International Association of Maritime Security Professionals

30 October 2023
Volume 1, Issue 2

Wavefront

Professional Certificate in Maritime Security (PCMS)

Wolfeville, NS

Most of the candidates for the PCMS have completed their first two courses. While the first course progressed as a cohort, some candidates required additional flexibility due to work environments. This flexibility is one area the Association prides itself on—offering a hybrid model (online with access to instructors) but still leaving that flexibility for one-on-one interaction.

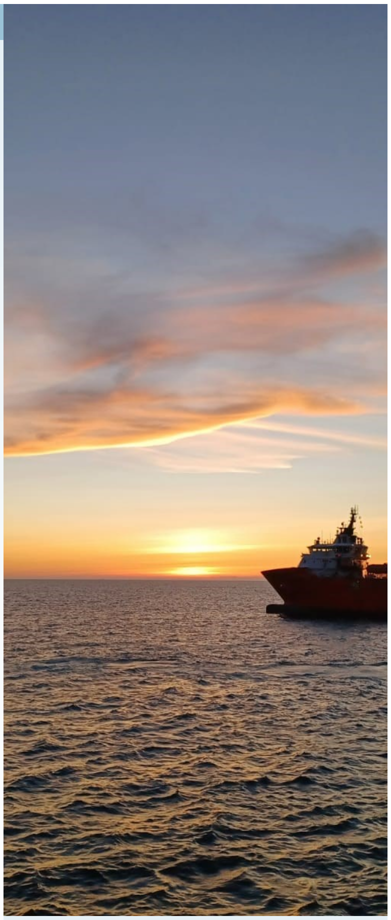
The Security Design course is arguably the most challenging course of the three. Based on principles very similar to many engineering disciplines, the content requires not just an understanding of some complex content but also challenges candidates to put those concepts to use in their own environments.

As candidates move towards the third course, this would be the final course offered in this program by the IAMSP. Those passing through will have been presented a structure with which to apply the academic courses presented by Acadia U that gives candidates a much more holistic understanding of the maritime security domain. It also achieves the benchmark (through examination and evaluation) that leads to the Association's recognition of their capability and achievement.

IACS Incoming Requirements

As we approach the implementation dates for the International Association of Classification Societies (IACS) , we will likely continue to see refinements in those rules. For those tracking their progress, we would recommend building in the same level of flexibility into your own efforts and encourage processes that include traceability to facilitate making those adjustments over the next few months.

The IACS' new unified requirements mark a significant set forward in the cyber security domain, but we will see challenges in its implementation and its monitoring. This will require the IMO, governments and insurance companies ensuring that IACS is given appropriate support so that we do not see instances of "watering down" or "corner cutting" creep into the requirements.



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.

Best Practices...A Hidden Vulnerability?

The role of best practices has been to assist organizations when faced with particularly challenging issues. The collective efforts, thinking, debate , and ultimately consensus can be a powerful tool when dealing with immediate issues.

Best practices, however, are written with an understanding of acts or conditions at a certain time. This is not because of any individual organizational failing, but is simply one aspect of how these things are produced.

That being said, the world is not a static place and arguing that the conditions now are the same as conditions twenty years ago will not get you much traction in communities that take issues seriously.

There are two keys here.

First, do not simply apply best practices without first examining the context in which they were written and the current environment. Blind application of even well-written best practices can lead to disaster because threats or vulnerabilities have been missed.

Second, instead of just applying the measure, application of best practices should include two parts., The first, and arguably most important, is that the sound practices (such as threat assessments, risk assessments, etc.) underpin the measures that were taken. The second is that the measures as applied reflect what was found in those assessments.

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

Other Implications

When looking at innovation in the military and dual use context, those involved in the conceptualization and design processes need to be aware of the broader set of requirements that are becoming more prevalent in the defense communities.

One major element is what is called the Assurance Case. This case can be described as a series of arguments supporting the claims that what is being done will not only work in its predicted environment but also within reasonably predictable contested environments.

These requirements are not unsubstantial and need to be in place as early in the project as possible to avoid significant costs later.

Dual Use Technology

Continued on Page 6…

Part 1—The Context

We are seeing a great deal of research and innovation in the ocean research and maritime space. Innovation, however, is not something that happens easily. While creative writers and movie makers may celebrate the "Eureka" moments that appear sporadically throughout history, those that are more involved in the innovation space understand the sheer trials and tribulations that an organization can go through when attempting to take a product from an idea to market.

One of these trials involves finding the funding necessary to bring a product to reality. People need to be paid, operations need to be covered, and the various inputs that need to be brought together all factor into this. As anyone involved in an innovative project understands., this effort alone can be significant.

It is in this context that we are putting forward a series of articles looking at dual-use technology. Those looking for funds will have noticed that there are several sources of funds that offer support for the development of these kinds of technologies. But what are the strings?

Part 2—What is meant by "Dual Use?"

In keeping this simple, "dual use" technology refers to technology, goods, or software that have both commercial and military applications. Why is this important? Because if your innovation falls into this particular category (or you guide it into this category) you should be aware that many governments apply export controls and regulatory requirements that may limit your market for the product.

Before we over-focus on the ability to reach a market, however, we should qualify that we want to reach the right markets. These expect controls (and other controls) are largely intended to ensure that technology does not end up in the hands of groups that would use that technology to do harm, aid in repressive regimes, and a host of other issues.

Infrastructure Life Cycles

Our current challenge with climate change is doing more than causing challenges with respect to cleaning up damages and restoring services. The more astute mind will also have started to ask the question "Do we need to rethink how we are managing the life cycles of infrastructure?"

Infrastructure (both physical and information systems) can be looked at in terms of a series of managed and interconnected steps that cover *conceptualization*, *planning, design and development, operations and management,* and *removal from service.*

Our current climate challenge starts early in this process with *conceptualization*. The process of conceptualization is really looking at what we want to accomplish and aligning that with the art of the possible. From the perspective of climate change and severe weather, we would be well-served to understand two things. First, that there is greater uncertainty as we move out into the future. This may affect the safety margins that we want to apply to that conceptualization. The second part is that we are seeing an increased frequency and severity of weather events. We only have to look at open media reports that Atlantic hurricanes are more than twice as likely to rapidly intensify from weaker / minor storms to major events.

There is also a tendency to build "to code." We may be well served to stop thinking of "to code" as being a high quality standard but rather as the minimum acceptable standard. The key here (as previously discussed with best practices on Page 2) is to first determine if the context in which the code was written was changed and, if it has, should different requirements be put in place (more stringent or additional)?

Finally, we need to establish a better balance between being proactive and being reactive. Like any other effort, this will require costs and being proactive is by no means a completely scientific approach. But we do need to understand that if we are going to prevent catastrophic impacts in the future, we will need to mitigate those threats, have the resources necessary to contain and isolate the impacts of those threats, and the resources on hand or within easy reach to respond effectively.

Continued on page 5..

Climate and Weather

Confusion still seems to exist when discussing climate change and extreme weather events. These two things, while linked, are not the same.

Climate change is must be looked at as in two contexts. First, it is systemic in nature. It is not just about sea temperatures, air temperatures, changes in humidity, or the distribution of moisture. It is about all of those things together.

It must also be looked at in terms of a longer-term shift. This is not a "one-and-done" kind of issue but is one that requires longer term solutions. Those longer term solutions are going to impact how we would like to organize ourselves and how we want to live—like it or not.

Extreme weather, on the other hand, is what hits you when you step on deck or walk out the front door. Severe storms, rainfall events, heat, winds, and other immediate conditions fall into this category.

Extreme weather may or may not be caused only by climate change. These are not simple systems, they are complex, adaptive systems that are rebalancing into a "new normal." What can be certain, however, is that the changes to climate are certainly one factor (and likely a very significant one) that is helping form these events.

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 consistent 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.

Connectivity Continued...

.When considering aspects of International Association of Classification Societies (IACS) Unified Requirement E22 Section 4.2.3 (System Description), caution should be exercised to ensure that the communication and interface aspects do not stop at the hull of the vessel. They need to look at the functionality of the system itself.

Consider, for example, an engine that may maintain a live connection back to a manufacturer that can make adjustments to that engine. There is, of course, a logical reason for this. It helps in the efficient and safe maintenance of the vessel and particularly a Category II / III systems.

If this connection, however, offers the means and opportunity for the engine's performance to be affected, it should also be looked at as a potential vulnerability. This doesn't mean that it must be removed. It simply needs to be identified, its risks assessed, and for appropriate risk management actions to take place. As ships become increasingly connected, we should be reinforcing the need to identify these "off-board" services that can have an impact on the safe operations of the vessel and ensure that they are considered not as secondary aspects but as intrinsic aspects of

Approaching Cyber Security

Organizations can approach cybersecurity two ways. The first, and most common, is to look at cybersecurity in line with other security domains as a cost of doing business that seeks to prevent losses. This is not untrue. It does have a cost (sometimes a significant one) and it does seek to minimize losses due to various forms of disruption, modification, or loss. This can trap an organization into having to rationalize the cost of security against some combination of historical impacts or predictions of future attacks. Either way, this traps security managers and executives in a situation where they are attempting to rationalize the costs of a program against what would appear (to those on the periphery) to be a reducing return on investment.

Another approach may be to look at cybersecurity as part of achieving operational excellence. Consider the difference between enforcing routing in a system in order to prevent the pivoting of an attack as opposed to enforcing that routing as part of efforts to ensure that the system maintains a level of surplus bandwidth to be operating optimally.

Another way to view this is quality being described in terms of a system doing what it is supposed to do and not committing resources in ways that are contrary to that purpose (an aspect of waste). If the approach to security is to integrate security controls into the design of the system so that overall security of the system emerges as an attribute of good design, three things are accomplished:

- We are ensuring a better understanding and control over the functionality of the system in question.
- We are reducing both the attack surface but also the vulnerabilities behind that surface that may be exploited by attackers.
- We are limiting the number of potential conflict or friction points that arise as security infrastructure is added to the system.

Security practitioners may want to give some thought to this approach.

Managing Infrastructure Issues

Continued from Page 3

What does this rebalancing (proactive from reactive) actually mean where we are managing infrastructure? The answer lies in the risks that are inherent in fragile infrastructure.

Fragility may be described in terms of the propensity of something to fail under certain conditions. As the oil gets older in our vehicle and is put under longer periods of strain, it eventually gets to the point where it no longer protects the engine the way it needs to and needs to be replaced. Where the engine operates in such a way that the lubrication process is under greater strain (temperature, etc.), then we may reach that replacement point faster.

This leads us to the first activity necessary to be proactive—understanding our own infrastructure. The question here is if an organization operates or uses infrastructure that is operating beyond its original design thresholds (worst case) or that is operating under greater strain (more likely). How does this affect the infrastructure's usable lifespan? The outcome of this question would be the list of infrastructure that may need to be looked at sooner than others in order to maintain operations.

If we consider how we design infrastructure, climate change and its manifestation through severe weather push us towards increasingly fragile infrastructure.

Why is this important? The shortening of the useful lifespan of infrastructure affects the return on investment associated with that infrastructure. Businesses (or other entities) need to realize their returns on investment within shorter timeframes.

This can lead to the second challenge—the margins associated with that infrastructure. As we shorten the useful lifespan of the infrastructure and constrain the time we have to realize the return on investment, we need to understand how that affects margins in the medium and long term.

This will also be impacted as a result of the costs associated with the next iteration of the infrastructure's life cycle. The costs associated with the removal from service are advanced towards the short term and the savings necessary to afford the replacement infrastructure are placed under a similar pressure.

This can be further compounded if the organization needs borrow money in order to play for the next cycle. The costs of that borrowing.

So how do we address this kind of challenge?

The first step involves the mitigation process and setting down the parameters for what can be acceptable. In many coastal communities, building within a certain distance of the shore is no longer permitted due to erosion and storms. The same concept applies to maritime infrastructure—set down what are considered to be the conditions under which risk becomes too great.

Second, don't just write preparation plans, but test them and train people in using them. Training is a perfect opportunity because you can begin without all the distractions of random (or even hostile) events going on around you. Build the way you would do it into the Standing Operating Procedures (SOP's) so that the steps become second nature.

Finally, begin with a review of your Mutual Aid Agreements (MAA's). Make sure that these are up to date.

This is just the starting point. While some will argue this is more Emergency Management than Maritime Security, the Maritime Security domain is both highly regulated and subject to all the same challenges. Taking steps like these help demonstrate that your security posture is covered for both the long term but also taking into account the period of uncertainty we are entering.

Dual Use Technology

Continued from Page 2

So, we should not simply discount the export controls as being something of an inconvenience. They should be looked at in terms of a valuable, if not indispensable, aspect of helping keep ourselves and our allies at less risk of harm.

This effort should not be construed as guiding organizations away from innovating in military or dual-use spaces. While innovation in this space may be maligned in certain circles, the reality is that it is a vital part of protecting nations and their populations.

Part 3— The Framework

This will look at the international and legal frameworks that surrounds this kind of activity. While not legal advice, it is intended to inform individuals and organizations who may want to consult with appropriately trained and experienced individuals as they approach that line in the sand.

As a result, organizations involved in innovation should be asking themselves two questions.

First, is what I am working on something that is primarily for a military purpose or something that may have both civilian and military purposes?

Second, what is it about my innovation that brings it into line with these two categories? Is it something tied to the innovation itself, some aspect of the innovation, or something within the innovation?

Part 3 will provide a starting point for those entering (or considering) this space so that they have a good footing upon which to build.

Part 4—Affects on the Opportunity Space

Like all choices, there are "pros" and "cons" to be weighed. The military and dual use markets are often lucrative and if the innovation can be tied to a major project, it can offer significant opportunities.

At the same time, entering this space may also mean that certain markets become more difficult or forbidden to access.

As this decision can affect the viability of the innovation, there is a need for business leaders to have an understanding of what entering this space means.

Part 5—The Effort Space

Those entering the military and dual-use innovation space should be under no false impression that this can be "business as usual." Working, including innovating, in this space requires that companies adopt a number of internal controls that will affect their governance structures, personnel, assets, information systems, activities, and supply chains.

These efforts are not done in isolation. There are stringent regulatory requirements that will come into play that will place constraints on the organization, its decisions, its infrastructure, and even its future plans.

General Conclusion

Innovators entering this space should be aware of the opportunities and impacts that will affect their efforts. While the "siren song" of organizations with deep pockets and significant funding opportunities may be attractive, organizations may be well served by the ancient warning of *festina lente* or to make haste slowly and to ensure that they are making their decisions with measured and forethought.

A Knowledge Gap

As we look towards new and improved ways of ensuring that security is built into the various systems, we need to review and update our education, training, and mentoring regimes to ensure that we maintain that critical mass of practitioners within the space.

While IT security practitioners are plentiful, what is lacking is a combination of IT security practitioners that have a good understanding of the maritime space, how it operates, and the various safety considerations that need to be considered.

At the same time, we need to be careful that the market is not simply dominated by structures that are more akin to guilds or licensing regimes. These tend to serve those organizations more than the industry itself.

One alternative to this may be to provide free familiarization training through the IMO eLearning platform. Courses on pollution control and similar challenges already exist in that space, they can be distributed fairly to any individual that has the capability to receive them, and can be separated from commercial interests.

This may also help communities that currently face economic challenges in accessing training. Care will need to be taken, however, in ensuring that access to the technology does not become the limiting factor. While there is only so far an organization can go to ensure fair and equitable distribution across all environments, we should not let perfect get in the way of good. An attempt should be made to keep things well balanced.

Some Thoughts on Response

Very often we look at security in terms of risk assessments and the various protective controls. One of the key challenges, however, involves the detection and response to suspect acts or conditions. This is becoming more important as we see demographic shifts in our societies and discussions surrounding some things that were assumed to be valid.

The detection of suspect behaviour is something that has several challenges. Is the behaviour actually suspect or suspicious? Is there a valid reason for the behaviour that may not be apparent? These questions have been looked at rather significantly over the past twenty years as a result of issues linked back to security posture changes resulting from 9/11.

But what about our own security organizations and how they are conditioned to respond?

The root of this challenge stems from three major factors. First, security guard positions are often considered entry level positions that do not require a significant amount of training beyond some basic regulatory training. In looking at position descriptions (including their training) for 50 positions across different companies, only five companies listed additional training beyond the regulatorily-required training as being mandatory. Over half of them considered additional training to be an asset (i.e., desirable but not necessary).

We need to move beyond the foot-stamping of saying the system is broken and start doing the hard work of finding solutions.

Second, security guards are tied to what are described as post orders that describe their roles and functions and act as their "playbook." These post orders, however, cannot describe every possible situation and, as a result, often have comments like treating people "equitably and respectfully." These kinds of subjective terms do not cast back to training or other sources of guidance making them arguable and subject to challenge. One person's view of respectfully is not necessarily the same as another's.

Finally, most security guard positions are not terribly well compensated with the majority being only slightly above minimum wage with some minimal allowances for uniform upkeep. This is often influenced by contract cost considerations (human costs can add up quickly). But how much additional effort can one really expect from an individual who is working under these conditions?

The result has been a shifting of the response away from the security force onto the different forms of law enforcement and emergency responders in the area. This will have its own challenges. Local police forces are often strained with many being in a position where they are having to triage their responses to property crime.

One option that has been rather innovative in this has been to have the port security personnel undergo training and volunteer with the local first responders. The proprietary guard force not only picks up the skills and understanding of the first responders, but can often form the personal ties within those communities that eases the relationship between the organizations. At the same time, the first responder community receives an influx of much needed volunteers that can help keep front line officers in the field.

Another option would be the reconstitution of the Ports Police. This organization, which had been formed as the law enforcement body under the Canada Ports Corporation was phased out in 1998 when the Harbours Commission Act was replaced by the Canada Marine Act.

While there are joint law enforcement bodies (such as the Integrated National Security Enforcement Teams) that can provide a degree of specialized services, these teams need to remain reasonably flexible and not tied down in day-to-day policing activities. The RCMP is currently struggling and may be described as being at a cross roads given its role as both a national police force and the contracted police force for several provinces. In short, they are not covering the demand as it sits now so it makes little sense to add another portfolio to it.

One of the reasons why the port police ran into challenges involved a complaint by the RCMP that there were jurisdictional issues that interfered with investigations. The police may want to look at structures such as unified command used in Emergency Management if there are challenges in dealing with multiagency operations. Another option may be to set up the Port Police as something similar to an auxiliary under the INSET.

Either way, it is clear that if we do not maintain a credible response and enforcement capability that can operate on a 24 hour basis, economic and supply chain pressures will only serve to give criminals an impetus to look at our port infrastructure ,

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

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 would like to congratulate Gordon Foot on his efforts climbing Mt Kilimanjaro and the efforts he has made on behalf of a number of charities.

For those who are interested, please check Gordon’s posts on linked in for the link to the Seafarer’s society.