International Association of Maritime Security Professionals

31 Aug 2024
Volume 2, Issue 4

Wavefront

A Need to Evolve

This issue of the bi-monthly newsletter focuses on the challenges associated with changing the model through which maritime security doctrine is developed. As the industry grapples with decarbonization, capacity building for seafarers, various forms of Maritime Autonomous Surface Ships (MASS), and digitalization, certain trends and issues continue to arise.

In keeping with the International Association of Maritime Security Professionals focus on building better, this looks to present constructive suggestions. More than enough organizations and individuals are contributing to the cacophony of criticism. While criticism has its place, it needs to be coupled with useful suggestions and opportunities for improvement.

These are presented in the spirit of starting or building upon useful discussions. As importantly, however, is we need to move past the discussions at some point and begin to look at the various forms of reform and evolution that are becoming increasingly necessary to protect and preserve maritime personnel, operations, and infrastructure.

Inside this issue

Special points of interest

- We are currently wrapping up the proofing phase of the CMSP courses. These are anticipated to be available beginning September 2024 as we move to the next phase of training modernization.
- We will be updating the IAMSP Learning Management System for those looking for online training in September-October.

The Rush Towards Easy Answers

Progress is incremental by nature, with very few exceptions. What becomes tempting, given the scare resources and time needed to address certain challenges, is to fail to address the longer-term and more systematic challenges.

We see this in the rush towards "standards." While standards have their uses, they do not necessarily replace proper due diligence. As a matter of fact, there are those that would argue that the blind application of a best practice or standard without validating that it is, in fact, appropriate to the environment, may fly in the face of sound practices.

This does not mean a standard is not useful. It means that we must both craft these standards in a way that does not drive unknown risks into operations or act as a crutch for those avoiding their responsibilities.

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.

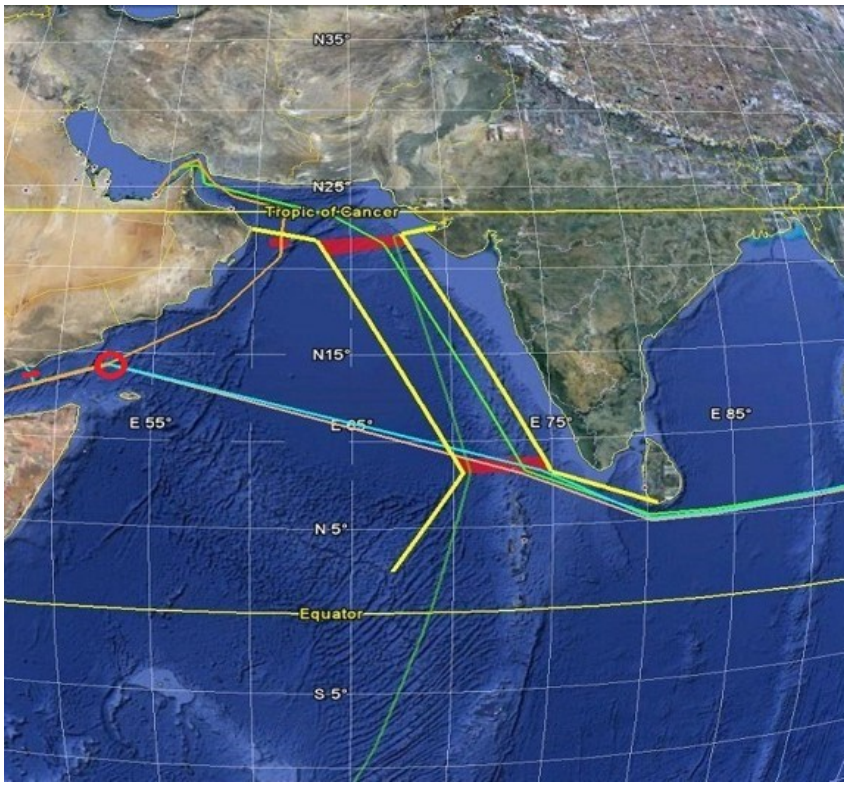
Technical Capacity Building

Continued on Page 6…

Just recently, the IMO's Technical Cooperation Committee held its 74th session at the IMO Headquarters. As noted in the address of the Secretary General at this meeting's opening, the vision is for a "strengthened IMO technical cooperation program which is responsive to the needs of the Member States, especially for developing countries." It further goes on to look for the program to be "built upon the achievements to date, and focus on the detailed needs identification, thematic programming, regional implementation, stronger partnerships, good donor relations, and results-based management." Additionally, "women empowerment must be embedded in all our technical activities and interventions."

The IMO Capacity Building Strategy (also referred to in terms of Resolution A.1166(32) of 28 January 2022, sets forward the mission, vision statement, overarching principles and work streams for this effort.

While space limits reposting the mission and vision statements (refer to Section 5 of the link above) and some of the identified weaknesses of the strategy (refer to Section 8), an opportunity exists for the IMO. While the IMO identifies certain institutions, such as the World Maritime University, Maritime Technology Cooperation Centres, and public private partnerships, it could place more emphasis on some of the Capacity Building activities that take place outside of the normal circles influenced by the IMO, such as education institutions that are not necessarily maritime training academies.



Expanding Upon a Model

Continued on Page 7

Recently, a model was discussed by Dr Peter Ricketts, a former President of Acadia U and current Professor of Earth and Environmental Sciences, that looked at a more complex model involving maritime security. Published in the Ocean Policy and Research Institute (No. 574 on July 5, 2024), the *Maritime Security in the Age of Climate Change—the need for a New Paradigm for Education and Training* presented a structure on how maritime security interacts with geopolitical, environmental, sociocultural, and economic domains. Some additional comments about that model may be warranted as it offers both new challenges and opportunities.

Maritime Security has often been looked at in terms of dependency-based models. As our ability to understand the world around us increases, we have found to be this simple model useful for addressing simple issues but not wholly representative when looking at the broader range of complex interactions. What we have found is that maritime security operates as one aspect of what may be better described as a *complex adaptive environment* or a *complex adaptive system,*

Certain aspects of complex adaptive systems are easily aligned with the concept of the maritime environment. Much of the system is self-organized with control being decentralized and often governed by the different interactions between parts of the system. The system may be subject to an impact that appear disproportionate to its impetus and that impact may actually grow or change as it moves through the system. The system adapts and can often "heal" in new ways.

Perhaps the two most telling things, however, can be summarized in terms of the following:

- Those studying the complex adaptive system are not necessarily aware of all the players in it nor are they aware of how those players interact.
- The system does not reset to its original state. It forms a new state as a result of its adaptation.

Understanding Systems

In this context, systems refer to a community of things that are managed or brought together to perform something more than any one piece could have performed on its own. In this context, we need to understand that the maritime sector is part of several larger systems—ranging from military to supply chain. Yet, we continue to see efforts within the maritime sector that fail to recognize that very basic principle of design.

A system also implies that there are desired goals to be met and objectives to be achieved. The failure to recognize how maritime security efforts connect with these larger systems can lead to what would otherwise be good project having dire consequences.

One such example of this involves most of the seaports around the world. While commercial shipping factors significantly, failing to recognize the impacts that new technological development could have on local populations, unregulated users of seaports, recreational communities, and others can lead to circumstances that runs afoul of the purpose of conventions such as SOLAS.

Ultimately, those involved in the engineering of these tasks and the management of these projects shoulder this responsibility, if not in their project charters (or equivalent) but in terms of the Values and Ethics statements that they committed to upholding.

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.

Insider Threat Toolkit

The recent IMO provision of an "Insider Threat Toolkit" provides a decent start for those looking at establishing an "insider threat program" but appears to align with much more traditional approaches to security management. There are some very specific areas that should be included in this guidance to ensure that the "insider threat" is actually addressed appropriately.

The first issue is in the definition of an "insider." This definition does not capture the nature of an insider from a security doctrine point of view. The insider is any individual that has been given access. It includes all employment (and similar) relationships and does not necessarily have to be part of the maritime shipping industry—at seaports it could be tied to any number of different sectors. A cyber-centric definition of an insider threat can be found through the CISA.

The first step in establishing this kind of program is actually developing an understanding on two fronts. First, you need to understand what you have and why it may be attractive "to the wrong sort." The starting point for this involves three major activities:

- Establish an inventory of assets and a method for identifying any assets (such as through a quick assessment process) that would identify assets that may be valuable due to their sensitivity, attractiveness, or ability to be sold .
- Establish controls that limit the access to these kinds of assets to only those that have authorization to them.
- Protect both the inventory and the control lists from unauthorized modification or deletion.

The second step in this involves ensuring that job descriptions are established and kept up to date. The job description is vital on two levels. First, it sets the basis for generating the list of those that are actually authorized to have access to certain assets, operations, spaces, or operations. If access is not required by the individual, it is denied unless their management authorizes temporary access (through a formalized process) to give them that access.

The job description is also important from the perspective of setting expectations. Where an employee is believed to have attempted unauthorized access, the job description provides a neutral, written, and most-importantly agreed-upon record of what the company expects and what the employee understands. If the access aligns with the job description, then any issue can be quickly dismissed without escalating to a staffing issue. If it does not, then there is a basis for requiring an explanation from the employee as part of an administrative investigation or something similar.

The second element in establishing an insider threat program that is not explained as fully as it could be involves the supporting policies and practices that become necessary to keep an organization clear of significant legal issues.

First amongst these is ensuring that the controls put in place to mitigate the risks associated with insider threat have clear purposes that can be communicated across the organization. The reason for this is simple: the arbitrary imposition of insider-threat controls will evoke a number of different reactions from different communities. Some of these reactions may come from "the wrong sort" trying to delay or even block the imposition of the controls. Potentially more damaging, however, are the reactions of the "good" personnel that may see the sudden imposition of these controls as being an attack against them or their work environment. This has the potential to actually promote the creation of insider threats as people may feel aggrieved by the imposition of controls and what they feel the company is saying by imposing them.

The second is ensuring that there are appropriate use rules generated for the controls and that privacy impact assessments are conducted along the way.

For this reason, we would encourage caution with the use of this kit. Before rushing to implement the measures in it, we would advise those seeking to establish these programs to seek out competent security practitioners who have worked with these kinds of programs in the past. Otherwise, the organization may create challenges it seeks to avoid.

eLearning

While the IMO Technical Cooperation committee is looking to deliver eLearning training by "transforming some existing IMO training material to eLearning courses to supplement the delivery of in-person technical cooperation activities." This is being done in conjunction with organizations, most notably the World Maritime University.

Currently, one can find the learning port at https://lms.imo.org/moodle310/ and the number of courses is somewhat limited. This is normal when rolling out a program. It takes time to develop, edit, and deploy this kind of learning. As the IMO proceeds down this route, however, it may benefit from certain practices.

First, while there is a tendency to generate "flashy" courses, this may cause certain communities to face challenges in accessing the courses. The "flashy" courses are often used to help keep the attention of those who are taking the courses. What it can fail to recognize, however, is that certain communities may face limitations due to their infrastructure. These limitations could come as a result of certain infrastructure being behind in the region (such as not having access to widely distributed fiberoptic networks for distribution and relying on copper line) or it may be the result of the courses being mounted on infrastructure that is operating at close to capacity. One option in addressing this challenge involves offering a "low bandwidth" solution for courses.

Second, the eLearning course needs to operate within an environment where the identity of the individual taking the course can be assured. The issue with identity takes on three aspects. First, are you delivering a course to an individual who should have access to the kind of knowledge you will be communicating? Many courses can be offered broadly, but certain courses should be limited to those that are able to prove their identity. The second aspect involves the setting of examinations and testing. In the typical classroom setting, the proctor (or person supervising the testing) is present and can detect all sorts of different unauthorized activities, including people posing as other people. Finally, there is the issuance of the certificate or some other form of credential. One option to deal with this is to include a registration process that involves an identity check and the creation of a student profile. All courses and testing are then made available in conjunction with that controlled student profile. This will not prevent all instances or attempts at fraudulent behaviour, but will address at least some of them.

Learning may involve common approaches, but is a highly personal experience and can be subject to a range of influences that can disadvantage otherwise "good participants."

When creating the eLearning platform, it is important to allow for certain kinds of off ramps or alternatives. Let's consider the delivery of an online program that becomes necessary for those involved in a specific activity.

Has the program taken reasonable steps in terms of offering an alternative means of learning in order to compensate for some form of challenge. For example, if the training involves a speaker talking to the student and the student faces challenges in hearing, can subtitles be activated to compensate for this and put the candidate back on a level playing field?

Addressing this kind of challenge as the program sets out saves significant challenges on several fronts. First, it avoids negative feedback from certain communities that could (rightfully) feel excluded from the opportunities the training offers. Second, it assists in communicating realist goals and planning objectives by ensuring that these kinds of tasks are built into the basic or general project plans associated with the learning. Finally, it can prevent disruptions that arise should an individual feel strongly enough about their challenges to challenge the program on various legal grounds, resulting in orders from the courts to either adjust or discontinue.

These challenges do not limit themselves to physical challenges. Other forms of challenges can present themselves (such as dyslexia) that can affect the candidates learning experience. It is immaterial to rate which challenges as which is most detrimental—these play out at a personal level.

Finally, in any training tied to continuous updating or learning, it is important to ensure that any record of successful completion (such as a certificate) includes either the date of the training or official version number. Should something arise where the individual needs to demonstrate what training they received, this information becomes very important to the process of identifying how exactly they were trained with respect to a specific topic.

These are simple steps that can improve the overall system and much easier to implement at the start of the process.

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.

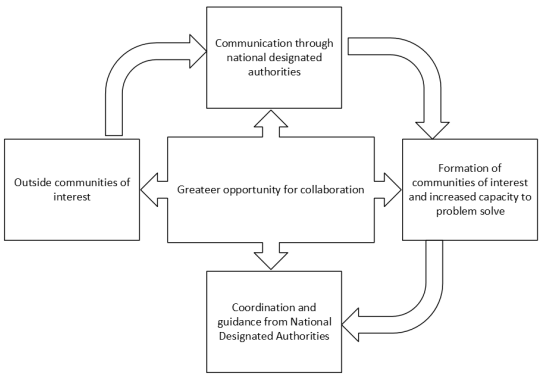
Technical Capacity Building

Continued from Page 2

Recently, the International Association of Maritime Security Professionals worked with Acadia University on such an endeavour to create the Professional Certificate in Maritime Security (PCMS) with the assistance of the Industrial Technical Benefits Program (ITB) at Irving Shipbuilding.

What was telling in the development of this program was that several federal departments and entities knew of this effort, were supportive of it (at least tacitly), but not once mentioned that it could be aligned with efforts in this light.

One aspect of what was missing, in this one limited example, was the reporting mechanism through which the project could be identified through the national designated authority back to the IMO Technical Committee, and then communicated out to other communities that may have had the same needs or faced the same challenges.



The establishment of a coordination portal, such as the one used for the Maritime Consultants, could assist in the identification and formation of communities working to address common challenges. For example, the efforts to develop the program at Acadia University could have linked with other universities seeking to develop similar programs. While the Acadia U program brought together a number of practitioners and professors that were able to form these kinds of consultative networks, the presence of this kind of capacity could both simplified and reinforced this effort.

A rough representation of what this framework could appear like is presented in the graphic above. For this to work, the National Designated Authority must first have the tools (such as the portal) but must also have the willingness to use those tools. Once the National Designated Authority, however, has opened the door, we can start to see the formation of broader communities of interest as well as the ability for the National Designated Authority to guide the discussion, if only in terms of where it wants to see its national maritime security policies heading.

While this structure may not be perfect, it offers an improvement over what we see in many other domains on three fronts.

First, it brings together communities that, in turn, limits the exposure of the system being exploited for purely commercial interests. We have seen, and continue to see, the promotion of "near-guild-like" approaches to various issues in the maritime security space.

Second, it provides an entry point for the regulatory bodies and other forms of oversight to ensure that what is being developed aligns well with matters of public safety, national priorities, and sound due diligence. We continue to see projects that have limited their consideration of how they will impact the overall maritime sector as they push towards getting their own technology or approaches to market. It is the job of the regulator to get ahead of that.

Third, it builds the capacity across the divide that the Secretary General seeks to bridge. This kind of portal need not be limited to contracting states or regions, it can present an open forum. While there are always some risks in this, those can be offset through guidance by the National Designated Authorities. For the Least Developed Countries and smaller island states, it offers an opportunity to be present at the table and not simply look for the generosity of those at the table.

Expanding on a Model

Continued from Page 3

This can present a challenge for those seeking to understand the impacts of their decisions.

Countering this challenge involves one of the basic principles associated with the design of sound systems—taking a multidisciplinary approach. This has two parts. The first means that it involves building out the communities that are involved in studying things so that the next stage of understanding represents a broader set of viewpoints. The second means that engineering-related processes (particularly when identifying the impact of decisions and stakeholder needs) should not fall under the oversight of the engineers but rather those who are responsible for the risks inherent with the use of the final product.

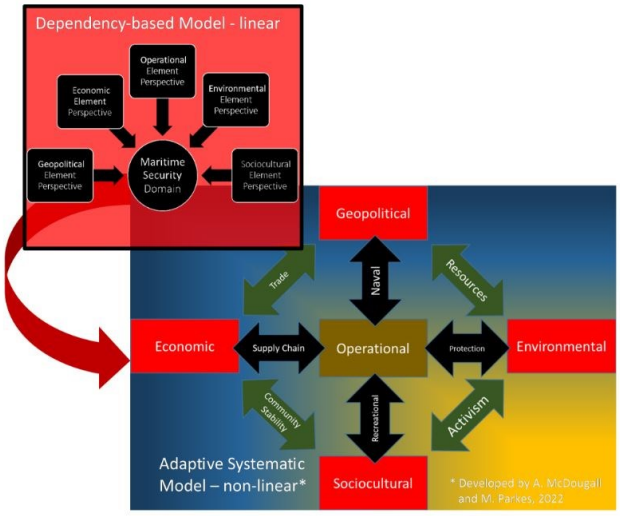
This represents an understanding that while certain processes within engineering are listed as technical processes, they are technical processes that may either be guided (but not controlled) by engineers or that may have outputs crafted to fit into engineering processes. The reason for this is simple, the owner of the risk is the one that is ultimately held accountable for the work done to identify (and minimize) the negative impacts associated with the work.

We need to expand our understanding of how things impact as an integral part of proposing, designing, developing, and rolling out new technologies that can shift the maritime security paradigm.

So how do we approach this challenge using this model? Simply put, we can begin to look at the identification of stakeholders from each one of the major categories of geopolitics, environmental concerns, sociocultural, and economic factors. We then bring those communities together with the understanding that the question involves how is the new technology being proposed for use and potentially impacting the various communities?

Consider the MASS question. While we have looked at the potential economic impacts and, to a lesser degree, certain environmental impacts, have we looked at the sociocultural and geopolitical impacts?

Second, we have to ask ourselves if we actually understand how these different factors influence each other. At this point, we could likely state that we can make qualitative assessments but not quantitative assessments because we don't yet understand those interactions to that level of granularity.



And it is in this that there are a range of exciting research opportunities for those involved in modelling, simulation, and the artificial intelligence fields. As we look at the technical capacity building put forward by the Technical Committee, perhaps some of the projects that can be shared with the other universities and centers involve efforts to better understand how these interactions happen and affect each other. These would, by necessity, have to be multidisciplinary and subject to fairly rigorous review across the wider maritime community. Nonetheless, if we are looking to make profound shifts in the maritime security paradigm, we needs to have a more granular understanding of how those shifts will impact immediate and wider communities.

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

As we begin to look past the fall of 2024 and into 2025, we see many of the challenges from 2024 persisting.

On natural fronts, severe weather continues to challenge those involved in design and operations. We have seen challenges associated with many of the models used to predict severe weather and other conditions as other factors that can influence weather emerge.

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.