International Association of Maritime Security Professionals

28 February 2025
Volume 3, Issue 1

Wavefront

The Changing Environment

We continue to see certain commercial fleets blurring the line between the commercial and the military. Those involved in commercial shipping should be particularly concerned with this trend and one might suggest that the International Maritime Organization (IMO) may want to reinforce the need for clear separation between the two domains.

If evidence arises that shows that commercial ships were involved in the damaging of subsea cables on behalf of a state actor's interests, this creates an clear challenge when looking at how coastal states can approach the issue of innocent passage. Article 19 of the United Nation Convention on the Law of the Sea (UNCLOS) sets down twelve conditions that are considered prejudicial to the concept of innocent passage of which this kind of damage would fall under "any act aimed at interfering with any systems of communications." Articles 112 through 115 (inclusive) provide more granularity to this framework.

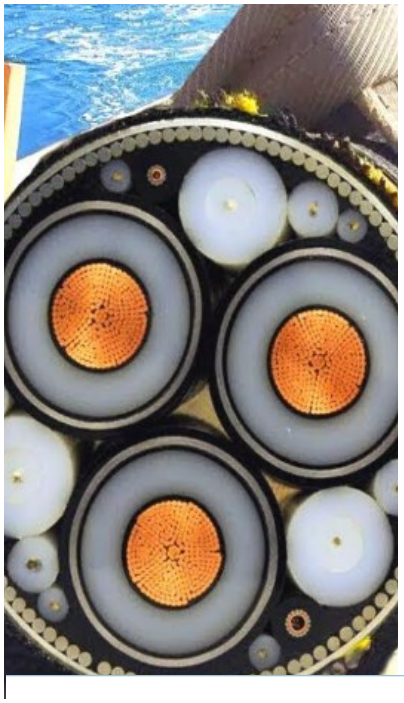
The primary concern in this changing environment involves an erosion of the rule of law. While these kinds of events may be difficult to prove to the standard of criminal courts (i.e., beyond a reasonable doubt), the willingness of state actors to abandon their responsibilities under the UNCLOS to facilitate state-sponsored action should be a troubling development for seafarers of all nationalities.

UNCLOS, while not perfect, provides a necessary framework that helps protect seafarers. It reduces their vulnerability to arbitrary or unnecessary state actions or even arbitrary detention. If state actors, particularly those that are signatories to UNCLOS, continue on this course, the consequences of those decisions may be wide reaching.

Inside this issue

Special points of interest

- The Association would like to welcome a new player in the Maritime Security domain in Canada. The National Centre of Excellence and Innovation in Maritime Security can be found at https://marseccoe.com.



Events of Note

As discussed in a previous version of this newsletter, we continue to see commercial shipping drawn into various conflicts. This blurring of the lines may pose significant challenges for the sailors on board these vessels that suddenly become pawns in international conflicts or where ships become targets.

The potential use of commercial ships to damage undersea cables bring them perilously close to becoming an active member of the conflict. Should it be proven that civilian companies or vessels were actually involved in taking direction from a state actor to further the conflict, it will likely result in a host of questions for the applicable courts and insurers of those vessels.

While the use of civilian fleets is nothing new, particularly in the South China Sea where there is very little except a blurred and porous line between state control and commercial fleets for some countries, approaching a norm.

In addition to the cables damaged in the Baltic Sea, Taiwan has now reported that it detained a China-backed cargo ship in a similar incident.

These incidents have spurred on the development of remotely operated vehicles (ROV) and Undersea Autonomous Vehicles (UAV) intended to monitor and respond to incidents involving undersea cables.

One of the key lessons being learned with undersea infrastructure is that the need to protect this infrastructure will accelerate research to free up high-value resources currently committed to protecting it.

Situational Awareness

Organizations need to ask themselves five key questions:

1. What do I have and what am I doing?
2. What am I lacking and what am I not doing?
3. What are my threats doing or moving towards?
4. What are my threats not doing or moving away from?
5. Am I maintaining the ability to answer these four questions based on reliable and credible information?

These questions look at operations, infrastructure, and personnel. They need to be part of the overall continuous monitoring structure,

Incoming Rules—the Arctic

Continued on Page 6…

The Polar Code includes a range of mandatory measures that cover safety and pollution prevention considerations. What we need to understand is that this Code is intended to supplement the various International Maritime Organization (IMO) instruments, such as the United Nations Convention on the Laws of the Sea (UNCLOS).

Currently, 14 states are reported to have neither signed nor ratified the UNCLOS, including the United States of America (USA). Of the 168 countries that have signed it, it is noteworthy that the USA is the only Arctic nation that has not.

The USA, however, does follow most of its principles as a matter of customary law and has participated in many of the forums tied to UNCLOS with relation to the Arctic and actually participates in the Arctic governance activities through the Arctic Council.

While the UN Polar Code covers a range of different circumstances, there is a need to go beyond the safety and environmental protection of the northern environments.

Later in March 2025, the Arctic Council will be holding the *Arctic Emergency Management Conference* (18 –20 March) under the leadership of the Emergency Prevention, Preparedness, and Response Working Group of the Council.

The EPRR focuses its activities through a number of different working groups. These are listed on their page (see link) and include issues such as Search and Rescue (SAR), environmental response, and radiation. For those looking for resources on their various policies, standards, and methodologies, they are included on the page.

While the UNCLOS might be argued as being largely adhered to (despite the lack of signature and ratification from the USA), we can move onto the Polar Code and its requirements. We need to be careful at this point in that the Polar Code does not cover port facilities, but focuses on the goal of providing for "safe ship operation and the protection of the polar environment." This is largely accomplished through each ship developing a Polar Waters Operating Manual PWOM).

Control Design

Continued on page 5.

Security controls include those "actions, devices, procedures, techniques, or other measures that reduce" the vulnerabilities within a system. (NIST CRSC-2). They can be described in terms of measures that accomplish any one or more of the following:

- Protecting the system against unauthorized acts or conditions that can lead to disclosure, modification, loss, or disruption.
- Detecting unauthorized, suspect, anomalous, or similar activities or conditions that could impact the system (from external sources, internal to the system, or the system's infrastructure itself).
- Responding in terms of taking steps to contain, isolate, and/or remediate either (or both) the impacts or the detected act or condition.
- Recovering infrastructure or services so that the system is gradually able to deliver critical, desired, then anticipated services in a reasonably trustworthy operating state.

These controls may be either technical or non-technical in nature. Technical controls may involve (but should not be considered limited to) features of design, configurations, or added security measures that accomplish the above. For example, a configuration that prohibits the connection of unauthorized devices or only allows the connection of authorized devices to the system. Non-technical controls often involve factors such as governance (policies, standards, etc.), training (awareness, technical), and work processes that support the system's ability to maintain a trusted operating state.

Certain controls may be *prescribed* or required as part of a regulation or certification. In this context, the security control will be either *performance-based* (achieves an outcome) or *prescriptive* (strictly defined). In the case of the latter, the focus shifts to the complete and correct implementation of the control. Note that this does not mean that you do not check to see if the control could adversely impact critical (including safety critical) systems. Performance-based controls follow a similar structure as described below.

Our first step involves understanding the goal of the security control. This may be described in documentation but should be understood in three contexts. The first, and most obvious, is how the goal (and control) affects the system itself. The second is how it relates to higher systems that it needs to interact with. The third involves if the goal is something that needs to be passed down to sub-systems.

A goal is generally aspirational. It may be expressed in terms of a "secure" or "trustworthy" state. It done this way, you will have to spend some time to understand what that "secure" or "trustworthy" state looks like. What are its characteristics?

The Scope

Several debates continue to rage between technical and non-technical parties about which is more important in the cybersecurity space. This argument is a waste of time. Both have their place. The gap here is that organizations need to understand the scope of cybersecurity and then ensure that the persons performing certain tasks are actually capable of performing those tasks.

For those that would continue this debate, the NIST Computer Security Resource Center has put in place the CPRT or Cybersecurity and Privacy Reference Tool. The listing of controls just on the home page is more than enough to illustrate that cybersecurity has both technical and non-technical aspects to it.

The second aspect of this involves ensuring that the control (specific measure) is not actually present but is actually implemented completely and appropriately. I can argue that I own a deadbolt for my front door and therefore my door is securable, but if I don't actually install and use that deadbolt than it is of little value.

This raises the concept of the depth of whatever review is being undertaken. While one might "check the boxes" to show that all controls are present, this gives little assurance that the organization is secure.

For this reason, it should not be enough to simply have a certificate that states that all controls were present. Any certificate should be backed by a report from the certifying body that describes who performed the work and to what extent the controls were actually evaluated.

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.

Vulnerabilities

Having identified the assets involved on the ship or in port, assessed their criticality, and developed an understanding of threats, we need to consider the vulnerabilities in the system.

In this context, we are looking at vulnerability in the context of a weakness that can be exploited or triggered by a threat. (Ref NIST CRSC-1) Understanding that threats exploit vulnerabilities to cause injury to assets, the impacts of those losses resulting in risk to the organization provides a framework.

Vulnerabilities come into being many ways. Some are the result of design that has overemphasized functionality to the point that the owner/operator is placed at a level of security risk. Some are the result of misconfigurations or other steps that have left openings, such as failing to ensure that only authorized devices can connect to networks. Some result from changes in technology on both the legitimate operations or threat side of the issue. These generally make up technical vulnerabilities or those that apply to software, firmware, or hardware.

In these cases, those addressing technical vulnerabilities may be well-served by programs such as the CVE Program. Several government programs publish information regarding vulnerabilities, such as the Cybersecurity and Infrastructure Security Agency, Canadian Centre for Cyber Security, as well as others.

Within the realm of technical vulnerabilities, we need to be cognization of unique threats within the realm of operational technology. This is a more difficult research effort as the number of non-commercial databases that publish this kind of information is limited. What often occurs is having to have an individual or team with appropriate education, skills, and experience examine the systems for common issues.

For those that need to understand the issues surrounding OT, there are often bulletins and reports published that discuss the different kind of vulnerabilities. Both the USA and Canadian agencies listed above include OT reports within their guidance material. Further, certain laboratories will publish reports that can provide the starting point for more detailed examination. (link to example report)

These technical vulnerabilities can be addressed in a relatively straight forward process:

- Identify the potential vulnerability.
- Identify its potential location or applicability within the system.
- Identify safety constraints (and other constraints) that need to be addressed if examining the system.
- Ensure that you have a "restore point" or something similar if things go wrong.
- Examine the system.
- Examine the "patch" or "fix" and its potential impacts on the system as well as the enabling systems. (you don't want to crash the system because of the patch)..
- After testing, apply the patch. This will usually be done at a time or in a manner that limits the potential impacts that the patch would have on the organization.
- Monitor the patch's functionality in terms of fixing the issue but also on other aspects of the system's stability.

Taking this approach reduces, but does not eliminate, risk. Care should be taken to understand the specific network environment, threat environment, impacts, and other requirements of the system under examination.

Vulnerabilities do not have to be technical in nature. They can be non-technical. These often appear in terms of missing, incomplete, misapplied, or even outdated policies, poorly crafted plans, unmanaged procedures, and so on.

These non-technical vulnerabilities can have three major impacts. A lack of formal delegation and requirements for formally delegated persons can lead to losses of control in technical domains such as system configuration and non-technical domains such as change management, access control, and others. Poorly crafted or outdated policies, plans, procedures, or other documents can lead to a lack of coordinated response , delays in that response, or an inability to maintain capacities.

Those looking towards identifying vulnerabilities need to pay attention to both domains.

Control Design

Continued from Page 3

Consider a "trusted space." One part of this may involve ensuring that all persons in the space have been authorized, are appropriately background checked, and are subject to enforceable rules of conduct. We can use that understanding to tailor our controls to ensuring that there is an appropriate authorization process, an appropriate background screening process, and finally a set of accepted rules for people to follow. These are the high level controls that can broken down into their various parts until you have specific steps to implement.

It is not just enough to have a control. A control should be part of a living system and that infers the need for it to be managed. Those familiar with capability maturity models, will not that this places an organization's needs fairly far up the maturity model (past the ad hoc, repeatable, or documented levels depending on the model used).

So, for the control, it needs to include aspects of governance (Who owns it? Who can change it?), and how it integrates into routines such as change management and configuration management. What we are looking for here is how the control becomes part of that adaptive or continuously learning effort that keeps the system protected as operating, threat, and infrastructure environments evolve.

Security Controls should be destined with an understanding of what they intend to accomplish, how that contributes to security, and how they can be both monitored and managed.

Finally, we need to be able to monitor the performance of the control. This comes in two parts—its infrastructure and its performance. The infrastructure aspect is relatively straight forward. It involves ensuring the equipment is performing within acceptable thresholds and can communicate effectively with whatever it needs to send information to.

On the performance front, we return back to the security goals. What threshold needs to be met for us to accept that the control is functioning? Consider our access control or trustworthy space issue. Ideally we might say that all persons should meet the criteria and that no person within the space would be found not to meet the criteria (proving both gives a greater assurance that the goal is being met). But at what threshold do we begin to state that the system is not functioning appropriately? This is a more nuanced question. For example, if we find someone coming up the gangway that doesn't meet one of these criteria, is it a full-blown failure or something else?

And this raises the second level of the control. What do we do when we detect a failure in the control? Outside of how do we detect it, how do we respond to the new conditions and how to we recover back into that trusted state. This can be tied to layers of defense or contingency planning. What is important is that as the control is being designed, there is some understanding of how to handle this.

Our final consideration in the design is what we are addressing about the vulnerability. Are we addressing the impact of the vulnerability or the likelihood that it can be exploited? More often than not, we will begin with the likelihood of it being exploited because our overall security posture may focus on protection from attack or prevention of attack. For example, we may establish procedures that limit the ability to bypass the control.

This operates the same way when looking at logical systems. The specific measures may not be the same, but the considerations made in the design of the control and what we are attempting to accomplish are very similar.

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.

Incoming Rules—The Arctic

Continued from Page 2

While the ship operations are important, we also need to remain cognizant of the port or facility-based operations. This working group currently falls under leadership of Russia that has been involved in massive infrastructure projects in the far north.

This aspect tends to focus on the industrial and environmental safety associated with the oil and gas industry and the movement of those products.

As we look at the concepts of Emergency Management (mitigation, preparation, response, and recovery), there are aspects that may warrant additional attention to bring them up to levels comparable with southern climes.

The first of these involves the treatment of seafarers and special provisions that may be needed in the north. This requirement stems from three unique operating conditions in the north. First, while many southern climes are survivable, northern climes (particularly in winter) are far less so. In fact, they may be considered hostile in some locations. The first requirement, therefore, focuses on the need for Arctic states to consider plans on how to house (temporarily) seafarers that have had to be put ashore or that were brought ashore under conditions provided in the code. From the security impact perspective, this moves beyond simply having infrastructure available, but also looks to the movement of persons that may, or may not, have gone through processes such as customs clearances.

Our second condition involves ensuring that the conditions under which seafarers are housed takes into account their ability to be removed from the area. The challenge here is the relatively limited transportation network in the far north. In this context, discussions that involve adjustments (if any) to immigration and customs laws that would allow for a seafarer to be brought back to where they could be repatriated or taken to the ship's next port of call may want to be considered as part of this regime.

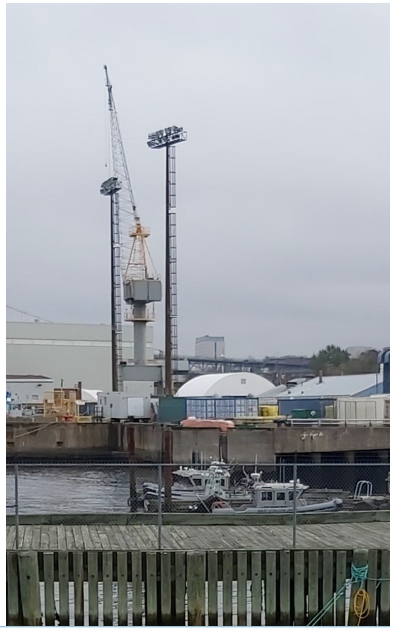
This brings up the challenge of abandoned seafarers. The International Transport Workers' Federation (ITF) had reported an 87% increase in the number of abandoned seafarers in 2024 (3,133) from 2023 (1,676).

Ensuring that sailors are protected against these conditions may well take two parts. The first would involve specific criminal charges brought against the company for the abandonment of the seafarer under those conditions, including provisions for those making the decisions to be held personally accountable. The second involves creating an obligation on the state to assist in the repatriation or safe movement of the seafarer as a last resort and to be accomplished within a set time frame. The state's costs in this effort would then be recovered from the company through customary enforcement measures.

The final aspect involves the guidance for nations with respect to the maintenance of resources in the north that would constitute an acceptable level of search and rescue, environmental response, medical services, and inspection/investigatory services. The reason for this is to provide impetus to the various members of the Arctic states to maintain an appropriate level of services in support of their claims of appropriate care and control over their territory.

With the gradual opening of Arctic shipping, these considerations should be considered prior to the opening of legitimate shipping routes.

Monitoring and Compliance-Automation



As we move into more a more detailed understanding of security for both ships and facilities, we need to be cognizant of some of the challenges that may arise. In this context, consider the challenges associated with the balancing of automation of controls and safety.

At this point, there may be a hue and cry because safety is considered sacred territory (rightfully) in the maritime space. But this is where the nuance comes in.

The case for automation generally involves any one or more of the following:

- Improved chances of stopping the attack as response can be near-instantaneous.
- Improved efficiency in terms of managing the control and enhanced assurance that the control will function as intended.
- Reduction of human error or better consistency in the application of processes.

Before rushing off to automate anything, our first step must involve understanding both what the goal accomplishes and how it impacts the system.

Automation may be beneficial in some cases, but needs to be applied judiciously and with an eye to both direct and indirect safety-related impacts.

Those considering automation should consider three levels. First, consider the benefits or risks of automation with respect to actually disrupting an attack on the system. Is it necessary to automate because people cannot respond quickly enough or there aren't enough resources to monitor the control? Other factors may arise as well.

Second, consider the likelihood that the automated response impacts safety-related systems. If the control is triggered, what are the possibilities (or probabilities) that a safety critical system is impacted? You want to avoid disrupting these for obvious reasons.

Third, consider what could happen if the automation is used against you. For example, if an attacker was able to determine that your control was automated, could that attacker then trigger the control to disrupt your systems or services? This would apply most where the control itself had some adverse impact on the ship. It may also apply to a condition where the control was applied but the ability to remove the control was disrupted.

This doesn't mean that certain controls shouldn't be automated. Quite the opposite. It only infers that when we consider automating certain things that we do so with a fulsome understanding of what that means beyond the simple impacts of reduced manpower and faster response.

If we are looking at automation, we need to also consider how that control is monitored on three aspects.

Our first aspect involves the functionality of the control, both in terms of performance but also in terms of communications regarding its state. How do we know that the control is functioning appropriately? A lack of reports of incidents may indicate that it is but it can also be attributed to failures in communications. Our first element, therefore is ensuring that we can monitor the control's "health" and monitor any changes in its known operating state.

Our second element involves the configuration of the control. If the control is automated, we may be assuming that the control is operating in a trusted state. How do we know that this has not changed? How do we know that it has not *been changed*? For each instance of change, we should be able to see who made the change, what was the change, and that they had the authority/authorization to make the change.

Our third aspect of monitoring involves the actions taken by the control. This relates to why we put the control in place. When did the control become active, what triggered the control, how long was it in place for, and when did it cease? This needs to be in granular enough detail to support operations but also investigations that may be attempting to determine timelines and events.

Finally, each aspect of this needs to be uniquely identifiable. This goes beyond usernames, logins, and so forth. When dealing with automation, we need a trustworthy time stamp for start and stop, specific identifiers for what was done (such as what services or processes were involved) and what specific services or infrastructure was affected. Failing to uniquely identify these will simply complicate post-incident investigation.

Taking these steps (ensuring you do your own due diligence to cover off unique conditions) may help ensure that you balance automation and safety appropriately.

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) and related issues in maritime security that seek to build capacity. It is not intended as a political forum and is strictly intended to be informative.

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