International Association of Maritime Security Professionals

29 February 2024
Volume 2, Issue 1

Wavefront

Professional Certificate in Maritime Security (PCMS)

Our first candidate is now into the final project, the equivalent of the capstone effort from the PCMS. We'd like to offer our congratulations for passing through the three eight-week courses in exceptional fashion.

As we review the feedback from the first candidate, we will be making some adjustments for the next cadre of participants. This is expected to kick off with the PCMS-0001 course (Maritime Infrastructure and Operations) the beginning of April.

The PCMS represents a truly unique offering and those passing through it will possess a much broader understanding of maritime security across several domains. With academic courses that range from Cyber Security to the Use of the Oceans in Conflict, candidates are exposed to a much broader set of viewpoints.

Our key adjustments to the program since its inception include an increased update cycle and the inclusion of "office hours." Instead of annual updates for each IAMSP course, the course will be updated when the current cadre completes the course and submits their feedback. Remaining current and relevant in this rapidly-changing industry is important to us and how we deliver value to those taking the time and making the effort within the program.

The second element involves the office hours. While many online courses allow for limited email-based interaction with the instructors, the determination was made to offer candidates the opportunity for face to face communications for approximately 2 hours per week. For those that have taken "normal" university courses, this is somewhat akin to being in the lecture hall for those courses.

Inside this issue

Special points of interest

- Our first group of candidates is now entering the final IAMSP set of courses.
- It is now apparent to many that it is not just our infrastructure that needs to change, but also how we manage and oversee that infrastructure that needs to evolve.

Cyber Security in the Maritime Sector

The recent announcement that President Biden has signed an Executive Order to formalize cyber security across USA seaports poses both opportunities and challenges.

While the USCG has an authority that spans both ports and ships, one might hope that the port's cyber security requirements will be able to dovetail well into those put forward for the shipping industry, including the potential impacts associated with the positions taken by the International Association of Classification Societies (IACS).

Those involved in this space should watch the rule-making process closely in the USA, particularly where close trading relationships exist with USA ports.

The announcement can be found on the White House press page.

Blindly applying "best practices" may open organizations to risks given the changing threat, operating, and other environments.

Other Implications

We continue to see examples of the rush towards functionality without clear evidence of due diligence in many projects.

While time to market is important, this rush towards functionality at the expense of the other non-functional requirements (including safety and security) simply avoids the issue of risk and leaves that gap festering into the future.

There is a need for regulatory bodies, including the Engineering Colleges, to step up to this challenge and to remind those certified or recognized individuals involved in these processes that such practices may run afoul of their professional responsibilities and may actually put them at risk with respect tot their credentials.

A changing battlespace—unconventional forces and proxy warfare.

Continued on Page 6…

Recent attacks on commercial shipping in the Red Sea and Gulf of Aden illustrate how modern conflict requires an adjustment in thinking about the capabilities on warships. Four major elements drive this thinking.

First, we see the use of non-state actors creating significant challenges for commercial shipping not just from sea, but also from land. The use of anti-ship ballistic missiles, drones (including one underwater drone), and other weapons from shore create a challenge for commercial ships.

In the 2009-2011 piracy campaigns within the region, attacks presented limited challenges. Skiffs or other small craft were used to carry the attacking pirates towards the ship and then boarding efforts were made. Making the argument of self-defence offered very few challenges. Once the attacking pirate forces had fired upon the ship from the skiff, using an escalation of force to the point that stopped that attack was pretty straight forward.

Attacking from within Yemen offers a complication. While the commercial ship still has the right to self defence, ensuring that force is applied appropriately and judiciously is likely not possible. Frankly put, the commercial ships do not have the hardware necessary to enter into that kind of engagement.

The debate also differs in that the nations of the world, through their naval forces, are charged with the safety and security of the shipping lanes. Operations to clear attacking forces and their infrastructure fall clearly into this role.

A Pivotal Moment in Naval Technology?

Continued on Page 7

Aircraft carriers, considered to be one of the mightier tools in a navy's arsenal, have been described as floating cities. While this many be overstated, a population of around 5000 sailors and air personnel can certainly be described as a reasonable-sized town. Are we, however, seeing a shift away from these kinds of capital ships?

This question comes from three sets of events or conditions.

The first involves the success of Ukrainian forces in using drones against Russian ships. The attack on the Russian missile corvette Ivanovets showed the relatively imbalance in terms of how small and relatively inexpensive weapons could be used to neutralize significant naval assets.

The second involves a similar challenge faced in the Red Sea as Houthi rebels use drones, including at least one underwater drone, as part of their campaign to attack ships in the region. While naval forces have shown themselves to be capable of defending themselves and commercial shipping, the cost imbalance continues to raise eyebrows.

Finally, there are considerations of what naval forces of the future will look like. Factors influencing these include the need for a greater number of highly capable ships, recruitment challenges for various navies, and the need to stay at sea for extended periods of time.

On "Competition"

Nation states will invariably compete at various levels. They may be limited to trade-related issues or discussions about policy at one level but can escalate to full-scale warfare on the other. It is naïve to think that because many feel that warfare is to be avoided that it is still not possible.

In fact, we need to come to grips with the fact that warfare and the upper end of intensity in conflict is becoming much more complex. Nation states may understand that the impacts of going to full-scale war don't make sense from a cost-benefit analysis but may take other steps to achieve their aims.

We see this illustrated two ways when we look at China and Iran.

China has taken a "whole of society" approach with respect to how it projects its interests. This means that competition may have diplomatic, military, economic, social, and other ramifications.

Iran on the other hand has chosen to use a set of proxies to project its interests. Instead of declaring war and going face-to-face, it has established this network to insulate itself from some of the ramifications.

These are currently grey areas that will need to be addressed in our thinking if we are going to remain relevant and capable of dealing with the modern environment.

Professionalization?

When we look at the concept of a profession or evolving maritime security from a practice to a profession, it is not a small task.

If the security industry writ large or the maritime security industry wants to aspire towards becoming a profession, it will need to address certain key elements. These are the following:

- Our starting point for education.
- Appropriate and unbiased accreditation.
- The requirement to develop both knowledge and skills.
- Certification achieved through credible and consistent examination.
- Is licensing necessary? Does the licensing body have both the authority but also the capability to administer it.
- The need to maintain professional development.
- Active participation in professional associations and societies.
- Adherence to a code of ethics.

Professionalization is a term often used in the context of "getting paid." While that may be true at one level, the goals of the International Association of Maritime Security Professionals is to work along the journey described above.

Fisheries Management and Maritime Security

The recent announcement that the elver fishery will be closed due to violence, threats and widespread unauthorized harvesting speaks to a flawed understanding of enforcement.

Stating that there was not enough time….to implement enhanced access for Indigenous communities, a new regulatory framework , … and a suite of operational changes to the management of the fishery rings hollow.

The problem here is that this approach fails to address two key aspects of the problem. The first involves the presence of buyers that are essentially willing to buy from anyone. These markets are generally Asian in nature and largely concentrated in China.

The second problem is that criminals seeking to make money are not going to be deterred by great pronouncements of closure outside of Ottawa. The criminal element that intimidated both fishers and property owners as they committed their crimes will simply carry on their misdeed and then sell to those buyers who are not particular about where they get their supply from.

The loss of the legitimate fishery essentially clears the field for illegal activity. While some might argue that any activity in a closed fishery would be considered questionable, detecting this kind of activity will be that much more difficult without the legitimate activity that can pick up on it.

What this exposes, however, is a system that cannot keep pace with the realities of the environment it is operating in.

This includes having some meaningful discussions with all parties involved so that we don't see the same chaos as the 2023 season and the abuses that occurred.

Understanding a view of Netukulimk

The elver fishery may offer an opportunity to demonstrate how this can be applied in a modern fisheries context. The first aspect of the elver fishery is that it is lucrative with the going rate being nearly $5000 /kg.

One of the underpinning concepts is having an innate awareness of the impact that you are having on the environment and the various entities within it. The second aspect of this understanding is only taking what is needed.

This is really the root of the matter—the difference between what is needed and what is wanted. Where commercial entities (on both sides of the debate) focus on profit and reward, then we skew our activity towards what is wanted. To make matters more challenging, there is no limit to what is wanted—it will always be more.

The answer may lie in the second recommendation in the Implementation of the Mi'kmaw and Maliseet Treaty Right to Fish in Pursuit of a Moderate Livelihood. If we work from the premise that the fishery is a finite resource (as we have learned through bitter example in several fisheries), then we can at least agree that there will need to be some limits on the total number of fish taken. This will, bluntly, affect some people's opportunities and rights.

Step 1 would be the establishment of a Council that binds all activities (commercial and Indigenous — no exceptions) on the water and adheres to the Netukulimk concept. It can be supported by scientific inquiries that help describe the health of the fish stocks and the like.

Step 2 may be to actually identify the total amount that can be removed from the fishery. Essentially this is a "fish first approach" that recognizes that if we go above this number, then we risk depleting the resources entirely.

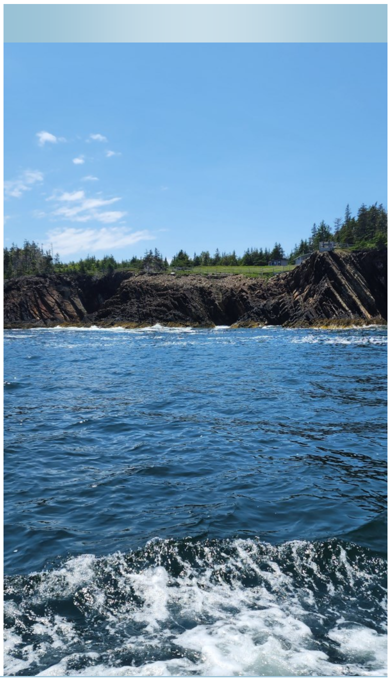
Step 3 would be to return to the concept of "necessaries" versus "wants." That is a discussion that needs to be had between all parties involved. As long as people put "rights" and "commercial" first, however, the argument will likely resolve itself when the fisheries collapse.

Managing Infrastructure Issues

Key announcements over the past two months have focused on how communities can fight coastal erosion. These have ranged from additional studies on how erosion is proceeding to how the state of Maine (USA) is looking at work that seeks to make its coastal infrastructure more resilient. The differences in these approaches warrants some exposure.

Maine's decisions with respect to infrastructure resilience focus on reducing the red tape associated with building better infrastructure where infrastructure is damaged or destroyed in coastal events. This measure, however, focuses on placing some distance between the infrastructure and the water level, such as building higher wharfs.

This approach essentially buys time but does not actually address the issue of coastal erosion. It simply attempts to place the infrastructure out of reach. For this reason, it is considered more of an interim measure that will last until conditions again force another change.



The reality is that climate change has passed a number of points and we are not going to have to focus on how to build resiliently to carry us through.

First, we need to be clear that there is not one magic silver bullet that is going to work in all scenarios.

Coastal erosion can be looked at in terms of a few different factors. First, and most obviously, there is the wave action on the shoreline that carries away material either directly or by undermining it to the point that it collapses.

Second, we also have to look at the issue of ground and bank stability. This is where manmade factors have contributed significantly to the issue. The removal of the natural stabilization (plants, trees, etc.) to clear spaces essentially removes some of the material that stabilizes the bank.

Combine this with inland drainage issues. Where water is directed to "run over" the bank and down the bank, erosion occurs. This is exacerbated by surfaces that fail to allow for natural absorption and instead divert the water.

The approach here might involve layers of activity. That begin offshore but then proceed up the bank. For example, aquatic plants and wetlands may help dissipate wave activity. Where the waves do impact the shore, this may involve moderate measures like grasses to prevent erosion but may involve heavier methods like armouring the coastline using stone.

The use of stone walls, however, should not be the only solution. Stabilization behind the stone wall needs to occur (trees, shrubs, etc.).) to reduce risks of over saturation or similar kinds of items.

What this speaks to is a need to declare a certain distance back from the shore to be a protected space where limited construction or interference (other than restorative) occurs. It also needs to be clear, however, that coastal erosion, to an extent, is a natural process and we need to figure out how to reestablish that balance point between ocean and land.

Changing Battlespace

Continued from Page 2

The second instance can be inferred from the recent use of a cyber attack against an Iranian spy ship.

While the opening of the cyber domain has certainly been discussed in various circles, the key difference here is that the use of cyber resources to disrupt a capability is now in the mainstream. There have certainly been cyber operations in the past on all sides, but they have largely been at the fringe of public discussion.

This also raises two salient points for those looking at the cyber security of commercial ships. First, with ships being increasingly connected to the internet and with internet-enabling services now being widely available, we can no longer trust the "air gap" between ships and shore.

Second, we cannot assume that bad actors will simply leave commercial shipping be. The Houthi rebels have already demonstrated a willingness to drag commercial shipping into the picture.

In brief, commercial shipping companies should be looking at cyber security in the same context as other threats to maritime safety (think interference with safety-critical system). The litany of excuses as to why companies should not have to exercise due diligence in this respect should be ended (forcefully) through very clear unified requirements (i.e., you don't sail if you aren't taking reasonable steps) and other regulatory means.

Our third element comes from an investigation that stems from the revelation that a North Korean missile fired against Ukraine contained a large number of parts linked to USA and European companies. The revelation here lies in how we look at the various sanction regimes that are considered to be an economic tool-of-choice.

What does this have to do with the maritime space? It speaks to the fact that we cannot assume that the sanctions are wholly effective. It also speaks to the need to look at how we are enforcing those sanctions across the whole spectrum — intelligence to enforcement operations.

Our final revelation comes from how non-state actors are contributing to a largely geopolitical situation. Houthi rebels have been widely reported as offering safe passage through the Red Sea to Chinese and Russian ships.

Often overlooked in western media is that a central Asian security body has been formed with Russia and China being key members. Iran has had long-standing ties with Russia (well over ten years) but has now taken steps to becoming a permanent member of that organization.

The Shanghai Cooperation Organization has recently celebrated its 20th anniversary. Western observers should note that when reading the various activities of the SCO, the "promotion of a new democratic, fair, and rational international political and economic international order" appears as one of the four main goals.

In brief, there is a significantly capable organization (that even includes one NATO member—Turkey) that seeks to rebalance the geopolitical landscape.

This brings us to our final challenge, the blurring of state and non-state actors when it comes to conflict. One of the worst kept secrets in this scenario involves Iran's involvement behind the scenes in terms of coordination and support. The use of the Iranian spy ship to assist in intelligence and gathering to support Houthi activities only strengthens the case that there are state actors operating in the background.

For the navies of the world, this means that the traditional approach of navy-on-navy will need to be augmented to include these non-traditional vectors. Failing to consider the use of apparently civilian assets (such as seen in the South China Seas) and even non-state actors (Houthis and other groups) have become the mainstream of conflict.

Changing Face of Naval Conflict

Continued from Page 3

Drones and a New Imbalance?

Part of the solution appears to be an increased interest in Degree 3 Maritime Autonomous Surface Ships (or MASS). Degree 3 ships are essentially remotely controlled vessels that do not have seafarers on board. As a result, they have no need for galleys, exercise spaces, crew quarters, or the like.

This is a new trend that may want to be looked at in Canada, where recruiting for the Navy has been challenging, despite many merits in the profession. Sydney Harbour (Australia) recently saw four USN vessels of this type said into the harbour. While Unmanned Surface Vessel Division One may be relatively new , reports are that the USN have indicated that they can see nearly 40% of their fleet being uncrewed by the middle of the 21st century.

With the increased attention being paid to MASS Degree 3 ships, we need to be very cognizant that good engineering will be critical to successful deployment and employment.

These challenges will reside in two spaces: design and operation. On the design side, we are still in relatively unclear territory when dealing with remotely controlled vessels. Yes, the technology specific to the vessel may be becoming more understood, but there are other aspects that need to be considered when looking at how these vessels will interact with other, and more traditional forms, of shipping and recreational boating.

The second element to this involves the resilience of the ship itself. Traditional warships were relatively well-designed to survive the rigours of both the ocean and conflict, but always had the fall back position of a well-trained crew on board that could affect repairs. This will need to be rethought when looking at the design of these newer ships.

And this brings us to a challenge that is often not discussed in polite company. What does one do if hostile forces get their hands on the technology and begin to reverse engineer it?

The recent capture of the Banshee drone in the Russia—Ukraine conflict may provide some insight in terms of the time it takes to capture something, reverse engineer it, and then identify exploitable vulnerabilities in it. While militaries attempt to put off the capture of equipment so as to protect its capabilities and limitations, it should be looked at in terms of an inevitability.

In the context of expanding navies, what is the approach that should be taken?

This debate is one that is not going to be settled here but should probably be discussed amongst the senior leadership of those responsible,

Either way, we need to ask ourselves what kind of transition we are facing. Are we seeing an end to the dominance of capital ships and fleets, an adjustment that sees those assets coming later after these lower-cost threats have been cleared or something else?

In all cases, the question cannot be ignored by those operating naval vessels nor should it be ignored by those designing naval vessels. Given that these smaller craft teeter on the fulcrum of asymmetrical capabilities, we would ignore their presence and their ability to become present at our own peril.

International Association of Maritime Security Professionals

The International Association of Maritime Security Professionals ’ goal is to build capacity within the maritime security space through a combination of efforts supporting education, training, and research. Made up of a combination of academics and practitioners from across multiple domains, the Association seeks to build a trusted community, not to dominate a market but to support those within the maritime security sector.

Publication Schedule

This newsletter will be sent out every two months (February, April, June, August, October, and December) around the last business day of the month. The focus of the newsletter are those activities within the International Association of Maritime Security Professionals (IAMSP) that seek to build capacity as well as other developments outside of the Association that may serve those seeking to improve their maritime security posture, education, skills, or experience.

The publication falls under the oversight of the Chief Learning Officer for the Association.

International Association of
Maritime Security Professionals, Ltd.
Registered Office
Office 4 - 219 Kensington High Street
London W8 68D
United Kingdom

Email: clo at iamsponline.org
https:.//www.iamsponline.org

We look at 2024 as a year that will see challenges in the Maritime space.

On natural fronts, conditions are in place for a difficult storm season in many parts of the world.

We see advancements in technology that offer both opportunities but that may also lead to new risks to be mitigated.

Finally, we see an increasingly difficult geopolitical situation as the global balances of power shift and uncertainty grows.

This alone becomes more than enough reason to work towards building, establishing, and maintaining communities that are not focused on the ledger but in terms of building the capacity available within the community.