International Association of Maritime Security Professionals

20 December 2023
Volume 1, Issue 3

Wavefront

A Shift in the Environment

As the conflict between Israel and Gaza continues, commercial shipping has come under increased risk. The most recent of these, the seizure of the MSC Aries is particularly problematic.

Iran's foreign ministry has claimed that the ship was seized for violating maritime law. It has not specified which laws. The sole other detail from the Iranians is that it is definitely linked to Israel.

The question that legal experts, lawyers, and courts will likely find at the front of their list of questions is if Iran has run afoul of international maritime law in the seizure.

We can dismiss the notion of this attack being an act of piracy. The United Nations Convention on the Law of the Sea (UNCLOS) involves an attack "committed for private ends by the crews of the passengers of a private ship or aircraft." Nor can we argue that Article 102 applies. It is clear that the helicopter involved and troops involved were military forces and had not mutinied.

So what about Article 106. Iran has been careful in its statements not to declare the ship as being involved in piracy. This calls into question the applicability of Section 106 because the seizure of the ship involved is "on suspicion of piracy."

What we do know is that the MSC Aries was taken in international waters and had not been pursued by Iranian forces from their territorial waters. This makes it a bit more challenging to argue the right of clear pursuit.

What this does show is that commercial shipping cannot hope to consider itself from this state-on-state action. Like the 1988 tanker wars, commercial ships may not find themselves as pawns and subject to malicious seizure at the whim of a combatant. This only further challenges our supply chain issues and increases the potential cost to shippers as insurance companies look to cover risks.

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.

Watching for a Critical Oversight in Cybersecurity—OpEd

Cybersecurity in ports should not be driven by ship-based cybersecurity requirements. While the focus of many of these regimes concentrates on ships, ports operate in a significantly different space.

First, ports are not homogeneous communities. They might better be described as a collage of communities, many of which have their own regulatory requirements. Failing to take steps to identify where ports may be subject to these regimes in support of a set of requirements suitable for ships could force ports into different forms of regulatory conflict.

Secondly, ports fall squarely within the port state's control and can often be tied to critical infrastructure.

Those involved in engineering would be well served to remined themselves that their engineering projects must respect the laws and regulations of the spaces in which the project intends to exist.

In brief, failing to recognize the constraints (external limitations) and restraints (internal limitations) in the larger system picture runs the risk of creating a silo around the maritime industry that does not serve the needs of the port community.

This begins with sound engineering practices and the identification of requirements (and constraints) as opposed to the rush to have products and services arrive first in the market.

The maritime sector does not operate in isolation. Consequently, rule making needs to respect the maritime sector's position in the overall supply chain and with respect to critical infrastructure.

The Role of Transportation

Transportation networks exist to move persons and goods from their point of departure to their intended destination so that they arrive on time, in acceptable condition, and for reasonable cost.

Acts or conditions that seek to degrade this mission may be seen as threats, each of which may manifest themselves as a result of the actions of many different actors.

While the maritime industry has grappled with physical and operational security threats for some time, its approach to Cyber Security threats is nascent and hurried, meaning that existing architecture and design processes must be checked to ensure they follow sound and safe practices.

CMMC 2.0 / CPCSC

Continued on Page 6…

Those operating within the shipbuilding industry should be aware of two regulatory regimes that are likely to affect cybersecurity requirements (as well as other controls)). The USA is currently working through the final rule-making for the Cybersecurity Maturity Model Certification (CMMC 2.0) based largely on NIST SP 800-171. Concurrently, Public Services and Procurement Canada (PSPC) has indicated that the Canadian Program for Cyber Security Certification (CPCSC) are likely to see similar requirements appearing in their contracting requirements beginning at the end of 2024.

These regimes began with the White House announcing a number of measures that are intended to assist in securing the USA defense supply chains. This particular effort falls under the oversight of the USA Department of Defense (DoD) Chief Information Officer (CIO) . Within the USA CMMC ecosystem, an accreditation body has already been established and various forms of consultants and assessors are being trained and identified. The Canadian offering, however, is more obscure in that the main announcements provide the only significant detail.

This will pose a challenge for the maritime shipbuilding sector, particularly since December 2024 is only approximately 8 months away. While this may seem distant, the steps necessary to become CPCSC compliant remain less than clear. Additionally, the time it takes for organizations to identifying their "Controlled Unclassified Information" holdings, the systems involved, and mapping the information flows associated with that particular kind of information will take time. Time will also be needed to conduct reasonable assessments and make any necessary adjustments to those systems (ensuring that there are no issues with parallel requirements such as under the Controlled Goods Program). Those who have been involved in the management of IT Security functions will understand at this point that there is not a lot of runway.

As we look towards contingency plans that may needed, we may be tempted to look towards the CMMC 2.0 model as a means of equivalence. While the Government of Canada has communicated that one of the goals is for the CPCSC and CMMC 2.0 certifications to be reasonably well harmonized (if not equivalent), what industry does not have at this point is that assurance.

Outside of Control

Continued on Page 7

The assumption that the next sets of serious conflicts will only involve military forces and targets is already proving false. The harassment (or outright attacking) of civilian ships in the Red Sea/Gulf of Aden only scratches the surface of maritime challenges.

Expanding this to events such as the underwater explosions on the Nord Stream 1 and Nord Stream 2 pipelines of 26 September 2022,, we face another challenge. How do we protect critical infrastructure that actually lies in less controlled, or even international, waters?

Consider the basic security framework of governance, identification, protection, detection, response, and recovery. This is simply the broader view of the NIST Cybersecurity framework but can also be applied to physical security concerns. Governance involves having that structure that directs activities and ensures an understanding of the environment (a gross oversimplification). It also ensures that where a challenge exists, some entity is accountable for addressing it.

Our first challenge comes when we look at the identification function. This speaks to how we have approached conflict, particularly in the west. Conflict has often been the problem of military forces and some other specialized government agencies. Can we safely say that this is a good assumption? One might argue when we look at what infrastructure Russia targets, the current use of assets in the South China Seas, and the examples being provided in the Red Sea/Gulf of Aden would show that this assumption no longer seems valid.

Then comes the issue of protection. The challenges associated with protecting widely distributed infrastructure (such as electrical distribution grids, water supply networks, telecommunications networks) is not new. Critical Infrastructure Protection specialists have struggled with these challenges for some time.

Detection of these kinds of issues gets much easier as you approach the time of the attack. It was not particularly difficult to identify that the Nord Stream pipelined had a problem after the explosions were detected. The pressure in the pipelines plummeted. As we move out and before the attack, however, detection becomes more challenging. Being able to detect activity below the surface can be complex. Determining that any detected activity is suspect becomes even more complex. Finally, there are the issues that can be raised with ensuring that detection does not involve a plethora of "false positives."

Responding to detected events will also pose significant challenges. Part of these challenges continue to be addressed through a shift in doctrine from a position that focused almost exclusively on robust ness (such as fortifying a production facility) to one that swung towards resilience (multiple facilities leading to more difficulties disrupting the overall supply).

As we consider expanding off-shore resources as a means of supplementing or event replacing our critical infrastructure, there is a need to ensure that we can protect and maintain that infrastructure appropriately. While the technology does have many advantages, does the plan for locating and establishing these wind farms have the necessary controls in place to ensure that they can be considered a trusted source of power?

These questions should be asked during the design phase so that appropriate controls can be built into the infrastructure as opposed to simply implementing a set of controls onto the infrastructure later.

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.

Transshipment and IUU Fishing

As we see increased efforts to control and exploit natural resources (particularly fisheries), we must take a more aggressive stance when designing the controls intended to counter IUU fishing.

Regulating the law-abiding fishing fleets is relatively simple. While some may attempt to stretch rules and an even smaller number attempt to bypass them, most tend to work within the various controls.

The problem here lies outside of the law-abiding community.

Transshipment essentially means that the smaller fishing vessels are offloading their catch on larger vessels that process and store the catch.

This provides the opportunity for the smaller fishing vessel to bend or break the rules and then simply state "all is legal" when off-loading the catch. At that point, an illegal catch can be mixed into legitimate catches, essentially opening the door through the controls.

Countering this requires full traceability of the first ship's actions, especially when operating in another state's controlled waters. This approach has been attempted by Peru, insisting that fishing vessels carry a satellite tracking system that would report their locations.

Consider the overall goal being to be able to determine that the full catch being imported can be considered acceptable.

Our first step does not involve processing but involves taking the fish out of the water. This is where IUU fishing actually occurs and this can be easily avoided when fleets use the transshipment structure.

The first instance would involve a number of fishing boats operating illegally but then moving their catches onto the processing vessel that may be outside of the various controls over the fishery. The illegal activity is hidden.

The second instance occurs when some of the fishing boats operate legally but others do not. The illegally caught fish are then mixed into those that were caught legitimately in what may be described as a scheme similar to laundering money.

These are just two of many different ways that can be used to hide the illegal harvesting of fish.

On option involves traceability. The government of Peru recently passed rules that requires ships to carry one of the government's satellite tracking systems on board. The intent here was to limit the opportunity for ships to shut off their own networks or trackers to avoid being detected "out of bounds."

Again, two scenarios challenge this control. The first is a simple refusal to carry the device. Peru encountered this reluctance first hand and encountered efforts that can be described as attempts to bypass the need to carry the system when coming into port.

These form the second scenario that has the fishing vessels coming to shore using a range of different conventions or measures as their cover for coming ashore without having complied with the regulations. These have ranged from AIS outages , declaration of mechanical issues, declaration of medical issues, and others. Reports indicate that in 2023 alone, seventy-five Chinese ships entered peruvian ports without the required satellite system and claiming force majeure reasons for entry.

The final element using transshipment to bypass these kinds of controls involves the certificates themselves. Even if all catches were legally made, the use of a primitive paper-based system for tracking the movement of the catch through the supply chain creates conditions where counterfeiting and document tampering become a challenge.

.One option involves phasing out the paper-based system and moving to a more credible tracking system. Today's technology makes it more than feasible to use an electronic system supported by a solid hashing function or blockchain. Coding this kind of report against the catch itself creates a more complex environment for those attempting to manipulate the documents.

In any cases, where transshipment is used in fishing, strong consideration should be given to (1) banning the practice outright, (2) limiting the practice to only appropriately licensed and trusted communities, or (3) modifying the regime to reduce the number of opportunities for people or companies to bypass the controls.

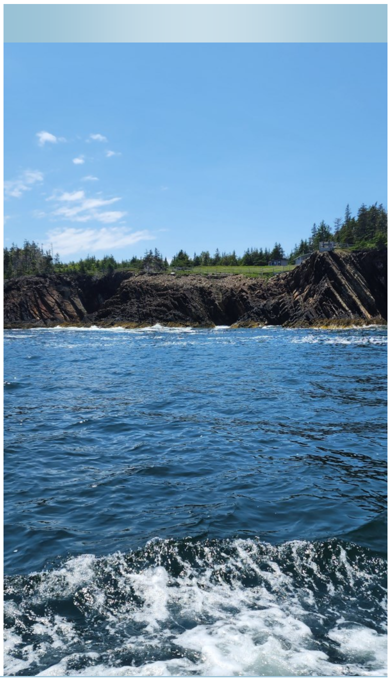
The PCMS Model

We are coming to the end of the first six months offering the Professional Certificate in Maritime Security (PCMS) with Acadia University. With candidates now wrapping up the final courses on the Association's side and getting ready for the academic courses, explaining the maritime security model may provide some context to the depth and breadth of this program.

At the center of this model sits maritime operations and, as a subset, maritime security. Around this central concept are four additional viewpoints: economic, geopolitical, socio-cultural, and environmental. These five elements are all linked.

Those undertaking the PCMS work through these five viewpoints to gain greater insight with respect to how maritime security affects them. Having completed the Capstone course, candidates are then offered the Association's practical courses.

These practical courses focus the knowledge gained through a rigorous and structured methodology based on Systems Engineering.



Having an understanding of maritime security is a first step towards building a better system.

A Resurgence of Armed Security On Board

The recent attacks on commercial shipping in the Gulf of Aden and on the Red Sea has created an increased demand for armed security on board vessels.

Unlike the situation of 2009-2011 that saw significant piracy-related attacks, today's operating environment is fundamentally different.

First, there are some similarities, particularly when considering the baseline piracy that has seen some commercial ships seized by pirates and taken to Somalia.

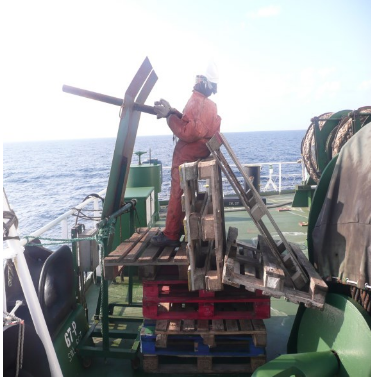
After that, however, many of the similarities end. Houthi Rebels have used rockets and drones to attack ships, a tactic not faced in the 2009-2011 campaign.

Additionally, attacks have included the use of helicopters to land on board the vessel. If known to be a "rebel" attack, this poses only limited challenges with respect to on board security teams.

Moving northward into the Strait of Hormuz, however, raises another challenge. The idea that commercial ships could be seized by state forces can pose real challenges.

For those companies seeking to enter the space, ensuring that you've included these challenges in your risk assessments and contingency plans for the protection of personnel will be essential.

Additionally, ensuring that you have appropriate insurance coverage for your personnel will also factor significantly given the potential liabilities that could arise with an unprepared team being taken.



As we look towards another certification being required for Canadian Shipbuilding Companies and the USA Defense Industrial Base, it is worth noting that this program is likely to overlap other similar programs significantly.

While Controlled Unclassified Information appears to be less controlled, it can often (but not always) fall into the category of Controlled Goods.

Companies will likely be well served to review their data classification (in terms of sensitivity and cybersecurity) to ensure that the definitions are clearly communicated. These differences should be incorporated into data management processes and labelling practices to ensure that information is treated under the right program.

This will require individuals to have an understanding of the Controlled Goods or similar programs as well as the new CMMC 2.0/CPCSC program.

We will be looking at some options on how to approach this challenge in future articles and with shipbuilding companies in the future.

CMMC 2.0 / CPCSC and Shipbuilding

Continued from Page 2

Consequently, the use of the CMMC 2.0 regime to achieve a certification that Canada will accept under its regime is not certain. The key risk being that industry may invest significant resources into a certification that carries little weight.

Certain industries, however, may be pushed down this pathway. While we would like to assume that the Canadian and USA Defense Industrial Bases are separate, they are not. As often as not, they are intertwined. Should the CMMC 2.0 and the CPCSC be out of synch with each other, then the industry will be forced into making a number of difficult decisions, including the following:

- Adopting the higher of the two requirements on single systems and then arguing that the higher controls levels offset any residual risks that come from not following the prescribed controls.
- Segregating networks and applying the prescribed controls in each. With many organizations already having to separate low-sensitive networks and those handling Controlled Goods, this will not be as simple as it sounds as issues such as access control, operations, and maintenance are considered.
- Removing themselves from one regime or the other depending on which program makes more sense from a business perspective.

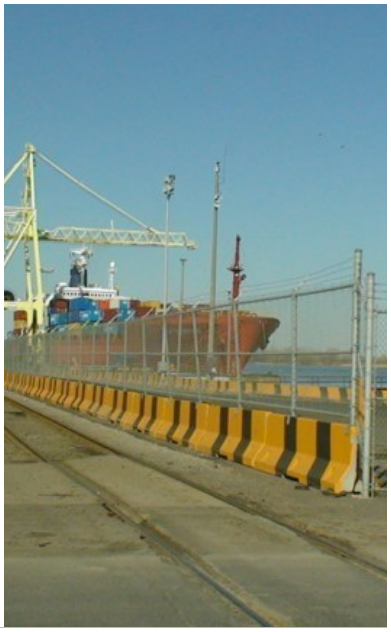
These decisions cannot be taken lightly and involve a level of planning. If these were completely new systems, then adding in the certification requirements would be relatively straight forward. These requirements, however, are likely to be applied on live networks. This means that organizations would be well-served to take the time to engage skilled practitioners and professionals, map out a reasonable plan for integrating those controls, and ensuring that there are appropriate test-beds or capabilities available to check the system before it affects operations.

For those offering this service, a second challenge exists. The USA CyberAB has communicated a restraint that only USA citizens will be able to achieve the necessary certification to conduct assessments at the CMMC 2.0 Level 2 or higher. In brief, Canadian citizens are shut out from this process and the trickle up impact is that many Canadian firms will be shut out from that market.

At this point, no similar restriction exists in Canada. While this may (or may not) come in the future, what is emerging as a relative lack of information is a situation where USA firms will be able to exploit the Canadian market and have their own market protected.

For Canadian Shipbuilders, this should be raising some red flags. Shipbuilding schedules are complex . There are more that enough challenges across the various supply chains to make the concept of appropriately maintaining and securing a supply chain difficult.

This, combined with the gradually diminishing lead time before requirements appear in contracts result in an increasing risk to most shipbuilding schedules. While it may not affect the cutting of steel directly, the instability in supporting supply chains (such as subcontracts who cannot certify) and enabling systems warrants much clearer and consistent communications.



Outside of Control

Continued from Page 3

.This resilience question also looks at the ability to redirect demand away from disruptions. For example, resilient systems may protect infrastructure to a point but then put in place a measure that redirects the demand for something should that first source be unavailable. The challenge here becomes the scale of establishing alternatives and what this means from a basic cost perspective. The other issue involves ensuring that enough surplus capacity exists in the system so that if new demands are placed on it, the system doesn't collapse under that weight.

Response in this context also faces challenges. The initial notification of an event is relatively straight forward, but containment and isolation become more challenging. Containment, or the stopping of an event from spreading, really takes two parts. The first involves being able to ensure that the actual event does not affect more infrastructure. The secondary, and sometimes overlooked, consideration is how the impact itself spreads. For example, a disrupted line and the rerouting of demand to a new line may actually impact the performance of the line that demand was shifted to.

We continue to look for the right balance between robust and resilient infrastructure. AI, automation, and remote operations will play an increasing role in this.

This challenge spills over from containment to isolation. Again, the event itself may be relatively easy to isolate. The secondary impacts or the indirect impacts, however, may not be as easily contained. The question becomes not how to deal with this in absolute terms, but at what point in containment and isolation do we move to being able to claim that the situation is being managed.

While the response for containing the specific event may be reasonably straight forward (re-routing communications or shutting a valve, additional complications may arise when dealing with international waters. How does one legitimize the response and how does one deal with someone or something that may pose a safety hazard to the response. For example, if divers are required, how does one deal with a vessel of some kind that begins to behave in a way that poses a risk to those divers.

The other reality of this situation is that the infrastructure may not be located near the intended target. In the coming conflicts, we need to be prepared for attacks against infrastructure that supports our own critical services occurring far afield. Given that civilian infrastructure and operations are now firmly inside the scope of how adversaries plan, it would be naïve to believe we can continue to avoid or dodge this issue..

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