs could be considered a significant evolution in offensive actions. A threat simulation study by NATO's CIED CoE in 2017[10] on the possible usage of drones from malicious actors accentuates the threat drones pose carrying a wide variety of ordnance from mortar shells to directional fragmentation charge, to name a few, and the impact of asymmetric and hybrid warfare scenarios on a fictitious simulated urban environment. and their protection against these asymmetric and unexpected attacks seems more important than ever.

Electronic Warfare

Hostile actors may conduct "activities in cyberspace to cause harm by compromising communication, information, or other electronic systems, or the information that is stored, processed, or transmitted in these systems[11]" as described in Framework for Future Alliance Operations Manual. The lack of understanding of the ramifications of EW can have critical mission impact – even in the simplest possible scenario. A man-in-the-middle cyber-attack monitoring the communications or the control of autonomous systems can prove dire. Drones carrying electronic warfare ordnance can disrupt operational capabilities rendering communication systems useless endangering the safety of the crew, the ship and the operation's success. Although there are no reported cases of sUAV with such capabilities so far, with the current technological advancement, soon it may be the case. Nevertheless, vehicles and aircraft with EW capabilities already exist, but they are harder to be utilised by terrorist groups since their cost of operation and maintenance is significant, and they require extensive training, but their threat should not be ignored.

INTERDICTION AND MITIGATION PLAN

After identifying the attack vectors using a drone, it becomes of main importance to interdict this threat. A proposed interdiction plan at a higher level consists of the following three steps:

UAV Detection Technology

Initially, to anticipate and eliminate the threat, enemy combatant drones must be identified. There are different methods to identify a drone with mixed results depending on the technology used, the environmental conditions and the technological advancement of the adversary drone. Often multiple sensors and devices will be integrated into a single system to provide higher detection success rates (e.g cameras, machine vision classification algorithms, and acoustic sensors).

UAV Identification Technology

As more drones are expected to occupy the airspace it is important to make a distinction between friendly and hostile drones. It would be catastrophic to cause damage or take out a friendly drone that serves a mission in the nearby area. Aircrafts and medium/long-endurance drones (MALE/HALE) already use a system known as Automatic Dependent Surveillance-Broadcast (ADS-B) which periodically transmits the aircraft position. Such technology could also be applied for small UAVs (sUAV). Although it is probable that malicious actors will fly their drones without such technology enabled, drone identification technology could prevent the wrongful targeting and elimination of friendly drones.

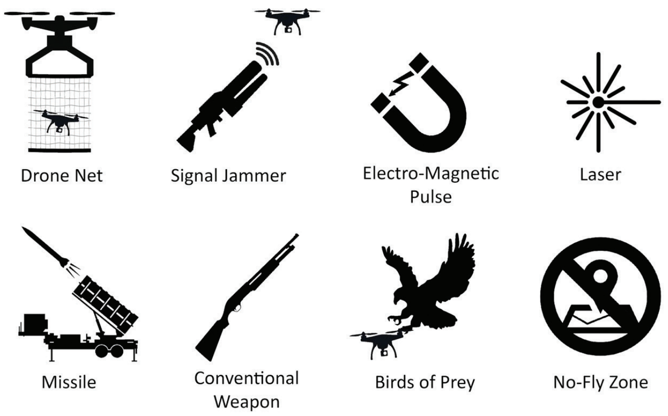


Figure: Indicative list of available Interdiction/CUAV capabilities

Counter-UAV Capabilities

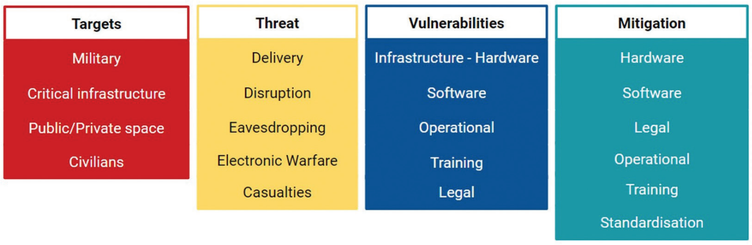
From ancient times till today, protection of military assets has been of main concern. Walls, outposts and armed guards may be the solution to conventional warfare, the use of drones to launch asymmetric attacks requires a new approach. Different types of Counter UAV (CUAV) measures are already available to provide a solution to this arising threat with “at least 235 counter-drone products either on the market or under active development[12]” exploiting a variety of techniques for detecting and/or intercepting drones. Since the available space on a vessel is limited, more compact solutions should be taken into consideration. It should also be noted that already existing solutions like the C-RAM have been upgraded to enhance their capabilities and neutralize drones as well. Below are presented some of the already existing CUAV technologies

EVALUATION PLAN

To properly assess the malicious drone impact, a proposed purple teaming evaluation scenario could take place, where the defence countermeasures will be tested to prove their effectiveness. Simply put, Red Team members will act as malicious actors using drones to emulate an attack against military assets. Simultaneously, the blue team is monitoring its systems, however, they cooperate to find measures that may improve the control or defeat the bypass. The aspects of the proposed evaluation plan contain a Threat Emulation, Operational Impact, and Threat Mitigation.

Threat Emulation

The purpose of the Threat Emulation is to challenge the full scope of the defences countermeasures described in the previous section, so that when an if a real attack the assets stay protected and the risk of failure in the military operation minimises. In the sector, Threat Identification, we identified the threats drones pose as an attack vector and those will determine the rules of engagement for the evaluation scenario. An example of this could be the following: “A drone equipped with a camera locates areas of importance in an allied naval base. After the drone unsuccessful elimination, a mortar strike hits the base, resulting in damages against infrastructure vessels and seaman casualties”. This scenario aims to determine the success of the countermeasures of the base.



Targets	Threat	Vulnerabilities	Mitigation
Military	Delivery	Infrastructure - Hardware	Hardware
Critical infrastructure	Disruption	Software	Software
Public/Private space	Eavesdropping	Operational	Legal
Civilians	Electronic Warfare	Training	Operational
	Casualties	Legal	Training
			Standardisation

Figure: Threat assessment chart

Operational Impact

By definition, the operational impact is the effect of the disaster on an organisation’s operation that determines the survival and continuity of the operation. The quantification of realistic impacts against a selected target, as described in the previous example may be variable, from loss of human life to financial damages due to the destruction of assets.

CONCLUSIONS & OPEN ISSUES

As drones are expected to be widely used by adversaries to launch asymmetric and hybrid attacks, the importance to successfully interdict this emerging threat is becoming more imminent than ever. Nonetheless, there are many obstacles beyond the infrastructure solutions. For instance, the current legal framework has to be revised and amended to determine the fly zones for civilian drones and the jurisdiction clauses. Evidently, despite the need to monitor critical infrastructures which may span for kilometers (e.g. road infrastructure) it is not possible for the military in terms of resources to monitor the whole infrastructure and more over may not fall under its jurisdiction leading to many unnecessary problems in case it is deemed necessary to intervene. Beyond that, it should be understood that the operational framework, even for military personnel is not always well-defined since this is closely related to the training of the personnel. The latter is very important when personnel notices the presence of a drone in an area. Can they identify whether it is an ally or hostile? Due to the time criticality, who should be informed and how the personnel should act against it? Evidently, the answers do not have a simple yes/no form as the identification, contrary to face-to-face interactions are not so simple. Even if the above are tackled a standardisation of procedures and the drones per se is needed.

Evangelos Mantas is currently employed as DevSecOps Engineer, having obtained a degree in Computer Science at University of Piraeus. His security research covers multiple aspects of drone operations and is the author of GRYPHON: Drone Forensics in Dataflash and Telemetry Logs, research published on 14th International Workshop on Security 2019 in Tokyo. He served in the Hellenic Army Special Forces as Sergeant and contributed to the development of General Upper Staff of Hellenic Army cyber-exercise “Panoptis 2019”. He is a peer instructor in University of Piraeus Cyber Security Team hoping to aspire a new generation of cyber security experts.

Constantinos Patsakis holds a B.Sc. in Mathematics from the University of Athens, Greece and an M.Sc. in Information Security from Royal Holloway, University of London. He obtained his PhD in Cryptography and Malware from the Department of Informatics of the University of Piraeus. His main areas of research include cryptography, security, privacy, data anonymization and data mining. He has authored more than 100 publications in peer reviewed international conferences and journals. He has participated in several national and European R&D projects. Additionally, he has worked as a researcher at the UNESCO Chair in Data Privacy and as a research fellow at Trinity College.Currently, he is an Assistant Professor at the University of Piraeus and adjunct researcher of Athena Research and Innovation Center.

REFERENCES

[1] https://www.geopolitica.info/technicals/

[2] https://defensesystems.com/articles/2015/05/27/uas-male-vs-hale-debate.aspx

[3] https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104470/mq-9-reaper/

[4] https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104516/rq-4-global-hawk/

[5] Khan, Umer. (2018). Urban Warfare.

[6] https://justpaste.it/jnabi7

[7] Almohammad, Asaad & Speckhard, Anne. (2017). ISIS Drones: Evolution, Leadership, Bases, Operations and Logistics. ICSVE Research Reports.

[8] Emil Archambault, Yannick Veilleux-Lepage, Drone imagery in Islamic State propaganda: flying like a state, International Affairs, Volume 96, Issue 4, July 2020, Pages 955–973.

[9] https://finanz.dk/iran-used-underwater-drones-in-tanker-attacks-insurer-claims/

[10] CIED CoE,(2017) C-UAV payload with IED. A LONG TERM SIMULATION BASED STUDY, North Atlantic Treaty Organization (NATO)

[11] ACT,(2018) FRAMEWORK FOR FUTURE ALLIANCE OPERATIONS, North Atlantic Treaty Organization (NATO)

[12] Holland Michel, Arthur. “Counter-Drone Systems.” Center for the Study of the Drone at Bard

COMMANDERS AND STAFF HANDBOOK FOR C-IED REVIEW AND WRITING SESSION

Following the decisions of the 22nd C-IED Working Group, NMIOTC with the cooperation of the C-IED COE hosted the 2nd Commanders and Staff Handbook for C-IED Review and Writing Session.

The objectives of the workshop were to review the Handbook and provide an updated version to the C-IED WG.

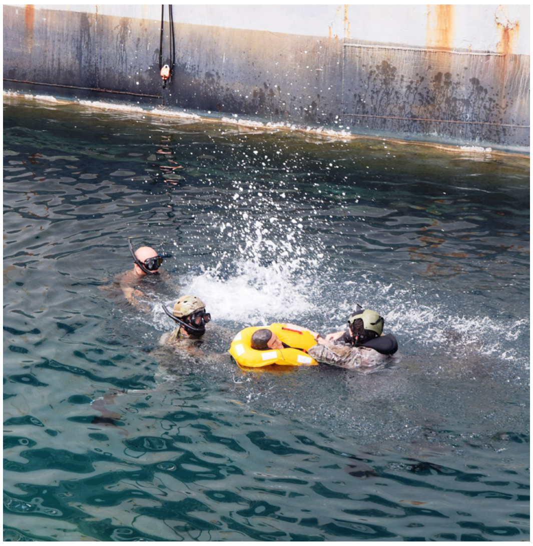
Six (6) representatives from five (5) countries (Greece, The Netherlands, Slovakia, Spain and The United Kingdom) participated in the Writing Session.

Course 21000
(Medical Combat Care In Maritime Operations)

Resident Course 21000 “Medical Combat Care in Maritime Operations” was conducted at NMIOTC’s premises from 14th to 25th September 2020.

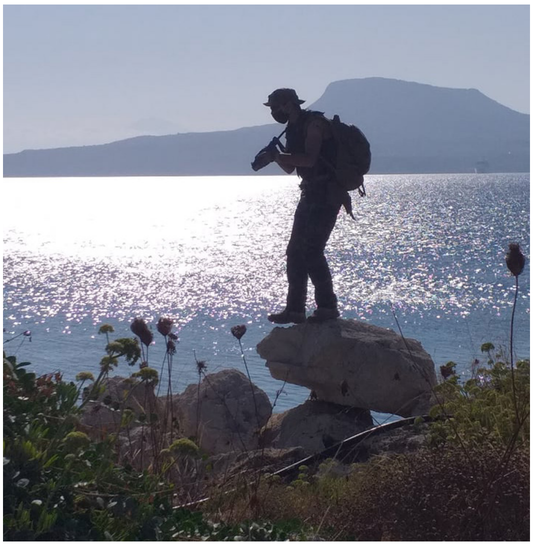
The goal of this course was to transfer knowledge and enhance trainees’ skills so as to provide combat medical care from the point of injury in the mission/theatre until the final transfer to the closest Medical Treatment Facility.

Twelve (12) participants from three (3) Countries attended the course (Greece, Japan and USA). Training was delivered from Subject Matter Experts (SME’s) certified as National Association of Emergency Medical Technicians (NAEMT) instructors and other augmenters specialized in Stress Management, telemedicine and HAZMAT. In addition, an assigned Medical Director was closely monitoring all medical interventions performed throughout the Course in absolute coherence with NAEMT’s policies, and regulations.



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

From 14th to 25th of September 2020, the Resident Course 8000 "C-IED Considerations in Maritime Force Protection (MFP)" was conducted at NMIOTC premises. The objective of the course is to address the existing and emerging C-IED threats, focusing on those faced by vessels when operating in confined and shallow waters as well as in non-friendly ports. In total, eleven (11) trainees from six (6) countries (France, Germany, Greece, Morocco, Tunisia and the United Arab Emirates) attended the course. Lectures and practical drills were delivered by NMIOTC Sea Trainers and Instructors in cooperation with augmenters from the UK and the Hellenic Army.



11th NMIOTC ANNUAL CONFERENCE 2020

The 11th NMIOTC Annual Conference took place on 29th September 2020 at NMIOTC premises Titled "Interagency and Whole of Society Solutions to Maritime Security Challenges". It was attended by 135 participants from 20 Allied and Partner Nations, International Organizations the international academic community, representatives from the shipping and IT industry.

Among the keynote speakers was the Commandant of the U.S. Coast Guard Admiral Karl L. Schultz and the Deputy Chief Of the Hellenic National Defense General Staff (HNDGS) Vice Admiral Ioannis Drymousis HN.

This year due to the current COVID-19 pandemic situation and in absolute coherence with standing World Health Organization (WHO) guidelines, further to the physical conference, a virtual conference has been delivered simultaneously.

The aim of the conference was to discuss issues and share perceptions of the international community on how to improve interagency, cooperation and collaboration on the field of maritime security and forward proposals and solutions for countering the maritime security challenges.

4th CYBER SECURITY CONFERENCE IN MARITIME DOMAIN

From 30th September to 1st October 2020, the 4th Conference on “Cyber Security in Maritime Domain” was held at NMIOTC, attended by 170 participants from Allied and Partner Nations, International Organizations the international academic community, representatives from the shipping and IT industry.

This year due to the current COVID-19 pandemic situation and in absolute coherence with standing World Health Organization (WHO) guidelines, further to the physical conference, a virtual conference has been delivered simultaneously.

The aim of the conference was to encourage participation and promotion of collaborative scientific, industrial, naval, maritime and academic inter-workings among individual researchers, practitioners, navy staffs, members of existing associations, academia, shipping companies, standardization bodies, including government departments, international organizations and agencies, public and private sector in general, regarding cyber security in maritime domain and cyber defense operations.

NMIOTC Course 1000 “Command Team Issues”

Course 1000 “Command Team MIO Issues” was delivered from 5 to 9 October 2020 by NMIOTC’s instructors.

The objective of the course is to assist Staff Officers and Naval Units’ Command Teams in the efficient application of NATO common standards in the planning and execution of Maritime Interdiction Operations (MIO).

The course was attended and successfully completed by a total of eleven (11) trainees, coming from five (5) countries (Brazil, Bulgaria, Greece, Montenegro, Romania) .

NMIOTC Course 2000 "Boarding Team Classroom Issues" & NMIOTC Course 3000 "Boarding Team Practical Issues"

NMIOTC courses "2000" and "3000" were delivered at NMIOTC's premises from 5 to 16 October 2020 by NMIOTC's instructors.

Course "2000" provided the theoretical training to Boarding Teams' personnel to better plan and conduct boarding operations.

Course "3000" which followed focused on the associated practical training for safe and effective Maritime Interdiction Operations.

In total, seven (7) trainees from four (4) countries (Jordan, Montenegro, Poland and Portugal) attended both courses

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

Train-the-Trainers Technical Instructors" Course was conducted in a blended form due to COVID 19 pandemic restrictions. Advanced Distribution Learning was delivered from 12 to 16 October virtually and from 19 to 23 October 2020 the training was conducted at NMIOTC premises

The aim of the course aim was to provide a comprehensive training package to the trainees in the field of acquiring the overall general familiarity in transmitting and certifying pedagogical knowledge and enhancing their presentation and speaking skills. Course 17000 is considered of a great value in the light of maintaining / improving quality of deliverable training thus raising the level of educational standards.

NMIOTC in absolute coherence with SACT's Quality Assurance Unconditional Accreditation award follows an Academic Staff Development Program. This program includes NMIOTC's instructors participation to Course 17000 after every rotation of military personnel as a matter of professional development and to ensure that NMIOTC instructors possess the knowledge and skills required to be involved effectively to the learning/teaching process.

Fourteen (14) trainees (8 military, 6 civilians) from Germany, Greece Romania and Turkey, participated in the course.

NMIOTC Course 14000 “Maritime IED Disposal (M-IEDD)”

NMIOTC conducted Resident Course 14000 “Maritime IED Disposal (M-IEDD)” from 19 to 23 October 2020.
The aim of this course was to educate and train EOD personnel to competently undertake IEDD Operations on-board vessels and other maritime infrastructure in support of C-IED and relevant operations. The training covers the subject concepts, philosophy and principles, equipment, ship insertion and maritime focused on IEDD methodologies, and best practices in the maritime environment.
In total, sixteen (16) trainees from five (5) countries (Belgium, Greece, Netherlands, Qatar and United Arab Emirates) attended the course. Training was delivered with the participation of Subject Matter Experts (SMEs) from the United Kingdom, in cooperation with NMIOTC Sea Trainers.

NMIOTC “Family” Photo

On Wednesday 18th of November 2020, NMIOTC personnel gathered for the traditional annual “family” photo.

Visit of USA Assistant Naval Attache to Greece, Captain Rose Rice
July 31, 2020

1st Steering Committee Meeting (SCM) IAMD CoE
September 9-11, 2020

Visit of the Honorable R. Clarke Cooper, Assistant Secretary Bureau of Political-Military Affairs of the USA October 16, 2020

Visit of IAMD CoE October 22, 2020

TCCC Training of Hellenic Police
July 6-8, 2020

Training of GRC SOF Team
July 6-10, 2020

Small Arms raining of 547 Airborne Battalion in CUTA
July 15-17, 2020

Training of HS LIMNOS Boarding Team
July 27-29, 2020

Training of Hellenic Underwater Demolition Team in CUTA
September 7-11, 2020

Training of Hellenic UDT on training platform ARIS
September 21-25, 2020

Container Inspection Training of Estonian Border Police
September 28 - October 9, 2020

Crew Control Training of HMS DRAGON Boarding Team
September 29, 2020

NATO OTAN
IED Defeat – Maritime Application
21
Capabilities:
- Awareness at all levels
- Search as an enabler
- Exploitation (Tac site/WIT/Levels 2/3)
- Information dissemination
- Engagement e.g. Law Enforcement
Way Forward:
- Concept of operations
- Doctrinal change

NMIOTC Course 12000,
"C-IED in Maritime Interdiction Operations"
October 12-16, 2020

Training of HS NIKIFOROS Boarding Team
October 26-27, 2020

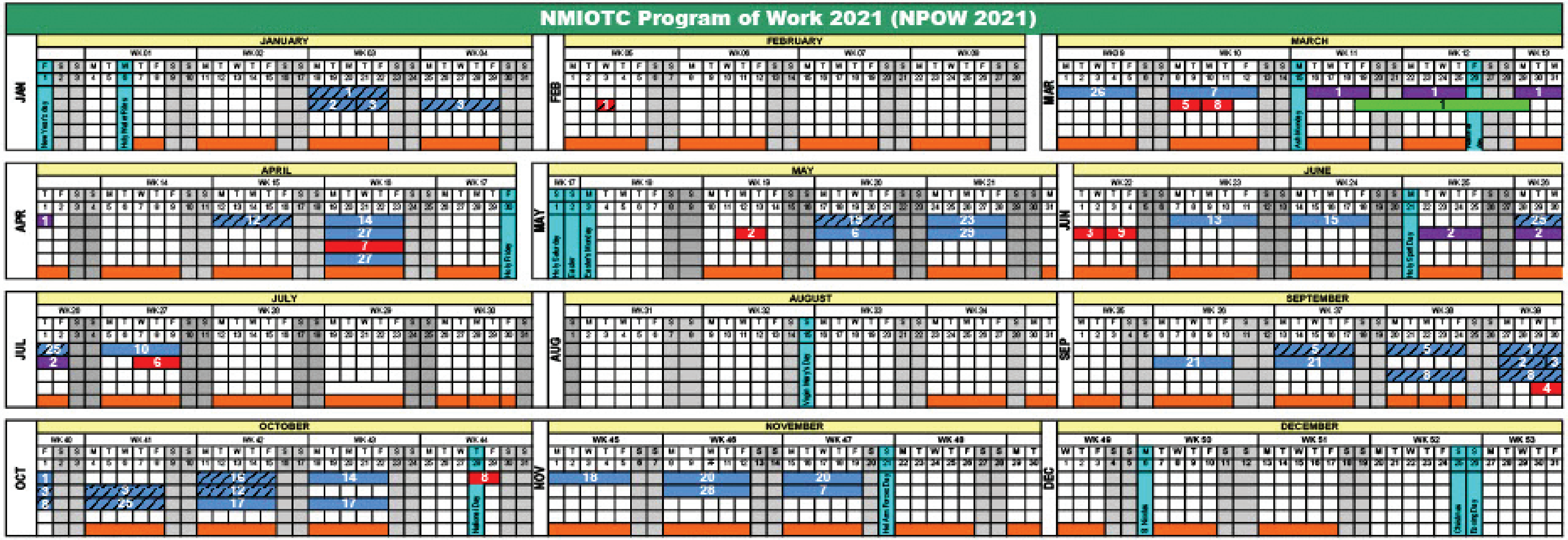
NMIOTC Course 12000,
"Maritime Interdiction Operations in Support of Managing Perilous Security Incidents on Coastal Critical Sites MIO MPSI CCS"
November 2-13, 2020

GRC SOF Team Training
November 2-5, 2020

Rethimno Police TCCC Training
December 7-9, 2020

Small Arms Training of Lithuanian Boarding Team
December 7-21, 2020

NMIOTC Program of Work 2021 (NPOW 2021)



COURSES (ETOC ID.)

1 Course 1000 - Command Team MIO Issues (MOP-MO-31201)
2 Course 2000 - Boarding Team Theoritical Issues (MOP-MO-21203)
3 Course 3000 - Boarding Team Practical Issues (MOP-MO-31205)
4 Course 4000 - MIO Final Tactical Exercise (MOP-MO-31207) (Upon Request)
5 Course 5000 - Maritime Operational Terminology Course (MOP-MO-21208)
6 Course 6000 - Weapons of Mass Destruction in MIO (WMD-MD-31209)
7 Course 7000 - MIO in support of Counter Piracy Ops (MOP-MO-31210)
8 Course 8000 - C-IED Considerations in Maritime Force Protection (IED-ED-31679)
9 Course 9000 - Legal Issues in MIO (LGL-LE-31613)
10 Course 10000 - MIO in Support of Countering Illicit Trafficking at Sea (MOP-MO-32012)
11 Course 11000 - AVPD Course (MOP-MO-32011)
12 Course 12000 - C-IED in Maritime Interdiction Operations (IED-ED-31904)
13 Course 13000 - Command Team Issues in MIO in support of International Efforts to Manage the Migrant and Refugee Crisis at Sea (MOP-MO-22015)

14 Course 14000 - Maritime IED Disposal (IED-ED-32008)
15 Course 15000 - Migrant Handling Team Issues in MIO in support of International Efforts to Manage the Migrant and Refugee Crisis at Sea

16 Course 16000 -Maritime Aspects of Joint Operations (MOP-MO-22078)
17 Course 17000 - Train the Trainers Technical Instructor (ETE-IT-34432)
18 Course 18000 - Maritime Biometrics Collection and Tactical Forensic Site Exploitation (MOP-MO-22373)
19 Course 19000 - Cyber Security Aspects within Maritime Operations (COP-CD-22104)
20 Course 20000 - MIO in Support of Managing Perilous Security Incidents on Coastal Critical Sites (MOP-MO-35613)
21 Course 21000 - Medical Combat Care in Maritime Operations (MED-MS-34411)
23 Course 23000 - WIT Supplement in the Maritime Environment (IED-ED-35437) (Pilot)
24 Course 24000 - Hybrid Warfare in the Maritime Domain (Under Development)
25 Course 25000 - Drafting, Production and Maintenance of NATO Standards (ETE-IT-35477)
26 Course 26000 - Tactical Combat Casualty Care (TCCC) / Combat Life Sver (CLS) in MIO (MED-MS-35547)
27 Course 27000 - Maritime Sniper Course (SOF-SO-35603)
28 Course 28000 - Radiological Search in Maritime Environment (WMD-CD-35614)
29 Course 29000 - Detection and Identification of WMD (CBRN Materials) in MIO (WMD-MD-35660)

ACTIVITIES

1 NAB (NMIOTC)
2 NCB (HNGS)
3 NMIOTC Annual Conference
4 Cyber Security Conference
5 NATO Nuclear Policy Symposium (NPS)
6 E-MED Security Conference
7 Annual Medical Discipline Conference / MMT WG
8 OSG in Brief
9 Gender Perpectives in Maritime Security: Women in Peace, Crises and War

EXERCISES / METTs

1 CCE / MTT

TAILORED TRAININGS

1 USMC 24 MEU
2 USMC Force Recon DFT
3 DETRA (US)

► Updated 4 November 2020

🟦 Training Courses 🟪 Tailored Trainings ▨ NATO Events 🟩 Exercise / MTTs 🟩 Trial Courses 🟥 Conference - Meeting 🟨 Unit Training 🟦 National Holidays 🟧 Available Period for Training 🟪 Evaluation of Courses / Maintenance

NMIOTC
Souda Bay 732 00 Chania
Crete, GREECE

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

Webpage: www.nmiotc.nato.int

Hellenic Army Printing Office