International Association of Maritime Security Professionals

31 December 2024
Volume 2, Issue 6

Wavefront

2024 in Review / 2025 on the RADAR

The past year has been particularly challenging within the maritime security space. Increasing global instability, the evolution in the complexity of cybersecurity threats, and other challenges have posed significant challenges for many within the space.

Concurrently, new regulations have started to take form. Evolutions in terms of traditional port, ship, and company security have started to take form. Formalized cyber security requirements have been outlined for some nations in terms of port security and ship security while the International Association of Classification Societies (IACS) have put forward new universal requirements for those in the shipbuilding industry.

Finally, we have seen the inevitable movement of organizations and companies as many position themselves to reap the benefit of these new challenges. 025 on the RADAR

For 2025, we are watching several trends.

Political instability continues to grow in certain regions, with maritime shipping being caught in the crossfire in a number of conflicts. The Gulf of Aden, Red Sea, Taiwan, and South China Seas will continue to see activity that will make maritime security more complex.

Shadow fleets have become more evident. Sanctions such as those placed on Russia and North Korea will challenge regulatory regimes. In this context, the gradual divergence of political views and groups may begin to pose more obvious challenges to various regulatory regimes, including the various MOU.

Climate change and the shifting natural resources, including fish stocks, will likely bring new pressures. This can be extended to issues such as the opening of Arctic sea routes, the rise in foreign fishing fleets, and the continued challenges of human migration.

Finally, cyber security will continue to pose challenges as we anticipate that certain nations and organizations will continue to use criminal proxy groups to attempt to build access or even disrupt critical services, such as transportation and energy. Additional, traditional cyber crime (ransomware, etc.) shows little sign o decreasing.

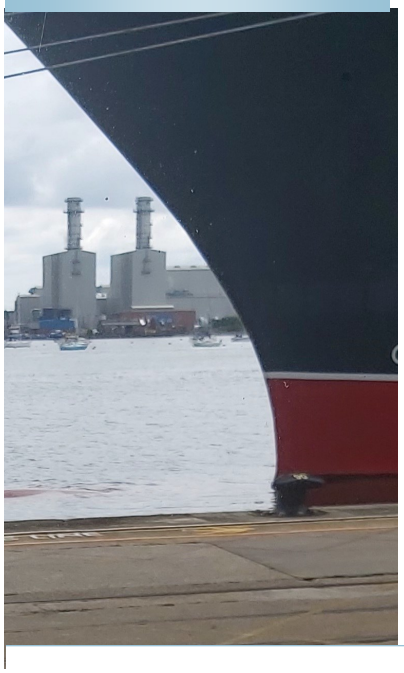
While we see 2025 being another challenging year, the increased focus of attention and growing understanding of the challenges does offer some comfort as we move ahead.

Inside this issue

On the RADAR.....1
Criticality 2,6
Climate and Severe Weather 4
2025 Geopolitical.....3,5
Cyber Regimes 7

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.



Criticality, Consequence, and Reliability

The concept of criticality helps build an understanding of just how important something is to your ability to perform a task or maintain a condition. What happens if the input or service (including work) fails to deliver as expected? What happens if it fails completely? Is there an impact on performance if it fails to meet any specific performance-related thresholds?

Building on the October's issue discussion on operations and design, criticality helps prioritize the contributions of people, assets, spaces, information (including data), and supporting services as part of an overarching understanding of operations.

So why is this important in maritime security? The answer is relatively simple.

Best practices may guide an organization on what step to take, but should be looked at in terms of if they align well with the critical aspects of your operations. Three situations present themselves.

First, does something need to be removed from the best practice in your context because it poses an unacceptable level of risk (such as a life safety risk.)?

Second, does something need to be changed for the same reason?

Finally, is there something you are doing that may require you to move beyond the best practices?

Criticality is useful in that it can help you align your operations and infrastructure with the best practices that will likely appear in 2025.

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,

Building Upon the NIST Approach

Continued on Page 6…

NIST Online Glossary (Ref A) defines criticality along two major lines. First, there is the "measure of the degree to which an organization depends on the information or information system for the success of a mission or a business function." This is as identified above and can be extended to the contributions of people, assets (infrastructure), spaces, information (including data), and supporting services that are brought together and managed for some pre-ordained result. This aligns more closely with the Systems Engineering approach described in NIST SP 800-160 Vol 2 Revision 1.

This can be closely aligned with (but should not be confused with) the approach that "refers to the (consequences of) incorrect behaviour of a system. The more serious the expected direct and indirect effects of incorrect behaviour, the higher the criticality level."

These questions may parallel each other but are not completely aligned. The first approach is limited that by once the mission fails, there are no further consequences to consider. In brief, it is internally focused with a natural limit of "0-performance" being a hard threshold to breach. The second approach, however, looks at the potential impacts that may result because of the failure of the organization's ability to deliver something or maintain a condition. The scoping of these impacts can be difficult and may be influenced by subjective arguments or claims.

From one engineering viewpoint, this is a question that operates at different system levels. Where the loss of the function impacts both the organization and those outside of the organization, the issue operates at one level higher than the system design itself. For these kinds of events, the approach using consequences can be argued as being appropriate because we are working to protect those around the organization. We can use structures such as the categorization structure in IACS UR E22 associated with life-safety (Categories 1, 2, and 3).We can further refine this by using guidance like the expanded injury tables that come with some national risk assessments. Ultimately, the focus is on ensuring that the work itself proposed by the company (or organization) does not adversely or inappropriately impact those around it.

The 2025 Geopolitical Environment

.For those involved in risk assessment or planning, the 2025 maritime security threat environment looks challenging. First, the threat environment will exhibit a broad range of threats that range across the natural and deliberate. Second, the threat environment will not only possess a broad range of threat actors but the divisions between threat actors will remain blurry. Finally, threats will continue to evolve with the operating, regulatory, and infrastructure environments.

BRIC vs "The West"

We continue to see a relative division between Western / NATO interests and those of the BRIC. As we continue to see the BRIC we can expect to see a number of key shifts. The rise of BRIC will begin to have a more significant impact on global maritime governance, particularly as the interests between the two groups diverge.

The second aspect of this involves the rise of an increasing capability to rival what has traditionally been the role of the United States Navy or NATO. Exercises in 2024 between various members are beginning to demonstrate that we may well need to see the maritime security space (and not just the geopolitical space) as having a multipolar aspect to it.

Finally, the rise of BRIC is likely to lead to increased challenges in terms of world governance. While the IMO has traditionally had a global outlook, it has been significantly influenced by Western perspectives. As China continues on the Standards 2035 approach, we will likely see the traditional source of standards (such as NIST) being challenged by the sheer level of energy that China can bring to this activity. (Ref F)

The rise in the prominence of BRIC (as compared to the West) will likely manifest itself in two ways. The first, as noted above, involves an increased involvement in the overarching international bodies and attempts to exert influence in those bodies.

The second, however, involves an increased willingness on the part of BRIC to either avoid or disregard the current global structure where those global structures are seen as not paying appropriate homage to BRIC's interests. 2024 (and earlier) has seen manifestations of this with the various shadow fleets operating to avoid sanctions and other measures. We can expect to see this trend continue as competition between the different views increases.

The Changing Face of War

Conflicts in various parts of the world continue to shape, if not change, how we need to look at conflict. Like the tanker wars (Iran and Iraq in the 1980's), we see commercial shipping suddenly become both a target and, arguably or allegedly, a tool within the conflict. The attacks on commercial shipping in the Red Sea / Gulf of Aden area have seen non-state actors using missiles, drones, even helicopter borne assaults.

Continued on page 5..

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.

Climate Change / Severe Weather

Storms

Climate change and severe weather will likely play a significant role in maritime security. These will include the direct impacts associated with severe weather, increasing sea temperatures, and similar factors. It will also manifest itself in indirect impacts, such as the increased migration of people, fish stocks, and the opening of new areas for exploitation.

While Atlantic Canada was spared much of the hurricane season, the southern USA and Europe were not so fortunate. While hurricane Helene (a category 4 storm) received most of the attention, southern USA ports faced disruptions each month of the season with Debby (August), Helene (September), Kirk (September) Isaac (October), and Joyce (November),

What was more telling, however, were the impacts of several storms that crossed the Atlantic and impacted parts of Europe, including the UK, Spain, France, and Portugal. Fed by warmer sea temperatures, these storms created significant challenges in terms of winds along the coast and inland flooding.

The core element associated with these storms involves the need to look at our models when recovering from these events. Rebuilding better (to suit the new environment) is still something meeting resistance in certain circles even if it is intended to mitigate the effects of future storms.

Migration of Fish Stocks

Fish stocks seeking cooler waters have shown trends that include movement towards the poles but also deeper migrations. Rising sea temperatures, aspects of increased ocean acidification, and other factors spur these migrations.

These migrations become important for two reasons. First, many of the conservation treaties rely on geographic areas that the fish may move out of. This may lead to increases by certain nations with respect to their IUU fishing practices.

As these fleets follow the fish stocks. We can expect to see increased marine safety and environmental issues. Should these fleets move northward (not necessarily into the Arctic per se but into northern waters, we can expect to see new challenges in terms of vessel tracking, potential conflict with established fishing communities in the area, and other similar kinds of events.

Human Migration

This challenge is not actually emerging but may intensity. While there are several legitimate routes taken by those leaving countries in strife (etc.), we can expect to see criminal networks continue to exploit sea routes and migration.

Of note is that we've also seen a shifting in the response to these criminal activities. While nation states have, in some cases, taken a harder stance and closed their borders to illegal migration of this type, we see a corresponding rise in the number of organizations that appear to be willing to assist the migrants.

Activism

Certain shifts in activism have been noteworthy over the past year. One of these has included (largely in the west), linkages between different causes, notably with the Palestine movement.

These "combined protests" create conditions where dialogue is nearly impossible as the protests often lack clear or accountable leadership and the broad spectrum of topics being covered make it difficult to present any entity that can respond to the issues.

One current theory is that the protest, being relatively photogenic in nature and being a good focal point for a cause, is also being aided by a sense that citizens demand more from their governments. Others promote a view that these protests can form as a result of coordination through social media .

This raises the third aspect of many of these protests. Many do not appear to focus achieving any change in a particular direction (such as constructive policies) but rather on a rejection of the status quo (similar to antipolitics).

Within the context of climate change, we can expect to see protests continue at sea ports, fueling points, and other locations that can be tied to the climate change cause. The relative lack of forward motion and the growing dissatisfaction within the "ban fossil fuels" movements are likely to continue posing challenges for port security and those working in supporting infrastructures.

2025—Geopolitical / Higher Level Threats

Continued from Page 2

.The second aspect in the changing face of conflict involves a combination of who is involved in the conflict and the level of intensity involved. Warfare by proxy (criminal or legitimate) is on the rise with alleged acts of "sabotage" being on the rise. Acts of sabotage against certain industries and against remote underwater infrastructure is murky enough that final (unequivocable) attribution is difficult. Where the actions are difficult to conceal or where counter-narratives cannot be presented, the use of proxies and even criminal groups is on the rise. The lack of clarity may increase tensions between major parties but will not likely lead to any significant resolution.

Finally, the geopolitical aspects of conflict are likely to spread capabilities thinner. The challenge here is that the war in Ukraine has led to an understanding that while Ukraine's supporters' capabilities may be stretched now, that condition may be temporary. (Ref F) This may become even more evident should NATO's leadership achieve its aim of mobilizing its member nations to "gird up for conflict."

Currently western powers are at a production disadvantage in terms of naval forces and similar large-scale military assets. This may be a temporary condition. This may well create a window within which competing powers decide that they need to act.

Consider the nature of shipbuilding. China's capacity to produce larger ocean-going vessels (necessary given the direction of trade), has been estimated as being over 230 times that of the USA. (Ref G) While this has obvious commercial implications, it can also have military or naval impacts.

This is tied to the ability to produce naval assets . China's naval buildup should not just be looked at in terms of numbers of ships. The ability to produce new ships (to replace those lost), crew those ships, or repair damaged ships all play a significant role in a nation's ability to project power. (Ref H) Currently, the USA and other NATO powers are lagging in this respect.

Beneath the traditional capital ships, we need to look at the rise of smaller, less expensive technologies that are proving a threat to those assets. Returning to the Russia-Ukraine conflict, the rise in the use of drones has demonstrated how reasonably inexpensive drones can be used to counter significant strategic assets (to the fleet level).

The rise of this technology will impact the ship design process as defending against this kind of technology, or even swarms of this kind of technology, will become increasingly important.

Defending against swarms of smaller vessels is not novel. Those operating in the Strait of Hormuz have had to contend with the Iranian Revolutionary Guard Corps (IRGC)'s use of small boat tactics swarming larger ships. (Ref I)

2025 may see this approach, however, enhanced through the use of sensing technology and Artificial Intelligence. The intent of those systems would be to present a swarm that requires the maximum level of effort by those defending to identify, assess, and engage the incoming members of the swarm.

This, in turn, may force the need for the increased use of technology as part of defensive tools. Remotely operated defensive pods, the use of AI to prioritize targets, and novel forms of munitions (area affect versus point specific) may well surface.

Below this level, we will continue to see the use of the proxies and others to harass and committed lower levels of attacks against shipping, both commercial and military.

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.

Criticality

Continued from Page 2

Criticism has been growing of late that many designs fail to pay appropriate attention to this level of assessment. Arguments are being put forward in some circles that those involved in the management of organizations and the design of their services need to be held more personally accountable for this kind of impact.

This aligns rather quickly with the values and ethics of many professional engineering societies that look to their members ensuring that their "clients and employers are made aware of societal and environmental consequences of actions or projects." (Ref B) Others may pertain.

In brief, those involved in formal engineering processes will need to ensure that they are acting both in good faith and with due care with respect to the impacts of their work.

This level of question should be addressed when looking at the Business Impact portion that sets the stage for identifying stakeholder and then system requirements.

System Criticality

The criticality of the system having been identified, we need to identify if there are certain aspects of that work that are more critical than others

In this approach, we can use models such as those provided by NISTIR 8179 (Ref D) This approach breaks the work into progressively smaller or more refined inputs to identify those pieces that cannot be done without.

Consider the movement of containers within a container handling facility. In that context, the movement of the container so that it arrives at the right location at the right time in acceptable condition and for reasonable cost is the overarching mission of the organization. We want the right container placed on the right spot on the ship so that it proceeds appropriately along the route.

This example raises an important point—that a system or process may have multiple inputs that are "critical." For example, we may not be able to load the container at all without an overhead gantry crane (or equivalent). We may not be able to identify the container if we lose the data that identifies which container needs to be moved at all. Each should be looked at individually with criticality used as an attribute or descriptor of the input and not rushed into prioritized lists (that may come later).

Criticality versus Reliability

While many of us are familiar with the security attributes of *confidentiality, integrity, and availability*, a fourth has been promoted—that of reliability.

Reliability, unlike criticality, looks towards "the ability of a system or component to function under stated conditions for a specified period of time." (Ref E) It can also be looked at in terms of the "probability of performing a specified function without failure under given conditions for a period of time." (Ref E).

Adding Context

It should also be clear that the consequences associated with work may not be constant in all cases. Consider the movement of a container of relatively innocuous items (kitchen appliances or something similar) as compared to a shipment of dangerous goods (such as explosives or uranium hexafluoride). The consequences of the shipment going awry are not the same across all three cases .

The criticality of the infrastructure, assets (including data), and people doing work does not change. The higher-level process is the same for each of the movements (less some of the confirmations).

As we look at reliability, we see this tied to both the internal and external level. Externally, the reliability of the work to only allow the appropriate movements and not to create undue risks links into aspects like public safety. At the work process level, the concept of reliability can be linked to the various performance thresholds that need to be maintained by the organization as an aspect of both efficiency (no wasted efforts) and viability (in terms of maximizing returns for effort).

This admittedly pedantic approach is important because of the complexity of design processes and the level of expected refinement. While there will be temptation to create new concepts and vocabulary (as some do to promote the "uniqueness" of their services, we need to be cautious that we are keeping these contexts clear.

Cyber Regimes

Cyber threats are likely to continue in terms of their capability as well as their pervasiveness. In this context, any deliberate action taken to reduce the operational effectiveness or degrade one of the security attributes (confidentiality, integrity, or availability) is being looked at in terms of a threat.

First, criminal activities are likely to continue expanding over 2025. While some reports peg the potential losses to cybercrime at around 8 trillion USD in 2023, it is expected to top 10.5 trillion USD in 2025. While the United Nations General Assembly adopted the UN Convention against Cybercrime on 24 December 2024, the rising presence of criminal services on the dark web, evolving attack technologies, and the willingness of state actors to use criminal groups acting against infrastructure with relative impunity will continue to challenge organizations. (Ref J)

Part of the challenge that 2025 will likely reveal is if these multilateral approaches have the necessary teeth to dissuade signatory countries from simply ignoring or refusing to participate in actions that those nations feel are against their interests.

While our reliance on cyber technology grows, we must ask if the codes or standards being used to guide the development or innovation in that space are paying adequate attention to ensuring that security is treated appropriately.

This is particularly evident in the Maritime Autonomous Surface Shipping (MASS) considerations that continues to operate under an non-mandatory Code of Practice. Given that the UN IMO is not expecting to commence development of the mandatory MASS code until 2028 (largely based on the current non-mandatory code), we are not likely to see a MASS Code come into force until 2030-2032. (Ref K)

This raises an existing question about the pace at which regulatory development can proceed when compared to the pace of innovation. The gap between the two is clearly evident. What is not evident, however, is any action being taken by the IMO or similar national bodies to place due diligence controls into the MASS space or any reinforcing messages by the various colleges of engineers involved to remind their members of public safety or similar issues that need to be addressed.

Added into this challenge, however, are regimes coming into force in North America, such as the CMMC 2.0 and Canadian Program Cybersecurity Certification (CPCSC) that focus on defense contracting. These regimes, largely based on the NIST SP 800-171 (which Canada will put a Canadian spin on it through ITSP 10.171).

This raises the key challenge for companies when dealing with the cyber security regime in the future. While sound engineering practices can lead to security becoming an emergent property of the system being worked on, companies will face a significant challenge in meeting the various certification requirements associated with different kinds of technologies.

The key here will be to ensure that the certification requirements do not overtake the security requirements associated with sound design. Certification, by definition, is a compliance-related exercise that can quickly drift towards being more about having the certificate than the underpinning work that leads to it.

We see this trend extended beyond North America and into the international space as the maritime industry continues to focus on standards-driven approaches and pressures towards clear (read prescriptive) guidance to minimize the potential disruptions from the certification process.

What we are also failing to see in these regimes are the neutral bodies that can act as a source of verification for the various aspects of certification. While the CMMC 2.0 has the CyberAB community, membership costs in that community are being looked at in terms of bordering on the excessive, if not prohibitive. The question then becomes “if the company has enough to pay the recurring bill—several thousand per year in terms of strict membership costs” as opposed to “is the company both capable and credible.”

This pattern of behaviour for certification bodies, however, is not unusual. Several regimes ranging from human rights to security to safety have started with good intentions to be taken over by administrations that demand high prices for membership if companies want to participate.

Hopefully, the cybersecurity industry learns from these errors.

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