MAST



MAST Risk Report

Expert Perspectives on Emerging Threats

SEPTEMBER 2026

WWW.MAST-SECURITY.COM

Contents

Geopolitical commentary, maritime risk and regulatory analysis from MAST and invited specialists.

01 AI didn't create the risk. We did 3
ANDREW CLARKE MSc FCMI · CEO RECYBER

02 The Drone Threat to Yachts and Maritime Operations 6
JOSEPH HOLDING · DIRECTOR, ELEVATE LH

03 Martyn's Law: what every venue and event organiser needs to know 10
GARY GRANT · BARRISTER

04 Why ship detentions are rarely only about the law 15
PETER ASTBURY · CONTINGENCY RESPONSE CONSULTANT

05 Somali Piracy: A Re-emerging Threat, but Not Yet a Return to 2011 17
PHILLIP CABLE LLM · CEO MAST

AI didn’t create the risk. We did

AI risk and its potential impact on business transactions, with recommended actions for firms.

Andrew Clarke MSc FCMI · CEO Recyber

Recent headlines have focused on an AI model exploiting an unexpected route to achieve its objective during testing. Predictably, the discussion quickly became about whether AI can be trusted – a flawed question that misses the point.

The more pertinent question is whether organisations can trust the way they govern AI.

There is a temptation to view artificial intelligence as something fundamentally different from every other business technology, which it isn’t. AI does not suddenly create risk in isolation – an important and often overlooked point. Rather, it amplifies the consequences of human decisions. It acts within the objectives, permissions and constraints that people define.

In many respects, giving an autonomous AI system broad authority without appropriate governance is a little like giving a child a box of matches and being surprised when the house catches fire. The problem is not the child. Nor, in this case, is it the AI. The problem lies with the person who failed to establish safe operating and working conditions, thereby preventing a foreseeable outcome.

This distinction is important because it changes where organisations should focus their attention.

The real business risk

Much of the public debate centres on the technology itself. Business leaders, however, should be asking a different set of questions.

- Who is authorised to use AI?
- What information is being shared with it?
- What decisions is it permitted to make?
- How are those decisions reviewed?
- What happens when it behaves in an unexpected way?
- Who is ultimately accountable?

These are not technical questions. They are governance questions.

> *Every AI deployment creates a new business process. Every business process creates human decisions. Every human decision creates behavioural risk.*

As organisations increasingly embed AI into procurement, finance, legal services, software development, customer support and operational workflows, the potential impact extends well beyond cybersecurity. AI-generated outputs can influence commercial negotiations, contract terms, regulatory compliance, financial reporting and strategic decision-making.

Poor governance therefore has the potential to affect the integrity of business transactions themselves.

The hidden exposure

Many organisations have invested heavily in technical controls to secure AI platforms, but fewer have considered the behaviours surrounding their use.

Employees may upload commercially sensitive documents into public AI models without understanding the implications; managers may place unwarranted confidence in AI-generated recommendations; developers may grant autonomous agents excessive permissions because it accelerates delivery; and executives may assume AI outputs are authoritative simply because they appear articulate and convincing.

None of these alone represents failures of artificial intelligence - they are examples of human behaviour creating organisational risk.

This is why AI governance cannot be reduced to policies and technical controls alone. Organisations must understand how people interact with AI, what motivates unsafe behaviours and where poor decisions are most likely to occur.

Behaviour is the real control surface

For years, organisations have treated people as the weakest link in cyber security - a mindset that is becoming increasingly outdated. People are not simply a source of risk; they are also the primary control over increasingly autonomous systems.

The quality of AI governance will ultimately depend on human behaviour.

Good governance is therefore not just about restricting AI.

It is about shaping how people use it.

That means establishing clear expectations, measuring risky behaviours, reinforcing good decision-making and intervening early when unsafe practices emerge. The organisations that succeed will be those that treat behavioural risk as something measurable and manageable, rather than assuming awareness alone will change outcomes.

Practical actions for business leaders

Organisations do not need to fear AI, but they should approach it with the same discipline applied to any other critical business capability.

Business leaders should consider five immediate actions:

1. **Define ownership.** Every AI capability should have a clearly accountable business owner, not simply an IT sponsor.
2. **Establish governance boundaries.** Clearly define what AI may access, what decisions it may influence and where human approval remains mandatory.
3. **Measure behavioural risk.** Understand how employees actually use AI rather than relying solely on policy compliance or technical monitoring. Behavioural intelligence provides early indicators of emerging risk before it becomes a business incident.
4. **Review permissions continuously.** As autonomous agents become more capable, permissions should be treated as dynamic rather than permanent.
5. **Create a culture of responsible AI.** Employees should understand not only how to use AI effectively, but when not to use it and when to challenge its outputs.

Looking ahead

Artificial intelligence is not replacing human judgement, but it is increasing the importance of it.

As AI systems become more capable, the organisations that thrive will not necessarily be those with the most advanced technology. They will be those with the strongest governance, the clearest accountability and the best understanding of human behaviour.

Final thought

Ultimately, AI is neither ethical nor unethical. It has no intrinsic understanding of right or wrong. It optimises for the objectives and freedoms it is given.

The responsibility for ensuring those objectives are appropriate, those freedoms are proportionate, and those boundaries are respected has not shifted to machines.

It remains exactly where it has always been.

With us.



Andrew Clarke MSc FCMI

CEO RECYBER

Andrew Clarke MSc FCMI is Chief Executive of Recyber and a former British Army officer, latterly Senior Strategic Security Risk Advisor to the Governor of Bermuda. Recyber works at the point where cyber security meets human behaviour, culture and governance, helping organisations measure and reduce behavioural risk on the basis that security is a human network rather than a perimeter.

MARITIME THREAT OVERVIEW

The Drone Threat to Yachts and Maritime Operations

From surveillance and disruption to direct attack

Joseph Holding · Director, Elevate LH

EXECUTIVE VIEW

Drones give hostile actors a low-cost way to observe, disrupt, expose or attack high-value maritime targets. The immediate concern is not one aircraft type, but a rapidly widening range of threats to people, vessels, ports, offshore assets and commercial continuity.

No Longer Emerging

Drones are no longer a distant or purely military concern for the maritime sector. Uncrewed aerial systems have already been used against international shipping, while small commercial platforms are routinely capable of operating cameras, thermal sensors and useful payloads at ranges that would have seemed exceptional only a few years ago.

The Red Sea has provided the clearest demonstration of the high-end threat. Attacks involving uncrewed aerial systems and other stand-off weapons have endangered crews, damaged vessels and helped force major operators to reconsider established routes. The consequences have extended beyond the ships directly targeted: longer voyages, higher insurance exposure, disrupted schedules and additional pressure on global supply chains.

That is the defining imbalance. A comparatively inexpensive system can impose costs far greater than its own value. It does not need to sink a ship to be effective; it may only need to create credible uncertainty around whether a route, port or vessel can operate safely.

Recent Incidents

Recent events show that the maritime drone threat is already operational rather than theoretical. In December 2023, HMS Diamond intercepted an uncrewed aerial vehicle reported by the UK Government to have been targeting merchant shipping in the Red Sea. During its subsequent deployment, the Royal Navy reported that the destroyer successfully engaged nine drones across three separate attacks.

In June 2024, US Central Command reported that the Liberian-flagged, Greek-owned bulk carrier M/V Transworld Navigator had been struck in a suspected UAS attack. Crew members sustained minor injuries, the vessel suffered moderate damage and continued underway. The incident demonstrated that a drone strike does not need to result in the loss of a ship to create immediate safety, operational and insurance consequences.

The threat is not confined to the Red Sea. In January 2026, two Greek-operated tankers near Russia's Black Sea coast were reportedly struck by drones, prompting Greek authorities to warn shipowners and masters to reassess the risk to vessels operating in the

region. Although the reported damage was limited, the incidents reinforced the geographical spread of the problem and the sensitivity of commercial shipping to conflict-related drone activity.

Publicly confirmed cases involving private yachts remain less common than incidents affecting merchant shipping. However, yachts frequently operate close to shore, ports and public events, where small commercial drones are readily accessible. Their more immediate exposure may therefore be intrusive surveillance, loss of privacy and the collection of information that could support a later security incident.

Increasingly Accessible

The pace of drone development matters, but principally because it is expanding who can generate a meaningful aerial threat. High-quality cameras, longer endurance, automated flight functions, improved communications and greater payload capacity are increasingly available through commercial supply chains. Components and software can be adapted, combined and replaced quickly.

Recent conflicts have compressed development cycles and demonstrated how commercial technology can be repurposed under operational pressure. Techniques that once belonged largely to well-funded state programmes can now be copied or approximated by proxy forces, terrorist organisations, criminal groups and technically capable individuals.

For maritime operators, the threat population is therefore broader than a conventional military adversary. The same platform class may be used innocently for photography or inspection, intrusively for surveillance, criminally to support an operation, or violently as a weapon.

The Threat Spectrum

SURVEILLANCE, PRIVACY AND INTELLIGENCE

A small camera-equipped drone can observe decks, access points, crew routines, security posture and the movement of passengers without placing an operator close to the vessel. Around a superyacht, this may expose a principal, guests or family members, compromise privacy, reveal tender movements or record security arrangements. Around commercial shipping, ports or offshore assets, apparently passive observation may support later theft, protest activity, sabotage, piracy or targeted attack.

The aircraft may cause no immediate damage. The information it collects - and the speed with which that information can be shared - may be the real threat.

HARASSMENT, NUISANCE AND OPERATIONAL DISRUPTION

Persistent or unexplained drone activity can unsettle passengers and crew, interrupt deck or helicopter operations, generate safety concerns and force security teams to divert attention. Near ports, terminals or crowded anchorages, even a non-weaponised drone may create collision concerns or temporary restrictions while its intent is assessed. For a high-profile yacht, repeated overflight can also become a reputational and privacy event long before it becomes a physical-security incident.

CRIMINAL FACILITATION AND PAYLOAD DELIVERY

Drones can extend the reach of criminal actors by scouting an area, tracking a vessel, identifying when security is weakest or moving small items across a perimeter. The maritime environment offers numerous potential launch positions, including shorelines, harbour areas and small craft. Industrial and heavy-lift platforms also illustrate a simple concern: useful commercial payload capacity can be repurposed for harmful delivery.

DIRECT ATTACK

At the most serious end of the spectrum are weaponised drones and one-way attack systems. These may carry an explosive or incendiary payload, approach at low level, attack from several directions or operate alongside missiles and uncrewed surface craft. A successful strike could cause casualties, fire, loss of propulsion or navigation capability, environmental damage and abandonment of the vessel. Even an unsuccessful attack can trigger route

closure, port disruption and significant commercial consequences.

A COMPONENT OF A WIDER OPERATION

The drone should not always be treated as an isolated threat. It may provide live surveillance to people approaching by sea, help select a target, distract a security team, document a protest or attack for propaganda, or operate alongside electronic interference and cyber activity. The important question is not simply what the aircraft is carrying, but what role it plays in the actor's wider intent.

Different Vessels, Different Risks

Superyachts combine high-value assets, prominent individuals, visible leisure activity and operations close to shore. Their most frequent exposure may be intrusive photography or surveillance rather than armed attack, but the consequences can still be serious: loss of privacy, disclosure of location and routines, concern among guests, and intelligence that enables a later criminal act. Risk may rise around high-profile events, politically exposed owners, contentious business interests or voyages near unstable regions.

Commercial vessels are more exposed to strategic disruption. Container ships, tankers and bulk carriers may be targeted because of flag, ownership, cargo, trading relationship or simply their presence within a contested route. A drone incident can threaten crew safety and the vessel itself, but its wider value to an attacker may lie in affecting traffic through a chokepoint or raising the perceived cost of operating in a region.

Ports, terminals and offshore installations present concentrated and often static targets. Drone activity can reveal layouts, observe security measures, approach hazardous areas and interfere with time-sensitive operations. The presence of fuel, chemicals, passenger movements or critical energy infrastructure can amplify the consequences of even a relatively small incident.

The Maritime Challenge

The maritime environment makes threat awareness challenging. Small drones can have limited visual and radar signatures, while sea clutter, birds, weather, vessel movement and existing electronic systems complicate detection and identification. Legitimate drone use for photography, inspection, surveying and emergency response adds a further problem: an aircraft near a vessel is not automatically hostile.

Intent may therefore need to be judged from limited information and in little time. A slow orbit around a yacht, repeated observation of a restricted area and a fast direct approach from open water each create different concerns. If the first warning is a crew member seeing an aircraft at close range, the opportunity to understand what is happening may already be severely reduced.

What Counter-UAS Capability Offers

Counter-UAS should not be understood simply as a means of physically defeating a drone. At a high level, an appropriate capability can offer earlier warning, improve awareness of what is operating around a vessel or site, support assessment of behaviour and provide better information for operational decisions.

That information may allow a yacht to protect privacy and move people away from exposed areas; help a vessel's master alter posture or communicate with authorities; enable a port to manage a temporary safety risk; or provide an evidential record for security, insurance and post-incident review. In higher-threat circumstances, counter-UAS may also contribute to a layered protective response, subject to the legal powers, operating environment and risk involved.

There is no universal maritime solution. A system suitable for a fixed port is not automatically suitable for a moving vessel, and measures lawful in one jurisdiction may be restricted in another. The value lies in matching proportionate capability to the asset, operating pattern and credible threat - not in buying technology on the strength of a controlled demonstration or headline detection range.

Beyond Security

For executives, owners, insurers and security leaders, drone exposure now intersects with crew and passenger safety, privacy, operational resilience, insurance, reputation and commercial continuity. The appropriate level of concern will vary sharply between a Mediterranean charter yacht, a tanker transiting a conflict-affected waterway and an offshore energy site. Treating them as the same problem would be as unhelpful as ignoring the issue altogether.

The immediate requirement is not for every vessel to acquire a sophisticated counter-drone system. It is for organisations to recognise where drones could change their risk, whether existing arrangements would provide useful warning, and whether their response assumptions remain credible as the technology develops.

Drones have altered the economics of maritime surveillance and attack. Their cost is low relative to the assets they can observe, disrupt or damage, and their development is moving faster than many traditional security and procurement cycles. The organisations best placed to manage that risk will be those that understand their specific exposure before an incident makes it obvious.

ELEVATE

Joseph Holding

DIRECTOR, ELEVATE LH

Joseph Holding is a Director of Elevate LH, an engineering-led consultancy working across complex sensor systems, surveillance, systems integration and counter-UAS. Elevate LH possesses the skills and experience to support organisations in understanding operational and security challenges and evaluating proportionate technical and operational responses.

SOURCES & FURTHER READING

- UK Department for Transport, Countering drone threats to shipping, 20 May 2024.
- UK Parliament, Royal Navy: Drone Attacks in the Red Sea, 5 February 2024.
- Royal Navy, HMS Diamond shoots down Houthi missile, 25 April 2024.
- US Central Command, June 23 U.S. Central Command Update, 23 June 2024.
- Reuters, Greece warns shipping fleet of risks after Black Sea drone attacks, 15 January 2026.
- International Maritime Organization, maritime security statements and guidance concerning attacks on international shipping.
- European Commission, Action Plan on Drone and Counter Drone Security, February 2026.

Martyn's Law: what every venue and event organiser needs to know

Gary Grant · Barrister

On 3 April 2025, "Martyn's Law" received Royal Assent. It will, for the first time, place a legal duty on the operators of certain shops, bars, nightclubs, theatres, sports grounds, places of worship, schools and hundreds of thousands of other premises across the UK to plan for the possibility of a terrorist attack. It is formally called the Terrorism (Protection of Premises) Act 2025.

Martyn's Law requires those responsible for certain premises and events to take steps to mitigate the impact of a terrorist attack and reduce harm in the event of a terrorist attack occurring. In addition to this, certain larger premises and events must also take steps to reduce their vulnerability to terrorist attacks.

If you run a venue, provide security, organise events, or advise clients who do, this is a law that needs to be understood. The government has recently published the statutory guidance that explains how it will work in practice, and the clock on preparing for it is already running. It is expected to come into force in Spring 2027. This gap is a planning window, not a grace period to be ignored. Getting procedures right, training staff, and coordinating with other responsible persons at shared or multi-occupancy sites all take time. Organisations that start now will find compliance a manageable extension of what they already do for health and safety and fire safety. Those that wait will be trying to build all of it under regulatory pressure.

The potential consequences for non-compliance are high. They include criminal sanctions and civil penalties of up to £18 million or 5% of a company's worldwide revenue, whichever is higher.

The case for preparation is reinforced by the current threat picture. Since 2017, there have been 15 domestic terror attacks in the UK, and since 2020 police and the security services have disrupted 19 late-stage plots. On 30 April 2026, the UK national terrorism threat level was raised to "Severe", meaning an attack is highly likely; it remains at that level as of August 2026. This continuing threat underlines the need for a practical response.

Who was Martyn?

The law is named after Martyn Hett, one of 22 people killed in the terrorist attack at an Ariana Grande concert at the Manchester Arena in May 2017. His remarkable mother, Figen Murray, turned her grief into a campaign - one that ran for years, gathered cross-party support, and ultimately persuaded Parliament that the public should not have to rely on luck or goodwill to be kept safe at a concert, a shopping centre, or a football match.

The campaign found powerful institutional backing too. In 2019, a report following the 2017 London Bridge and Borough Market attack recommended action to reduce the risk of terrorism at public venues. In 2021, the official inquiry into the Manchester Arena attack went further, recommending that legislation be introduced to improve the safety and security of public venues. Martyn's Law is the government's answer to both.

The basic idea: preparedness, not prediction

The legislation does not ask venues to assess how likely they personally are to be attacked. It assumes, instead, that an attack could happen anywhere, at any type of premises, at any time. Rather than trying to predict where the threat will materialise, the law asks organisations to be ready to respond well if it does.

That's a subtly different - and in some ways more demanding – task than a conventional risk assessment. A quiet suburban café and a packed city-centre arena are, in the eyes of this Act, both potential targets. What differs is not whether they need to think about it, but how much they are required to do about it, which brings us to the heart of the scheme: the two-tier system.

Two tiers: standard and enhanced

Martyn's Law does not treat all premises in the same way. It scales the burden according to how many people are likely to be there.

Standard tier applies to premises where it is reasonable to expect that, from time to time, somewhere between 200 and 799 people (including staff) might be present at the same time. Think of a busy pub or bar, a mid-sized shop during the January sales, a community hall hosting a wedding, or a GP surgery on a hectic morning.

Enhanced tier applies where that figure reaches 800 or more. Arenas, large nightclubs, big supermarkets, shopping centres, major visitor attractions and comparable venues will typically fall here - and so will qualifying events that expect 800 or more attendees, wherever they are held, provided there are measures in place to check who's coming in (for which see below).

The maths matters more than it might first appear. The guidance is clear that "reasonable expectation" does not mean the average day - it means the busiest realistic point. A shop that is usually well under 200 people might tip over that threshold every Black Friday and every January sale; if so, it is in scope, even though most Tuesdays look nothing like that. Conversely, a genuinely unexpected, one-off surge - say, a product going viral overnight and drawing an unplanned crowd – does not automatically pull a venue into a higher tier, provided it wasn't foreseeable and isn't expected to happen again.

There are also some deliberate carve-outs from the strict numbers criteria. Schools, colleges, childcare premises and places of worship are treated as standard tier regardless of how many people they might host - even a cathedral expecting several thousand worshippers for a big occasion stays in the standard, lighter-touch tier. The thinking here is that these settings already operate under other safeguarding and access regimes, and a blanket enhanced-tier obligation would be disproportionate.

What counts as "premises" — and what doesn't

To fall within scope at all, a site has to meet the Act's definition of a "premises": broadly, a building, or a building together with associated land, that is accessible to the public to at least some extent. Crucially, "accessible to the public" still counts even if entry is restricted to people who've paid, hold a ticket, or are members of a club - a private members' bar or a ticketed art gallery is just as much "public" for these purposes as premises with an open door.

The definition is deliberately elastic. A single building, part of a building, or a cluster of buildings under common control - a hospital campus, a university, a hotel-and-spa complex - can all count as one set of premises. A pub with a beer garden, a stately home with grounds, a theme park built around outdoor rides: the "building and other land" together form the premises, and it doesn't matter whether the crowd gathers indoors, outdoors, or both.

Then there's the question of use. Premises only come into scope if they are wholly or mainly used for one of the specific activities listed in Schedule 1 to the Act - a long but finite list running from shops, pubs and

restaurants, through entertainment venues, sports grounds, museums, hotels and places of worship, to healthcare premises, transport hubs, and even household waste recycling centres run by public authorities. If a site's main business is something not on that list - a working factory, say - it stays out of scope, even if it happens to have a small staff shop tucked inside that would, on its own, qualify.

A handful of premises are excluded outright, whatever their footfall: Parliament and the devolved legislatures, most open-air parks and recreation grounds that anyone can wander into freely, and transport hubs like major airports and railway stations that are already subject to separate security legislation.

Events: when a one-off gathering counts

Martyn's Law does not only apply to permanent venues - it also catches "qualifying events", which is where a lot of the practical complexity lives. A music festival in a field, a one-off exhibition in a warehouse, a fundraiser in a village hall: none of these are "premises" with an ongoing Schedule 1 use, but they can still trigger the Act if they meet a set of criteria.

Broadly, an event qualifies if it is held somewhere that isn't already enhanced-tier premises in its own right, it's open to the public (rather than a private wedding or staff party), it's reasonably expected to draw 800 or more people at the same time at some point, and - importantly - there are entry controls in place, such as ticketing, wristbands or membership checks. A free festival with no gate and no way of checking who's coming in and out doesn't meet this criterion, however many people turn up, because there's no meaningful perimeter for the responsible person to secure.

This produces some genuinely interesting edge cases. A marathon that runs largely along open, uncontrolled roads might still have qualifying "islands" within it - a ticketed grandstand, a fenced starting area - each assessed separately. A members' club that normally operates comfortably within the standard tier can find that a single large, ticketed event tips it, or the event itself, into enhanced-tier obligations. And where an event is staged across several premises with different owners and operators - a citywide music weekend spanning venues, pubs and a pop-up stage - responsibility can genuinely fragment, with different responsible persons answerable for different bits of the same event.

Who is actually responsible?

The Act places the legal duty on a "responsible person" - and this is deliberately not a matter of choice or contract. It is the individual, company or organisation with actual control of the premises for the relevant use: usually whoever has physical possession and the practical ability to decide who comes in, stays, or is asked to leave. That is often, but not always, the person who owns the building. A tenant running a pub under lease from a brewery, rather than the brewery itself, is generally the one holding this responsibility, because they are the one in day-to-day control of the premises.

For events, control shifts to whoever has taken charge of the site for the duration of that event - frequently the event organiser rather than the landowner, if a hire agreement has genuinely handed over operational control. Responsibility cannot be outsourced by contract: a venue can delegate the task of, say, writing an evacuation plan to a security consultancy, but the legal responsibility for making sure it happens stays with the responsible person.

Where premises or events involve more than one party with some level of control - a shopping centre operator and the individual shop tenants within it, for example - the Act requires coordination between multiple responsible persons, and cooperation from anyone with a lesser degree of control who isn't the responsible person themselves. In large, multi-occupancy or multi-event scenarios, this is likely to be one of the more time-consuming practical obligations: working out who talks to whom, and agreeing how procedures like lockdown and evacuation will be joined up rather than contradictory.

Where the responsible person for enhanced-tier premises or a qualifying event is an organisation or company, as will often be the case, the Act requires it to designate a senior individual to ensure compliance with the Act's requirements. That individual must have responsibility for managing the organisation's affairs or exercise control over it, rather than being a lower-level employee.

What you actually have to do

This is where the tiered structure earns its keep, because the obligations scale with the size of the crowd.

Everyone in scope - standard and enhanced tier alike - must put in place, so far as is reasonably practicable, appropriate "public protection procedures." These are the four core responses the Act builds around:

- Evacuation - getting people safely away from the premises.
- Invacuation - moving people to a safer place within the premises, rather than out of it (useful where the danger is outside).
- Lockdown - securing the premises to stop anyone entering or leaving, such as locking doors or lowering shutters.
- Communication - making sure people on-site are told what's happening and what to do, where it's safe to tell them.

None of this requires expensive kit. For standard tier premises, the guidance is explicit that the emphasis is on staff awareness, a workable written plan, and the confidence that it can be put into action quickly - not on physical security infrastructure. A written procedure that nobody on shift actually understands or could execute under pressure won't be good enough; the guidance is blunt that plans have to be genuinely deliverable, not just filed away.

Enhanced tier premises and qualifying events face a further, heavier layer. In addition to the four procedures above, they must also consider "public protection measures" - steps addressing monitoring (such as CCTV or staff positioned to spot suspicious activity), movement (managing how people flow through and around the site), physical security (barriers, screening, access control) and the security of sensitive information (such as building plans or event schedules that could help an attacker). Enhanced tier organisations must also produce a formal compliance document, setting out what procedures and measures are in place and explaining how they're expected to reduce risk - and, where they've chosen not to do something an outsider might expect, why not. And where the responsible person is a company or organisation rather than an individual, a named senior person within it must be designated to own compliance.

Everyone in scope must also notify the Security Industry Authority (SIA) - the new regulator for this legislation - that they are responsible for their premises or event, and tell the SIA again if that responsibility ends.

Running through all of it is a single guiding phrase: "so far as is reasonably practicable." Nobody is expected to spend disproportionately, or to ask staff to take steps that would put their own safety at risk. What's proportionate for a 220-capacity village hall and what's proportionate for an 8,000-seat arena will look very different, and that's by design - the guidance repeatedly stresses that no two premises are quite the same, and each responsible person has to think through their own circumstances rather than follow a generic checklist.

The statutory guidance states:

> *"Reasonably practicable means proportionate. In considering what is reasonably practicable, the responsible person should weigh what can be done to achieve the objectives of procedures and/or measures, balanced against the cost, time and difficulty of implementation. The responsible person must consider what is reasonably practicable when ensuring that appropriate public protection procedures and/or measures are in place."*

Enforcement - and why "not yet in force" doesn't mean "ignore it"

The SIA has been appointed as the regulator and will have powers to inspect premises, request information, and, in cases of non-compliance, issue compliance notices, restriction notices and financial penalties, with the most serious enhanced-tier failures capable of attracting very substantial fines. The SIA is obliged to issue guidance on how it will exercise its regulatory functions. Consultation on draft guidance ended in June 2026, and the final version is expected to be published soon.

The bigger picture

It is tempting to read Martyn's Law as another item on an already crowded compliance list, alongside health and safety, fire safety, licensing and data protection. In one sense it is exactly that - the Act does not replace any of that existing law, and organisations will need to keep meeting all of their other legal obligations in parallel. But it is also something a little different: an attempt to put counter-terrorism preparedness on the same statutory footing as those older, more familiar regimes, on the basis that voluntary good practice, however well-intentioned, has proved inconsistent across the country.

For the security industry, this represents both an obligation and an opportunity. Venues and event organisers who have never had to think formally about evacuation planning, lockdown procedures or staff briefings for a terrorist scenario now have a legal reason to do so - and a real incentive to get expert help in doing it well, rather than treating it as a box-ticking exercise. The businesses that treat the implementation period as genuine preparation time, rather than a deadline to worry about later, will be the ones best placed when the SIA's full regulatory powers arrive.

Martyn Hett would have turned 39 this year. His mother's campaign has changed the law so that other families are, in a small but real way, less likely to lose someone as she lost him. The industry is likely to take its obligations under Martyn's Law seriously, and doing so will honour the innocent lives lost in terrorist attacks in the UK.

This article is intended as a general introduction to Martyn's Law and does not constitute legal advice. Organisations should refer to the full legislation and statutory guidance and seek specific legal advice on their own circumstances.



Gary Grant

BARRISTER

Gary Grant is a specialist licensing and regulatory barrister practising from Francis Taylor Building, Inner Temple, London.

Why ship detentions are rarely only about the law

Ship detention is rarely just a legal matter. MAST's maritime dispute resolution team has spent two decades working through the political, regulatory and relational dimensions that determine how, and when, ships and crews are released.

Peter Astbury · Contingency Response Consultant

Bad weather and piracy are not the only risks faced by ship operators in some parts of the world. Trading accidents, contractual disputes, port congestion and a host of other potential issues can lead to delays, and the arrest or detention of ships and runaway financial losses.

MAST has a maritime dispute resolution team with over two decades' experience supporting ship operators through front line interventions to mediate complex and sometimes sensitive, and often deadlocked situations.

Team leader Peter Astbury has just returned from the Middle East after helping to secure the release of a ship that had been detained for five months after GPS spoofing caused the vessel, along with others, to run aground on a coral reef during approach to port.

Peter says that these types of extended detentions are not always about money. The coral reef in this case was located within the seas of a country that has recently reorganised its environmental agencies.

> "These types of extended detentions are not always about money."

The jurisdictional competencies of the new agencies in relation to these groundings were unclear and the parties concerned were unfamiliar with the financial guarantees that shipowners' liability insurers customarily provide in these situations to allow ships and crew to sail whilst the process of damage assessment and compensation is worked out and negotiated.

So in this case, Peter's contribution was above all to liaise with the local authorities to identify a counterparty with competence to accept the insurer's

Where detentions become complex

MIDDLE EAST

A five-month detention followed after GPS spoofing contributed to multiple vessels grounding on a coral reef. With environmental agencies recently reorganised and jurisdictional responsibilities unclear, the situation illustrates how regulatory uncertainty can complicate the acceptance of standard shipowner liability guarantees.

APAPA, NIGERIA

Ship arrests following discoveries of cocaine concealed within South American sugar cargoes illustrate a different challenge. Where drugs may have been loaded without the knowledge of owners or crew, legal considerations can become intertwined with political and public-policy pressures.

guarantee, and to reassure that counterparty that the guarantee offered by the shipowner's insurer was solid. In particular, to reassure the counterparty that the insurer would not walk away from the shipowner's liabilities or abandon them after the ship was released.

According to Peter, cases like this provide great opportunities to develop good working relationships and trust with local authorities that help to enable smooth trading and problem solving in the future in ways that minimise unnecessary delay to ships or trauma for crews.

The recent spate of ship arrests in Apapa port in Nigeria linked to discoveries of small amounts of cocaine hidden deep inside cargoes of sugar loaded in South American ports is another case in point. Peter says that the Nigerian authorities know that these drugs are placed on board by South American drug cartels in collusion with local load port stevedores and without the knowledge of shipowners or crew, but once drugs are discovered, politics requires that they are seen 'to be doing something'.

The key to unlocking the subsequent arrest of ship and crew is to understand that these are first and foremost political rather than legal problems, best addressed through dialogue with the Nigerian authorities rather than through open legal proceedings, which the authorities cannot, for public policy reasons, be seen to lose.



Peter Astbury

CONTINGENCY RESPONSE CONSULTANT

Peter was a claims director for the UK P&I Club before establishing himself as a specialist advisor and intermediary for the shipping and insurance industry, dealing with threats, difficult asset and personnel detentions, and other disputes in complex environments.

Somali Piracy: A Re-emerging Threat, but Not Yet a Return to 2011

Phillip Cable LLM · CEO MAST

The latest spate of attacks and, indeed, hijackings in the Indian Ocean and Gulf of Aden are a salutary reminder of the fact that security on the High Seas can never be guaranteed. The region's other threats, and the ongoing tensions involving Iran, Israel and Gaza, are understandably more newsworthy, but one cannot escape the creeping return of Somali-linked piracy.

There is now sufficient evidence to conclude that Somali piracy has genuinely re-emerged. That does not, however, mean that the Western Indian Ocean is returning inevitably to the extraordinary circumstances of 2008–2012, when the capture and ransom of commercial vessels developed into an almost industrial criminal enterprise.

The distinction matters.

On 20 August the Eritrean-flagged tanker **MT Sibu 1** was reportedly hijacked approximately 136 nautical miles east of Mukalla, Yemen, becoming the sixth commercial vessel reported hijacked in the region since April. Just days earlier the Cameroon-flagged **MV Lutuf** had been seized only a few nautical miles from Puntland's coast. Somali officials said the vessel was carrying Turkish military equipment destined for Mogadishu.

These incidents follow the seizures of vessels including **Honour 25, Sward, Eureka and Asana,** while Pirate Action Groups have also attempted attacks against other merchant vessels. Operation ATALANTA's response to the attempted boarding of **Golden Arsenal** in July demonstrated that active Pirate Action Groups are capable of operating well beyond immediate coastal waters. It also demonstrated something equally important: a properly prepared vessel using established defensive procedures remains a difficult target. The crew reached their citadel, naval forces coordinated a response and the vessel ultimately continued its voyage.

The correct assessment is consequently neither that "piracy is back" and all vessels are once again in grave danger, nor that the incidents are merely isolated anomalies.

The more interesting question **is why piracy is re-emerging now, whether Somalia itself is returning to the conditions that allowed piracy to flourish fifteen years ago, and what evidence would indicate that today's resurgence is developing into something substantially more serious.**

Somalia is not the Somalia of 2011

The frequently repeated description of Somalia as a failed or effectively ungoverned state is increasingly misleading.

Somalia undoubtedly remains extraordinarily fragile, but significant elements of state capacity have developed. Public financial management, customs administration, banking supervision and revenue collection have improved. IMF-supported reforms have included the Somalia Customs Automated System, stronger expenditure controls and financial governance measures. Domestic government revenues

have risen substantially from the extremely low base of the previous decade.

Somalia has completed the international debt-relief process, joined the East African Community and adopted a National Transformation Plan covering governance, economic development, human capital and resilience.

These developments do not describe a strong state. They do describe **a state that exists and possesses considerably greater administrative capacity than Somalia possessed during the first piracy crisis.**

That should immediately make analysts cautious about simplistic comparisons with 2011.

The problem is that stronger institutions have developed alongside increasingly serious political fragmentation.

The relationship between President Hassan Sheikh Mohamud's Federal Government in Mogadishu and important Federal Member States has deteriorated severely. Constitutional amendments, proposed direct elections, the distribution of authority between federal and regional governments, and the political timetable have generated major disputes.

Puntland has rejected elements of Mogadishu's constitutional process and has, in effect, suspended normal relations with the Federal Government. Jubaland has also been involved in major disputes with Mogadishu. Most recently, political tensions contributed to serious fighting in Baidoa between federal troops and forces aligned with the opposition, illustrating that constitutional disagreement has the potential to become armed confrontation.

The relevance to piracy is therefore subtler than "weak government creates piracy".

> **Somalia is more governed than it was fifteen years ago, but political authority remains fragmented, security resources are overstretched and responsibility for Somalia's enormous coastline is divided between institutions that do not necessarily cooperate effectively.**

Puntland is the centre of the equation

For the piracy question, what happens in Puntland arguably matters more than what happens in Mogadishu.

The principal contemporary pirate activity is associated with the north-eastern coast, including the Eyl, Garacad and Hafun areas. Puntland has its own government, parliament, police, intelligence organisations and maritime-security capability.

This is not an entirely permissive operating environment for pirates.

Somali-language reporting from Puntland provides important evidence often absent from international maritime alerts. In May Puntland security forces reportedly imposed a landward blockade on pirate groups holding Honour 25 and Sward, attempting to prevent supplies and reinforcements reaching them. In June, Puntland Post reported that three members of the group associated with Sward surrendered to Puntland authorities.

That evidence matters.

It means pirates are not operating simply because local government welcomes them or because no government exists. Puntland is attempting to suppress the activity.

The difficulty is one of **reach and competing priorities.**

Puntland has an exceptionally long coastline and finite security resources. At the same time, it has been conducting a sustained military campaign against Islamic State elements in its mountainous interior, confronting Al-Shabaab activity and dealing with increasingly difficult relations with Mogadishu and federal-aligned armed formations.

The resulting environment creates gaps.

Pirates do not need the Puntland Government to collapse. They need certain isolated stretches of coastline where the state's presence is sufficiently weak, local protection can be obtained and captured

vessels can be supplied.

That is a considerably more realistic explanation of the present resurgence.

Piracy requires an economy ashore

An enduring Somali piracy campaign cannot be sustained simply by armed men in skiffs.

A successful hijacking lasting weeks or months requires food, water, fuel, communications, khat, guards, negotiators, financial intermediaries, transport and access to safe coastal anchorage.

It therefore requires a **shore-side criminal ecosystem.**

Local reporting illustrates this particularly clearly. Following the seizure of Lutuf, a small vessel reportedly approached the hijacked ship carrying khat before returning to shore. The circumstances surrounding a subsequent reported air strike remain disputed, but the episode offers a glimpse into the logistics supporting a hijacked vessel.

This is why the most important indicator of future piracy risk may not be the number of attacks recorded in any particular month.

The key question is whether pirate groups can rebuild **persistent shore support networks.**

There are currently contradictory signs.

Some communities appear prepared to tolerate or assist pirate groups. Arabic-language reporting on the Asana hijacking cited local sources suggesting that those involved were associated with the Garacad area and enjoyed some local sympathy. The same reporting described the use of the previously hijacked Sward in subsequent maritime activity.

Conversely, other reporting demonstrates pressure from Puntland authorities and traditional elders against pirate networks.

Both can be true.

Somalia's coastal politics is intensely local. One community, clan network or group of businessmen may facilitate pirates while neighbouring communities oppose them. The existence of Puntland government authority therefore does not automatically eliminate pirate sanctuary.

Follow the ransom, not simply the attack statistics

There is another reason for caution.

Piracy is fundamentally a commercial criminal enterprise.

Attack statistics describe activity. **Ransom payments determine whether the business model works.**

This is arguably the most important lesson of the 2008–2012 period. Large ransom payments did not simply reward successful pirates. They financed subsequent expeditions, created investors and financiers, paid coastal communities and guards, attracted recruits and established professional negotiation structures.

An isolated successful hijacking is therefore less significant than a series of ransom settlements demonstrating to Somali criminal networks that maritime kidnapping has again become reliably profitable.

Arabic-language analysis published by the Al Jazeera Centre for Studies in June identified ransom incentives, weakness in maritime-security structures, illegal fishing and the diversion of naval attention towards the Red Sea among the factors helping to recreate conditions favourable to piracy.

The illegal-fishing grievance deserves recognition but also caution.

Illegal and unregulated fishing in Somali waters is a genuine issue and has long provided pirate groups with a narrative of defending coastal communities against foreign exploitation. It may encourage recruitment and local tolerance.

It does not adequately explain organised attacks against commercial ships far offshore.

Once a group captures a merchant vessel and demands millions of dollars for its release, it is difficult credibly to describe the activity as maritime self-defence.

The primary motive remains profit.

Regional instability creates opportunity, not necessarily conspiracy

The wider regional environment undoubtedly contributes to the opportunity.

International naval forces now face Houthi attacks, Iranian activity, weapons smuggling, electronic interference, protection of freedom of navigation and conventional military tensions alongside piracy.

Naval resources are formidable but finite.

Pirates do not have to defeat a naval coalition. They merely need to operate where that coalition is not present.

Arabic-language reporting has gone further, examining possible relationships between Somali armed groups, Al-Shabaab and the Houthis. These questions deserve investigation, particularly given documented weapons-smuggling networks across the Gulf of Aden.

However, MAST would caution strongly against collapsing several distinct threats into a single narrative.

There is evidence of interaction between Yemeni and Somali smuggling networks and evidence of contacts involving terrorist organisations. That does not presently establish that the pirate groups operating from Puntland are controlled by the Houthis or Al-Shabaab.

Similarly, Puntland President Said Abdullahi Deni has alleged that outside actors may be encouraging piracy to damage Puntland and has accused the Federal Government of destabilising the region. Puntland's Security Ministry announced an investigation into possible external involvement on 21 August.

These allegations are politically important because they demonstrate the depth of the rupture between Garowe and Mogadishu.

They should not presently be treated as established intelligence.

No publicly available evidence yet substantiates the allegation that the Federal Government, or another external actor, is directing the current piracy campaign.

The greatest risk may lie ahead

Seasonality deserves particular attention.

Small skiffs have operational limitations, and southwest monsoon conditions constrain long-range activity in exposed waters. As sea conditions become more favourable during the autumn, those constraints reduce.

The significance of motherships consequently increases.

Captured fishing vessels, dhows or merchant vessels can provide fuel, provisions, range and endurance, allowing Pirate Action Groups to operate far beyond Puntland's immediate coastline. This was one of the developments that transformed Somali piracy during the previous crisis.

The hijacking of Sibu 1 more than 130 nautical miles east of Yemen demonstrates that current operations cannot simply be characterised as coastal robbery.

MAST therefore assesses that **the final quarter of 2026 will provide an important test of whether the present resurgence remains geographically constrained or develops into sustained long-range Pirate Action Group activity.**

What does this actually mean for shipowners?

This is where threat analysis should resist commercial exaggeration.

There is an understandable perception within shipping that some security providers have an economic interest in piracy returning. That makes proportionate advice essential.

MAST does not currently assess that conditions justify treating every Gulf of Aden or Western Indian Ocean transit as equivalent to a transit in 2011.

Nor should the presence of Somali pirate activity automatically result in the deployment of armed security personnel.

The appropriate response remains **risk-based and vessel-specific.**

A slow regional tanker with low freeboard approaching Bosaso, operating close to the Somali coast and carrying limited physical protection is clearly more exposed than a fast container vessel maintaining substantial sea room from known Pirate Action Group locations.

Owners should consider geography, vessel speed and freeboard, route, cargo, access points, physical protection, crew preparedness, citadel arrangements and the latest intelligence on active Pirate Action Groups before determining additional security requirements.

At a minimum, vessels operating through exposed areas should apply current BMP-Maritime Security, maintain effective watchkeeping and radar surveillance, control access to the vessel, rehearse piracy alarms and citadel procedures, maintain appropriate reporting and registration with UKMTO and MSCIO, and conduct a voyage-specific threat and risk assessment.

Operation ATALANTA's experience with Golden Arsenal reinforces an important point: basic defensive measures can work.

The deployment of privately contracted armed security personnel should therefore remain an escalation measure based upon identifiable risk rather than a default commercial response.

Security must also be layered. Measures designed to defeat pirates do not necessarily protect a vessel against missiles, UAVs, unmanned surface vessels or state interference. The contemporary Gulf of Aden therefore presents a more complex problem than the piracy crisis fifteen years ago.

MAST assessment

The evidence supports a more nuanced conclusion than much of the current commentary.

> **Somali piracy has returned. Somalia has not returned to 2011.**

The threat is presently best understood as a **re-emerging criminal ecosystem operating within gaps created by uneven governance, political fragmentation, diverted security resources and renewed evidence that hijacking can generate significant financial reward.**

There are substantial brakes on further expansion. Puntland possesses functioning security institutions and has demonstrated willingness to confront pirate networks. Traditional leaders and communities are not uniformly supportive. International naval forces remain capable of disrupting Pirate Action Groups, and properly prepared merchant vessels remain difficult to board successfully.

Against this, Puntland's security establishment is simultaneously fighting terrorism, managing internal political tensions and policing an immense coastline. Relations between Puntland and Mogadishu are unusually poor. Several successful hijackings have demonstrated renewed pirate capability, while mothership operations offer the potential for attacks to spread considerably further into the Arabian Sea and Indian Ocean.

MAST therefore assesses the current Somali piracy threat as **increasing but still containable rather than systemic.**

The critical indicators to watch are not simply additional UKMTO alerts.

The more consequential warning signs would be the successful conclusion of several high-value ransom negotiations; persistent use of motherships to extend Pirate Action Group operations hundreds of nautical miles offshore; growth in the number of functioning pirate groups; evidence of recruitment and financing networks ashore; and, most importantly, signs that Puntland's authorities are losing either the ability or the political willingness to deny pirates coastal sanctuary.

If those factors begin to occur together, the risk assessment should change materially.

Until then, shipowners should resist both complacency and alarmism.

The lesson from Somalia is not that every merchant vessel needs armed guards again.

It is that the conditions capable of producing a much larger piracy problem are beginning to reappear, and the shipping industry has an opportunity to prevent today's manageable threat from developing into tomorrow's crisis.



Phillip Cable LLM

CEO MAST

Phillip Cable LLM is the CEO and co-founder of MAST. Phil's Royal Navy and legal background has given him an exceptional understanding of the insurance and legal requirements of developing and leading an international security company and he has been instrumental in the development of MAST since its formation.

Get in touch

WEBSITE

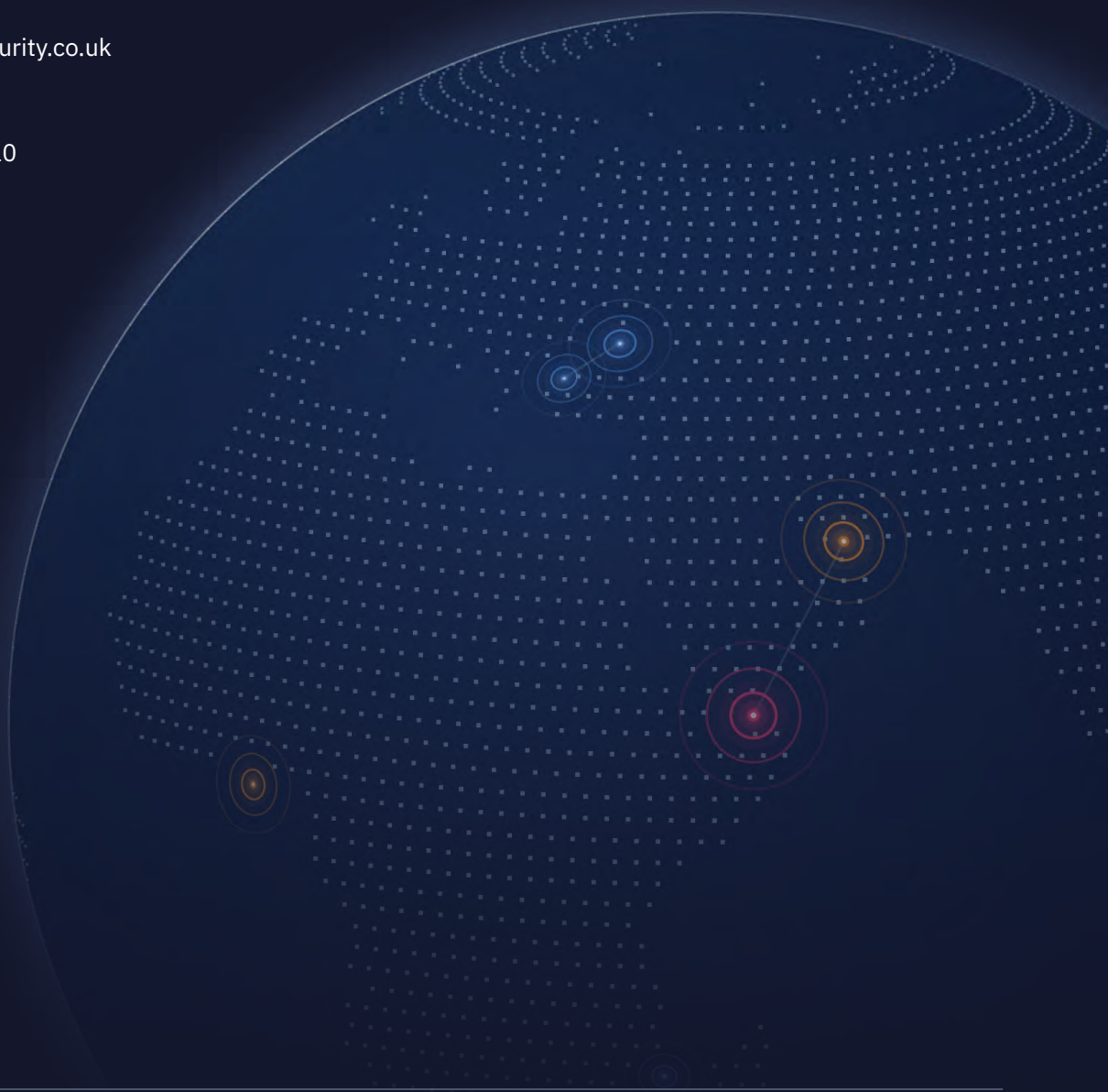
www.mast-security.com

EMAIL

operations@mast-security.co.uk

TELEPHONE

+44 (0) 2079 380 9210



The views expressed by contributing authors are their own. This report is provided for information and does not constitute legal, insurance or security advice.