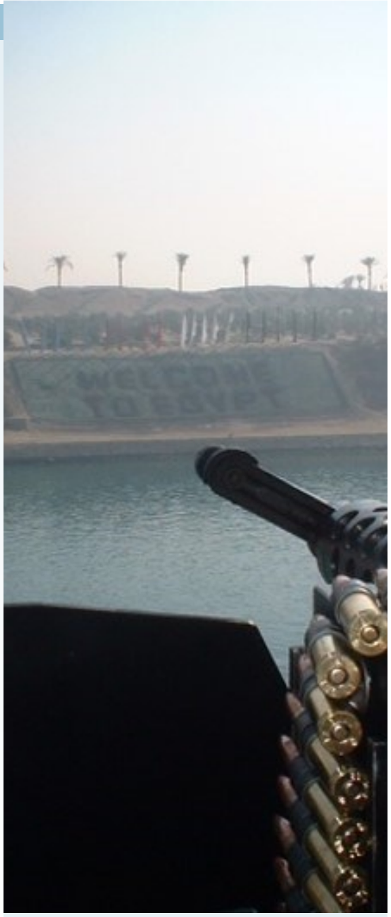
International Association of Maritime Security Professionals

30 June 2024
Volume 2, Issue 3

Wavefront



Time to Rethink Naval Strategy?

Those involved in setting naval strategy face significant challenges as part of the job, but the recent months have provided some insights into three emerging challenges.

First, the relatively asymmetric conflict in the Red Sea and Gulf of Aden continues to create challenges for both naval forces and commercial shipping, While it would be naïve to believe that the Houthi rebels are acting in isolation, the challenge of how to address their continuing threat to commercial shipping remains. This first challenge presents itself in terms of forces on land threatening strategic shipping lanes.

Second, the conflict in Ukraine has demonstrated how conventional sea power (frigates, missile carriers, etc.) can fall prey to the same challenges. The question here is not whether or not we need the equivalent of capital ships, but what the nature of close in defense on naval assets will need to look at in the near future.

Third, China presents both examples of how non-traditional maritime assets (coast guards, fishing fleets, etc.) can be used as part of a strategic master plan to seize, occupy, and attempt to control waters. The recent attack by PLAN forces on Filipino forces in the South China Seas presents some lessons in *real politik* for those that believe that we can carry on leveraging edicts and declarations by courts and entities like the United Nations.

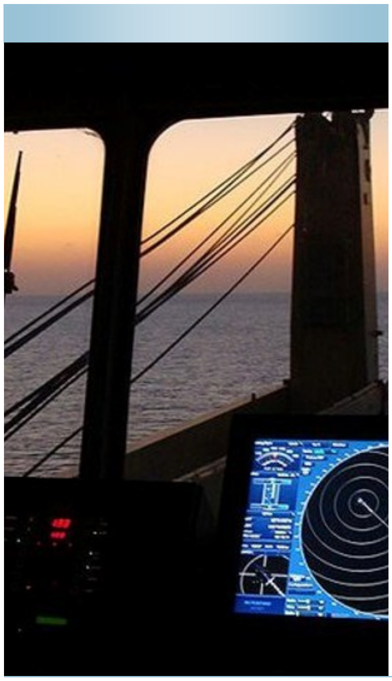
These transitions are of sufficient gravity for those involved in the design, construction, and operation of maritime assets (military and civilian) to warrant a shift in our focus to a more critical set of offerings in our newsletters.

The focus for these two months, therefore, will be on some of the events that we have seen in the maritime space and where it may be taking maritime security as an industry.

Inside this issue

Special points of interest

- We are currently wrapping up the updating phase of the CMSP courses. These are anticipated to be available beginning July 2024 as we move to the next phase of training modernization.
- Look for an announcement due to a new supporting partnership with the Canadian Maritime Industry and Shipbuilding Association in the coming weeks.



Another Commercial "Standards Body?"

Recent announcements that an organization is forming to address maritime cyber security standards raises some obvious questions.

We need to be cognizant that every national state draws upon the direction of the International Maritime Organization to set its own standards. This presents unique challenges for private sector entities of this type as it may be *an* accepted approach, but becoming *the* accepted approach may be a bridge too far.

We must also ask ourselves about the utility of another standards body. Between flag state requirements and the guidance in safety-focused organizations like the International Association of Classification Societies, do we need a body attempting to enter yet more complexity into this space?

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

Compliance vs. Security

The IT Security industry continues to focus on standards-security. This, in itself, is not necessarily a "bad" thing. Caution needs to be exercised.

First, each operation is relatively unique when balancing operations, threat environment, and organizational culture. This means that the blind application of a standard can be described as a "good fit" but will not necessarily pass the "best fit."

Second, standards are in the public domain and slavish adherence to the standard is little different than publishing your security posture.

The role of standards should be limited to defining the criteria for practicing and sound practices, not prescriptive lists that are use do simply lessen workloads.

The Drone Challenge

Continued on Page 6…

Two arenas present a wealth of information on how drones (or remotely operated vessels) can challenge traditional shipping. The first and most obvious involves the conflict in Ukraine where drone technology has not only successfully attacked Russian naval assets but has also demonstrated how quickly such technology can be brought to bear and pushed through innovation cycles. The current situation in the Red Sea and Gulf of Aden shows how non-state actors can employ this technology (even if with the help of state actors). While various weapons have been used to varying degrees of success by Houthi Rebels (ranging from missiles to drones), the events have illustrated just how susceptible to this kind of attack commercial shipping lanes can be.

Ukrainian attacks against major naval assets fall into two broad categories. The first are traditional missile attacks, often using the Neptune anti-ship missiles. This threat is not new, particularly for those that have studied the South China Sea as China maintains a capability to launch shore-based missiles against approaching naval forces as part of its defences. The second category involves the remotely-operated sea drones that have been used with significant success, including the recently revealed Stalker 5.0, Sea Baby, and the Magura 5.0, both of which are being used with some success.

The key aspect of the use of drones in this conflict, however, is not their range (which has been increasing), their increasing payloads (over 250 kg), or the fact that some can be controlled from just about anywhere with an internet connection. The key aspect to their use lies in just how quickly this technology can adapt to changes in its use and its target.

Projecting Drone Capabilities Beyond

Continued on Page 7

As we look at “sea drones” (that come very close if not overlapping in the context of Degree 3 Maritime Autonomous Surface Ships), one of the challenges that presents itself is that of range or the distance the drone can cover. Obviously, the advantage of a “kamikaze” drone is that this range can be extended out in one direction versus other assets that must return, essentially limiting the outer range of their operations without various forms of supporting services and infrastructure.

The People’s Liberation Army Navy (PLAN) of China may be giving some insight into an evolution of drone deployments. The reports of a fourth carrier-like vessel likely being a “drone carrier” for aerial drones. Currently, this is still highly speculative, but it does raise a different point when considering how navies can respond to new challenges.

Challenges for naval innovation are not few. At the start of the line are budgetary concerns where navies, like any other government activity, face challenges in balancing the costs of past activities, present operations, and development for the future. The second involves trustworthy infrastructure that can be used to facilitate innovation. Innovation bases part of its value on being able to be “first” with something to market or in some form of capability. It is not enough just to have infrastructure, that infrastructure needs to be trustworthy not to simply sell your innovations out from behind you.

Passing Competition

While nation states tend to compete, we are seeing activity that now passes the threshold of “competition” and can now be described as conflict.

On one hand, we have the rather obvious cases of Ukraine and the Gulf of Aden. There is little argument about what level the conflict is at in these regions.

The South China Sea, however, that has seen a gradual escalation culminating in a direct altercation between Chinese and Filipino forces begins to surpass this and comes dangerously close to the threshold of conflict.

What has become clear, however, is that the rule of law on the high seas is being challenged when running too close to issues of national interest. What has also become clear is that the current model for calming these situations or, if necessary, compelling parties to back down and find more peaceful means of resolving their differences, has failed.

This will herald another age of maritime naval power as nations seek to asset and maintain control over their waters. The obvious focal points for these challenges will be in disputed waters (such as much of the South China Sea) but also in the less controlled waterways such as in the Arctic.

A Portside View

Drone technology within the port environment offers some significant security benefits. Consider the port in terms of three functions: (1) the servicing (including coordination) of ships, (2) the transition point between different modes of transportation, and (3) a socio-cultural focal point.

Serving as a tool for detection and the early phases of response, the drone offers two distinct advantages.

First, the drone has the ability to remain on station longer than a person and does not suffer from fatigue-related issues. Consequently, area coverage is increased.

Second, the operator can enter any range of different situations without personal safety issues. This not only improves the operator's own personal safety but can also reduce the employer's liability with respect to taking reasonable steps to protect the operator's safety.

There are some hidden advantages to this as well. When we compare the operating environment of the drone *operator* as compared to the craft *operator*, we can see significant differences associated in the time it takes to prepare an individual to operate in certain environments and the levels of effort needed to maintain the physical and mental fitness to operate successfully in those environments. Consider that within the Canadian military, it can take from 4-5 years to become a pilot and a fraction of that time.

As a common sense point, consider a high-gravity turn. For the pilot, they may need to withstand an 8G turn, something that requires significant physical fitness, specialized equipment, and so forth. These factors do not exist for the Remotely Piloted Aircraft System (RPAS).

The appropriate utilization of drones may offer both immediate detection and response capabilities but also force sustainability opportunities.

Within the context of force sustainability, we have three major advantages that come to mind.

First, consider that one drone operator does not necessarily have to be uniquely tied to one drone. While this may be the case in some environments, in others, the drone operator could be working with what is essentially a "swarm" of drones operating in an area. With increased automation and the emerging capabilities associated with Artificial Intelligence, the use of drone swarms may offer advantages in the defensive context. While human oversight will likely be necessary given the nature of the mission (particularly since defensive port operations occur near civilian populations).

A cautionary should exist here, particularly given some of the lessons learned in the security industry. It was quickly discovered that those operating Closed Circuit Video Equipment (CCVE) systems could monitor around 8-10 monitors relatively effectively. This, however, is somewhat subjective as there are a number of "human factors" that can come into play at an individual basis.

The second option involves those tasks that take significant time when a vessel is in port. Consider tasks like anti-fouling. These tasks are necessary but cannot be described as being pleasant or easy in any sense of the word. Tasking drones with this kind of work may not just improve the trackability of the work, but may offer other advantages depending on the nature of the drones' sensor packages. For example, the drone may be able to not only perform the task, but additional sensors may be able to conduct other basic hull inspection processes and record the results. The advantage is a 24 hour capability (less maintenance time for tools, etc.) that can capture a full view of the hull as it progresses. Other surrounding drones could be used to monitor water quality as the tasks progress in order to quickly detect and contain any issues.

These kinds of capabilities already exist for pleasure craft and could easily be modified to deal with larger vessels (either through the number of drones deployed or expanding the capability of a single drone). Those questions, however, would best be answered by looking at a cost across the total lifecycle of the drone.

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.

Cybersecurity and Drones

In addressing this question, let's look at our ultimate goal—a reliable and trustworthy system. Reliability may come from aspects of the design (ranging from architecture to configuration) that includes robustness, resilience, and redundancy. Within this context, cybersecurity plays its own role. Protecting the infrastructure against different forms of attack and interference factors significantly and will become increasingly important as the criticality (impacts) of the service increases or the threat environment increases.

For those looking at the cybersecurity aspects of drones, we need to take a holistic approach. Where remote piloting is involved, the drone is of little value if the operator cannot connect to the drone. For those designing the drones, it would be useful to review cybersecurity from the perspective of each of the seven layers of the OSI model (physical, datalink, network, transport, session, presentation, and application). This will require a multidisciplinary approach that takes more than a basic understanding of Systems Engineering.

But how far should this actually go and how does an organization decide what is reasonable? While not intended for this specific purpose, the International Association of Classification Societies (IACS) Unified Requirements (UR) for electrical and electronic installations (specifically UR E 22) that has recently been modified might provide some guidance for those seeking to demonstrate that reasonable care is being taken.

When taking this approach, consider three scenarios. What is the purpose of the drone and does the drone perform any work that would intersect with potential loss of life or injury by those in proximity to the work or those that may rely on the outcome of the work? The second would involve a situation where the drone ceases to function as expected (such as no longer responding to commands). Would this situation result in a potential loss of life, injury, or damage to the environment? Finally, could the drone be misused in such a way to have the same impacts? In brief, if a drone's control was hijacked, could it be converted or used (even in an impromptu way) as a weapon to cause the same impacts?

These three different conditions can guide the categorization process. Where all three come back with it being negative, then the Category 1 guidance for quality management and testing can be used. As the impacts increase, then does the category and, as a result, the rigour expected of the quality management, supply chain, and testing regimes.

The lack of personnel on board drones or remotely operated vessels may be an advantage, but it also comes with some disadvantages if things are not reliable.

This will also depend upon how the drone is being deployed. If it is being deployed as an isolated (or standalone) piece of equipment that doesn't connect to the ship, then this categorization may be enough. But those designing the drone will need to look to ensure that the drone is not intended to be considered part of the "equipment carried on board" the vessel, at which point those involved in the design processes (particularly for cybersecurity) will need to examine IACS UR E27 for requirements for equipment carried on board vessels.

Getting this right will require some time to be spend with the drone's business leadership to correctly identify and record the various use cases associated with the technology. While it will be a business decision as to how far this exercise will go (i.e., determining what the intended markets are, etc.), it may be prudent to remember that getting it close at the start is often easier than attempting to make wholesale adjustments or corrections after the product has been designed or is being built.

Where this will factor significantly is if the drone is being intended as either civilian equipment, dual-use equipment, or military equipment. Where the drone is being considered for military or dual use functions, two additional factors may come into play.

The first involves any certifications required of the purchasing nation with respect to its supply chain security in the Defense Industrial Base (DIB). In the USA, this may involve the evolving Cybersecurity Maturity Model Certification 2.0 (largely based currently on NIST SP 800-171 Revision 2) or the emerging Canadian Program—Cyber Security Certification (that is largely expected to be on some form or interpretation of NIST SP 800-171 Revision 3).

The second involves the criteria that the military organization (such as the Department of Defense, etc.) may place on the engineering documentation. In Canada, for example, the Defense Administrative Orders and Directives (DAOD) 3033-0 now calls out a requirement for Systems Engineering in capital projects. Part of this involves the requirement for an "Assurance Case" to support the various claims.

All told, those designing this equipment may benefit from clearly understanding how it will intersect with these.

Skills Development

This question has two parts.

First, how do we “catch up” those working within the maritime industry with new technologies and situations? This is not a simple question given that there are estimated to be over 1.8 million seafarers of which about 1 million are ratings and the other 800,000 or so are officers (International Chamber of Shipping).

Part of this is identifying what the appropriate baseline training is. Certain nations are moving towards greater digitalization and automation but this is not consistently applied across all seafarers.

The challenge here is that by applying standards intended to address the most complex challenges, are we forcing those that do not have this need to carry an unnecessary burden or even limiting certain populations that may not have access to expensive training resources.

The second part involves how to adapt existing training to the new requirements for those that are entering the industry. One trend of concern is only limiting entry from maritime academies. While this may be prudent for those operating on ships, this approach fails to recognize that this approach may cause undue impacts, if not harm, in maintaining the employee base in other modes of transportation or operations.

The Drone Challenge

Continued from Page 2

Consider the rate at which drone technology can be adapted as compared to those used on major naval assets. Simply put, the rate of production for drones allows different generations to be adapted and produced much more quickly than the naval assets.

This places naval architects and other members of design teams in a challenging position. While a degree of comfort can be had in using historical data as the basis of design, this approach will result in one of two things.

First, it may place constraints on where the naval asset can actually be deployed. If it’s one thing that has been illustrated time and time again in the Ukrainian conflict, it is that a decent drone swarm can easily saturate the defences of a fairly major naval asset, cause significant damage requiring longer repairs, and offers a significant return on investment in terms of the capabilities disrupted.

Second, it will likely force changes with respect to close in defence. While some discussions seek the “silver bullet” solution to the drone problem, this is once again likely to have to involve layers of defence around the vessel that take into account the ship’s ability to identify, assess, lay guns on target, engage, and confirm the effectiveness of the engagement.

This cycle presents the cornerstone of the ship’s defence and, depending on the nature of how drones are employed (singly by stealth or in detected swarms), may drive the need for technological change in the naval assets.

Part of this key is likely to involve a concept similar to modularity where close-in systems are able to be adapted and swapped out to meet the changing environment. We do not need to change out the entire warship, just certain equipment that is carried on board it.

Modularity becomes one response to how the current warship can adapt to the challenges posed by drone forces.

Our second element involves ensuring good design behind the tools / weapons used to protect the ship. These systems do not operate in isolation and those involved in the future design of warships will need to keep a vigilant eye on the engineering processes to ensure adequate space, power, and room for weight. They will also need to ensure very good documentation and discipline so that these systems can be integrated successfully.

The second evolution is very likely to involve the interaction between combat management systems, automated defence systems, and ammunition. This ties to a challenge associated with a concept referred to as the saturation of defences and the need to prevent the sea drone from impacting the vessel.

The cycle discussed earlier describes a limitation that can be offset different ways. Increased automation and stability systems may reduce the number of times a cycle needs to be repeated before success can be declared. Automation integrated with intelligence functions may offer ships the ability to significant increase the efficiency associated with dealing with inbound drones. Finally, adapting the kind of ammunition used to deal more with successfully addressing all incoming threats in an area versus simply jumping target-to-target may offer other approaches. The specifics of these considerations, however, will be just one of many engineering-led challenges.

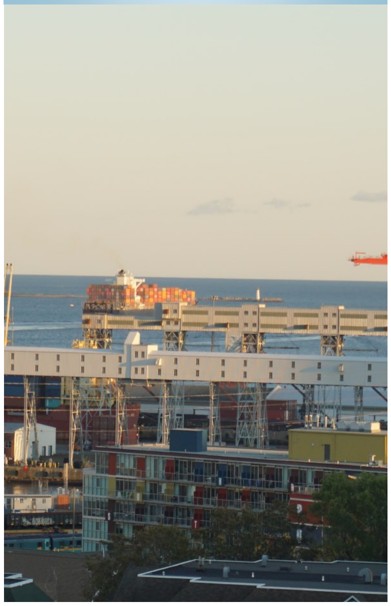
Strategically, however, the challenge lies in the rate of production and adaptability. Where major warships often take years to design and months to build, the sea drones shorten tighten down this cycle (similar to an OODA or Observe, Orient, Decide, Act Loop) significantly and leave those operating the drones with the initiative. Addressing this challenge may require those operating the major warships to look at issues like modularity, broadening the number of facilities able to handle repairs to prevent maintenance bottlenecks, and expanding their supply chains (itself not without risks) so that warships, still a necessary part of a nation’s ability to project power, remain an effective tool.

Projecting Drones Abroad

Continued from Page 3

After cost and infrastructure comes the ability to bring the right capabilities to the table to innovate. This may well be a matter of contracting and not human resources. Too often, organizations seek to engage or hire "unicorns" or those rare people that have broad, advanced, and unique combinations of education, training, and skills. Where those people can be found, they are often not cheap, may be difficult to manage, and ultimately can act as a single point of failure in the innovative capacity.

The concept illustrated in this case involves making organizations *learning* organizations. The learning organization, however, is not distinguished by the presence of a "unicorn" but more often than not being able to identify needs, relate those needs to personnel or capabilities, bringing those capabilities into teams, managing those teams effectively, then capturing their work in such a way that the team can be unformed so that resources are available for the next challenge.



At this point, aerial drones continue to be the most likely resources to be supported by their own vessels while sea-based drones, while potentially evolving into this space, will take time to overcome logistical issues.

Could this drone carrier be used to project the use of sea drones in this context? While it is possible, one might argue that it is not probable. The reasons for this can be divided into two categories: value and supply chain.

On the value front, we need to consider the dimensions of the drone. If we look to drones like the Magura 5 with dimensions of approximately 18 feet (long) and 5 feet (wide), and height of around 3 feet (given a height above the waterline of about 19 inches), we can draw a box around one drone as needing approximately 20 feet x 5 feet x 3.5 feet or approximately 350 cubic feet per unit for storage. If we look to dimensions of about 100m x 20 x 4m or some 8000 cubic meters, we have a total space of 282 517 cubic feet. Under even the most cheerfully optimistic conditions, this would only allow for some 800 drones to be stored. Those with naval design backgrounds would challenge this number immediately due to the need to move equipment, prepare the drones, and the like.

On the supply chain front, having this kind of capability makes *some* sense but the logistics for it would be quite challenging. The sea drones are not easily moved, making replenishment by sea the most likely means of "restocking" the weapons. This presents its own logistical challenge when considering the space needed and the capabilities to move them from ship to ship. The alternative would be to resupply at friendly ports.

At this point, we could argue that the aerial drone capability is likely the forward limit of this capability. While they present some of the same challenges, they offer greater operational flexibility to those employing them. The limitations may well be the number of command stations offered on board the vessel.

Where this kind of deployment makes sense is in the support to an attack, such as an amphibious assault, where the vessel can stand off some distance (such as still in international waters) and then surreptitiously launch its fleet of drones which would then be guided into ports and other waterways to disrupt infrastructure and sow confusion immediately before an attack. Where a balance of reusable/redeploy able drones are used, this may also involve a wave of drones sent to destroy infrastructure at the onset of the attack and then more nimble drones that can penetrate up waterways in support of land forces.

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.