MAST



MAST Risk Report

Expert Perspectives on Emerging Threats

OCTOBER 2026

WWW.MAST-SECURITY.COM

Contents

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

01 The person is not the problem 3

ANDREW CLARKE MSc FCMI · CEO RECYBER

02 The promise and peril of Magnitsky-style regimes 6

TOBY CADMAN · HEAD OF CHAMBERS, OUTLINE CHAMBERS

03 One scale for hybrid threats 9

JAMES DAVIES · FOUNDER AND CEO, SENTINELLA GLOBAL

04 The crew remembers. Does the industry? 14

DR JESSICA SIMONDS · ASSISTANT PROFESSOR, RABDAN ACADEMY, UNITED ARAB EMIRATES



The person is not the problem

Rethinking responsibility for behavioural cyber risk

Andrew Clarke MSc FCMI · CEO Recyber

Behaviour is the unit of measurement. The person is not the unit of blame.

Cybersecurity has spent years telling employees what they should and should not do.

Do not click suspicious links. Use strong passwords. Report anything unusual. Follow policy. Protect information. Challenge strangers. Escalate concerns.

When something subsequently goes wrong, it's therefore tempting to locate the failure in the individual: somebody clicked, shared, bypassed a control, failed to report, made the wrong decision or did not follow the process. It's a convenient, but often incomplete explanation.

Human behaviour does not occur independently of the environment in which people work. It is shaped by organisational rules, technology, workload, incentives, competing priorities, available alternatives, perceived consequences, decision authority, and the effort required to do the secure thing.

The person may present where risk becomes visible, but that does not always mean it's where it originated.

Security behaviour is a systems outcome.

Behavioural science provides a useful way of understanding this distinction.

Michie's COM-B model proposes that behaviour depends upon three interacting conditions: **Capability, Opportunity and Motivation**. For an employee to behave securely, they must therefore be sufficiently capable of identifying and performing the required behaviour, have a realistic opportunity to do so, and be motivated to act.

That shifts the question from **"did the employee know what they were supposed to do?"**, and requires organisations to ask:

Could they do it? Was the environment designed to enable them to do it? And, given the competing pressures they faced, was there sufficient reason for them to do it?

Training addresses only part of that equation.

An employee can understand a policy perfectly well and still circumvent it because following it prevents them from completing their work. They can recognise a suspicious event but decide not to report it because the reporting process is cumbersome, they are uncertain whether there is sufficient evidence, or previous reports disappeared without feedback. They can know exactly what good security looks like and still lack the authority to make the necessary decision.

In each case, the behaviour is real. But attributing it simply to an individual "human risk" score risks misdiagnosing its cause.

Compliance and circumvention can coexist.

Recent research reinforces this distinction. A recent study examined how employees respond when information-security rules conflict with the demands of their work. Their study suggests that obstructive policies can increase intentions to circumvent or avoid security requirements without necessarily reducing an employee's intention to comply.

This matters because compliance and circumvention are not necessarily opposite ends of a single behavioural spectrum. The same employee may support a security policy, understand why it exists and generally attempt to comply with it, while simultaneously finding ways around it when operational circumstances make compliance impractical.

A single score describing that individual as more or less "risky" struggles to represent those behaviours adequately. Asking who broke the rule is not helpful.

The better question is: **what conditions made bypassing the rule a rational or necessary response?**

> *If secure behaviour repeatedly conflicts with getting the job done, the organisation has created a security design problem as much as an employee behaviour problem.*

Reporting is behaviour too.

The same principle applies to reporting.

Research published in 2026 distinguishes between different responses to suspected scams, including private action and formal public reporting. Their findings indicate that reporting decisions are influenced not simply by whether someone recognises a problem, but by factors including effort, uncertainty and confidence in the available evidence. This has an important implication for cyber security.

A low reporting rate cannot automatically be interpreted as poor awareness or irresponsible behaviour. Employees may recognise suspicious activity but decide that reporting it is difficult, pointless, embarrassing, or unlikely to result in action. They may attempt to resolve the problem themselves. They may be uncertain whether what they have observed meets the organisation's threshold for reporting.

The organisation therefore owns part of the reporting behaviour. If reporting matters, organisations must make it easy, psychologically safe and worthwhile.

Behaviour extends beyond prevention.

The same argument becomes even clearer during a serious cyber incident.

The NCSC's October 2026 guidance on disruptive cyber attacks emphasises that organisational resilience depends upon people being prepared to operate under degraded conditions, make decisions in uncertainty, understand their responsibilities, use alternative communications and practise how they will respond before an incident occurs. These are behavioural security outcomes too.

Cyber behaviour is therefore much broader than susceptibility to phishing. It includes the ability to **comply, bypass, avoid, report, decide and recover**. Each is a different behaviour, produced under different conditions and requiring different capabilities. Reducing them to one employee-level score obscures more than it reveals.

Organisations must own the environment.

This does not remove individual responsibility.

Employees still make decisions and their behaviour matters. Organisations need to understand where behavioural susceptibility exists and intervene where necessary.

But measurement should not become attribution.

Research outside cyber security increasingly warns against what systems scientists describe as **"shifting**

the burden" by concentrating intervention on the visible behaviour of individuals while overlooking the institutional conditions producing that behaviour. It is argued that individual behaviour cannot sensibly be separated from the systems within which it occurs. The lesson for cyber security is important.

If an organisation trains people repeatedly but leaves insecure workflows unchanged, it cannot place responsibility solely on the employee when predictable workarounds emerge.

If it tells people to report incidents but makes reporting difficult, it should not interpret silence simply as disengagement.

If it expects decisive action during disruption but has not delegated authority or rehearsed decision-making, hesitation is partly an organisational outcome.

And if people are measured against behaviours that the organisation itself makes difficult to perform, the measurement system is measuring the organisation as much as the individual.

Measure behaviour. Diagnose the system.

Behavioural risk management therefore requires two levels of measurement.

First, organisations should identify and measure specific behaviours over time: whether people **comply, bypass, avoid, report, decide and recover**. Second, those behaviours should be interpreted alongside the organisational conditions capable of producing them: **capability, opportunity, motivation, workload, policy friction, available alternatives, reporting cost, decision authority and operational consequence.**

That distinction changes the purpose of behavioural measurement. The objective is no longer to identify "risky people", but to identify **where behavioural risk exists, why it exists and what the organisation can change to reduce it**. The strongest human security systems do not demand perfect behaviour from imperfect people operating inside poorly designed environments. They create environments in which secure behaviour becomes the easiest, most practical and most natural course of action.

Behaviour is the unit of measurement. The person is not the unit of blame.



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.

SANCTIONS AS ACCOUNTABILITY

The promise and peril of Magnitsky-style regimes

Targeted human rights sanctions were meant to close the gap between atrocity and consequence. A decade on, they have become a permanent feature of the risk landscape, and an increasingly political one.

Toby Cadman · Head of Chambers, Outline Chambers

When Sergei Magnitsky died in a Moscow detention centre in November 2009, having exposed a vast tax fraud and been imprisoned for his trouble, there was no realistic prospect of an effective domestic prosecution of those responsible. The response that followed was not judicial but executive: the Sergei Magnitsky Rule of Law Accountability Act of 2012, a United States law allowing the government to freeze the assets of, and refuse entry to, the Russian officials it held responsible. The idea was simple and powerful. If the perpetrators of serious abuses could not be prosecuted, they could at least be denied the comforts of the free world: its banks, its property markets, its schools and its holidays.

That idea has travelled well. The United States globalised its regime through the Global Magnitsky Human Rights Accountability Act of 2016, put into effect by Executive Order 13818 in December 2017. Canada, the United Kingdom, the European Union, Australia and others followed. The United Kingdom's Global Human Rights Sanctions Regulations came into force in July 2020 with the designation of individuals connected to the Magnitsky case and the murder of Jamal Khashoggi. The European Union adopted its own global regime on 7 December 2020; according to the Council, it currently applies to 151 individuals and 45 entities, up from 135 individuals and 37 entities when the listings were last renewed in December 2025. The framework itself was extended in December 2023 for three years, and the current listings were prolonged in December 2025 for one year; both now run until 8 December 2026, so a renewal decision is due within weeks. In the United States, the government reported that 744 foreign persons remained designated under the Global Magnitsky programme at the end of 2025.

Why it matters to business

For the readers of a risk report, the significance of these regimes lies less in their moral ambition than in their reach. A designation freezes assets and prohibits anyone within the jurisdiction from making funds or economic resources available to the person listed. That prohibition extends to entities they own or control, although the tests differ: the United States applies a 50 per cent aggregate ownership rule, while the British and European regimes also capture entities that are controlled by a designated person without being majority-owned. A supplier, joint venture partner, landlord or customer can become untouchable overnight, and the obligation to identify and act on that change falls squarely on those who

deal with them.

The regimes are also not aligned. The United States, the United Kingdom and the European Union apply different criteria, run different lists and make different choices. The European Union's regime, for example, does not extend to corruption. The United Kingdom addresses corruption through its separate Global Anti-Corruption Sanctions Regulations 2021, and the United States covers corruption within the Global Magnitsky programme itself. Screening against one list is not screening against all of them, and a business operating across jurisdictions must understand which rules bind which of its people and transactions.

Due process and the high bar to challenge

Sanctions are imposed by ministers and officials, not by courts, on the basis of 'evidence' that the designated person may never see in full and never have an effective opportunity to challenge. The standard in the United Kingdom, under the Sanctions and Anti-Money Laundering Act 2018, is reasonable grounds to suspect. That is an extremely low threshold for a measure whose practical consequences (frozen assets, lost livelihoods, reputational ruin, often for years) can rival those of a criminal conviction, but without the criminal standard of proof or the full disclosure that comes with it.

The courts have accepted that designations engage fundamental rights and must be proportionate. But in Shvidler, decided in July 2025, the Supreme Court made clear how much latitude the executive will be given. The Court held that it must reach its own view on proportionality, but that considerable weight is owed to the government's judgment on matters of foreign policy, and that sanctions must often be severe and open-ended to be effective. Lord Leggatt's powerful dissent, which would have found the designation of Mr Shvidler disproportionate, is likely to be cited for years. It did not carry the day.

The practical lesson is that the most effective challenges are frequently those brought early and administratively: a well-evidenced request for ministerial review in London, a properly prepared delisting petition to the Office of Foreign Assets Control in Washington, or an annulment application before the General Court in Luxembourg, which must be lodged within two months (plus ten days) of the listing being published or notified. Litigation has its place, but it is rarely quick and rarely certain.

The politicisation problem

The more serious threat to these regimes now comes from within. Their legitimacy depends on the perception that designations follow evidence of abuse rather than political convenience. That perception has been badly damaged.

According to the United States government's report to Congress for the 2025 reporting period, seven foreign persons were designated under the Global Magnitsky programme and four were removed by the end of the year, producing a net increase of three. During the same period, earlier designations were terminated for Antal Rogán, the minister heading the Hungarian Prime Minister's Cabinet Office, in April 2025, and for former Paraguayan president Horacio Cartes and his affiliated companies, in October 2025. Brazil's Supreme Federal Court Justice Alexandre de Moraes was designated in July 2025, in a move criticised by human rights and anti-corruption organisations as an attempt to shield a political ally, and was removed from the sanctions list on 12 December 2025. Members of Congress questioned whether the statutory advance-notice requirements governing terminations had been satisfied.

At the same time, the sanctions toolkit has been turned against institutions and actors associated with international accountability. Acting under Executive Order 14203 rather than the Global Magnitsky programme, the United States has designated International Criminal Court judges, prosecutors and other officials, as well as organisations said to support the Court's work. It has also designated a United Nations Special Rapporteur. Whatever view one takes of the Court, the sight of economic sanctions being

used against those involved in investigating alleged atrocities ought to give everyone pause.

None of this means that targeted sanctions have failed. They remain one of the few tools capable of imposing a tangible cost on those who commit grave abuses beyond the reach of any court. But a sanctions regime that is applied selectively, withdrawn on request and used against the guardians of accountability ceases to be a human rights instrument and becomes simply another lever of foreign policy.

Looking ahead

For risk professionals, three points follow. First, designation risk should be treated as dynamic and political, not merely legal: who is listed, and who is delisted, may change with an election. Second, divergence between the major regimes is likely to widen, increasing the compliance burden for anyone operating across them. Third, both the European Union's framework and its current listings expire on 8 December 2026, so the Council must decide in the coming weeks whether to renew the regime and which designations to keep. The more consequential question is whether the Union will finally adopt targeted anti-corruption sanctions. The proposal on the table is for a separate, dedicated corruption regime rather than an extension of the existing one, and in January 2026 the European Parliament regretted that it remains blocked in the Council by some Member States. Its adoption would materially narrow one of the principal differences between the European, British and American approaches.

The idea born of Sergei Magnitsky's death, that those who commit grave abuses should not enjoy the privileges of the societies whose values they violate, was a good one. It deserves to be defended, which means insisting that it be applied consistently, with due process, and to the people who actually deserve it.



Toby Cadman

HEAD OF CHAMBERS, OUTLINE CHAMBERS

Toby Cadman is Head of Chambers at Outline Chambers, a specialist international set based in London. His practice covers international criminal law, public international law, human rights, sanctions and extradition.

One scale for hybrid threats

Five hybrid threats now reach Mediterranean operators through five different channels. Reading them on one scale, against one auditable method, turns a pile of alerts into a ranked set of decisions, from the bridge to the boardroom.

James Davies · Founder and CEO, Sentinella Global

At 06:00 on a Monday, a fleet security manager opens five windows on their desktop. The first is a GNSS interference advisory for the eastern Mediterranean. The second is an AIS alert: a tanker with a patchy history has gone dark eight miles from an anchorage where one of the company's vessels is waiting for a berth. The third is a national CSIRT bulletin warning of denial-of-service attacks against port and logistics websites in the region. The fourth is the latest round of sanctions designations, and nobody has yet checked whether any of the new names operate near the company's next port calls. The fifth is an email from the regional aviation security agency warning of increased drone incursions into restricted airspace.

Each of these is a real category of risk in the Mediterranean today. Each arrives from a different source, in a different format, on a different schedule, and usually lands with a different person. None of them answers the question the manager actually has to answer before the 08:00 call: which of my ships, ports, or routes needs attention first, and what do I do about it?

My background is in federal protective operations and all-source intelligence: where the work is rarely about whether a threat exists. Threats always exist. The work is deciding which one deserves a team's attention and resources: the next hour, the next security team deployment, and the next euro. Maritime operators face the same problem, and the hybrid threats now crowding the Mediterranean only complicate things. Not because any single one is new, but because they arrive fragmented.

My argument is simple: scattered alerts become ranked decisions when they are transparently tracked in one place and against one auditable methodology. Doing so at every level of an organisation, from the duty officer to the board, gives all involved just one number to watch, one system to audit, and one uniform way to justify their decisions.

What does "hybrid threat exposure" mean, in practical terms?

Before we continue, let me clarify what the security sector means by the phrase "hybrid threat exposure": it is how a maritime asset is exposed to hybrid threats, not confirmed threat activity against an asset.

By "hybrid threats", I mean activity that stays below the threshold of armed attack, but still disrupts how a ship, a port or a subsea cable operates. The actors behind it usually prefer deniability to damage, and they are known to combine methods to further obfuscate the origins of their actions. From an operator's point of view, there are five vectors that matter the most, and seeing them side-by-side helps them prioritise their resources and attention.

Vessel behaviour near the asset. One of the most common and worrying types of behaviour are ships

that switch off AIS close to a port, anchorage, or cable route; loiter without a commercial reason; or anchor where they have no business being. A gap in AIS transmission is not proof of intent, but it is still a measurable fact, with repeated gaps near the same asset forming a pattern worth tracking.

Navigation signal interference. GNSS jamming and spoofing have become a working condition in parts of the eastern Mediterranean. In ship-tracking data from late 2024 and early 2025, researchers at Georgia Tech University found vessels off the Levant that appeared to have "teleported" inland to near Jordan's main airport in bursts that matched escalations in Gaza. A related problem is false or duplicated identity: two hulls broadcasting the same MMSI, or a hull whose broadcast identity does not match its movements.

Sanctions and shadow fleet activity. Sanctioned or high-risk vessels operating close to ports, anchorages, and infrastructure create two exposures. The physical one is a poorly maintained, poorly insured hull in a congested approach. The legal one is that providing services to a designated person can itself breach EU sanctions, and "we did not check" is a weak position that is becoming harder to defend.

Cyber attacks on the networks ships depend on. The ship may be well protected; the port, terminal and logistics systems it relies on often are not. In a single week this March, Cyprus took 52.5% of the 5,828 denial-of-service attacks that SOCRadar recorded from NoName057(16), a pro-Russian hacktivist group. Most hit government sites, but transport, finance and energy were targets too. In August, the tanker VL Prosperity was hacked near Gibraltar; the US Coast Guard says "foreign cyber actors" were involved. Attacks like these, unsurprisingly, cluster around political escalations: exactly when operational pressure is highest.

Drone incursions. Uncrewed aircraft over port areas, terminals, and coastal infrastructure are a growing concern. The identification signal that EU rules require commercial drones to broadcast is unauthenticated and can be spoofed, which makes it structurally similar to AIS: the dark targets and the false targets are the signal. This is where our own methodology is now extending.

None of these vectors are exotic. The difficulty is that they rarely arrive alone and an operator missing when the vectors overlap can be disastrous.

Fragmentation is the real risk

Let us consider how these vectors typically reach an operator. AIS anomalies come from a vessel-tracking tool watched by an operations desk. GNSS advisories come from navigational warnings and the bridge's own observations. Sanctions updates come from a compliance team, often weekly, and often in a spreadsheet. Cyber alerts come from IT or a managed security provider. Drone sightings, where they are reported at all, come from port security staff by radio or email.

This leaves operators with five vectors, five owners, five different cadences, and five different formats to review. These are the three consequences of trying to stay on top of such important, yet ultimately fragmented reporting.

The convergence goes unseen. Hybrid activity is most telling when vectors coincide: GNSS degradation in the same week as unusual loitering near the same terminal, while that port's systems are under denial-of-service pressure. Any one of those signals is noise, but together they form a picture. When each signal lands in a separate inbox, nobody holds the picture.

Attention follows volume, not exposure. Without a common unit, the loudest alert wins: the one with the most red in the email, or the one from the most senior sender. A busy security manager will rationally deal with what is in front of them, which is by no means a failure of diligence; however, it is the predictable result of having no way to quickly and concretely compare a GNSS advisory with a sanctions update on one system.

Nothing can be compared over time. If last month's assessment of a port was a paragraph of prose and this month's is a different paragraph by a different

analyst, nobody can say whether exposure went up or down, or why. Boards, insurers and regulators increasingly ask exactly that question.

What one auditable methodology changes

The remedy is not more data, but how that data is relationally consolidated and presented. Most operators already receive more alerts than they can process, so the remedy is a common way of reading them. At Sentinella Global, we built Mare around a standardised maritime hybrid threat exposure score (MHTES) for each asset, whether it be a port, a subsea cable or a vessel, on a single scale with five bands from Minimal to Severe. Without going into the internals, four principles do most of the work and apply to any serious scoring approach, whether it be ours or anyone else's.

The same rules for every asset. A port in Sardinia and a port in the eastern Mediterranean are scored by the same method. The rules do not change per client, per region or per quarter. That is what makes a reading in one place comparable to the same reading in another, and what stops a score drifting toward whatever its reader wants to hear.

Every reading traces back to its sources. A score that cannot show the evidence that produced it is just an opinion with a number attached. Each and every reading should point back to dated evidence: which vessel, which AIS gap, which advisory and which designation. If an auditor, an insurer, or a sceptical captain asks why a certain asset is rated "High", the answer should take one click, not a meeting, to understand the rating.

Measurements and inferences are kept apart. An AIS gap is a measurement: the signal stopped at a known time and place. A suspected spoofing event is an inference: a pattern that suggests manipulation. Both matter, but they deserve different weight in a decision, and a methodology weighting exposure should differentiate between the two, rather than blending them together.

Absence of data is never read as absence of threat. If a feed fails, the honest output is "unknown" instead of issuing an "all clear". Decision makers must have an accurate and honest read of their systems at any given time, to include understanding if a sanctions screen returning "no hits" is due to a failure to load data or a genuine lack of hits. This may seem obvious, but it is a characteristic in security platforms that is not always guaranteed.

With those principles in place, the five vectors stop being five separate problems. They become inputs to one reading per asset, and that reading can be ranked, trended, and explained in simple, traceable terms.

At ground level: the next hour

For a duty officer, a captain, or a port facility security officer, the value of this methodology is first and foremost triage. A ranked list of assets, each with a band and the two or three signals driving it, answers the first question of the shift: where do I look first?

Take a vessel bound for the eastern Mediterranean. Her route reading rises because GNSS interference has been reported along the approach, and two vessels with gaps in their AIS history have been loitering near the anchorage. The practical response is standard: brief the bridge team, cross-check position by both radar and visual bearings rather than trusting the satellite fix, increase the lookout at anchor, and confirm arrival arrangements with the agent. What changes is that the captain receives this as one coherent brief before arrival instead of unrelated notices discovered en route to piece together live.

Bands also make thresholds possible. An organisation can decide in advance what happens when an asset moves from Moderate to High: who is informed, which checks are added, and when the reading is reviewed again. Pre-agreed thresholds take the improvisation out of the night watch. They also make the shift handover a sentence rather than a story: "Port A moved to High overnight on GNSS interference and loitering; nothing else changed."

At management level: the next month

For a company security officer, a designated person ashore, or a fleet security manager, the questions are about resource allocation. Which ports justify additional guards or a fresh security assessment? Which routes justify extra training for the crews who sail them? Which service providers, including port and terminal operators, deserve a pointed cyber question?

A common score lets these decisions be compared across the whole fleet and port rotation, rather than argued case-by-case. If three of twelve port calls account for most of the fleet's elevated readings over a quarter, that is where the training budget, the extra watchkeeping and the conversations with port agents should go. Because the method is stable, management can also see whether the measures worked. If exposure at a port stays "High" after mitigation, the problem is not where they thought it was.

This kind of scoring changes the conversation with underwriters and P&I clubs as well. A company asked how it manages risk on a given trade route can produce a dated series of readings with the evidence behind them rather than an assurance stitched together from multiple sources. That is a stronger position at renewal and a far stronger one after an incident.

At executive level: the next year

Boards and executives decide on routes, ports, partners and investment, and they are increasingly accountable in person for cyber and security risk management. Under the EU's NIS2 Directive, the management bodies of essential and important entities must approve and oversee cybersecurity risk-management measures, and they can be held liable for failures. NIS2 itself excludes individual vessels from its scope, but the ports, terminals and shore-side companies that ships depend on are inside it.

Flag administrations are closing the gap at sea. Italy's Circolare 177/2025, issued by the Comando Generale delle Capitanerie di Porto, requires Italian-flagged ships, ISM companies and port facilities to integrate cyber risk management into their safety and security systems from 1 November 2026. The IMO has expected cyber risk to be addressed in safety management systems since 2021.

What these regimes have in common is that they ask for a demonstrable, ongoing process, not a one-off report. A board cannot demonstrate a process built on five disconnected streams of alerts. It can demonstrate one built on a consistent reading per asset, reviewed on a set cadence, with an audit trail that shows what was known, when, and what was done about it.

The same series supports strategic choices. Should the company accept a charter that requires repeated calls in a region where exposure has been rising for six months? Should one terminal partner be chosen over another with a similar price but a weaker cyber posture? Should a cable owner pay for an alternative route survey now rather than later? These are judgement calls, and a score does not make them. It frames them in the same language the operations team uses every day, which means the bridge and the boardroom are finally reading the same map.

What a score cannot do

It would be dishonest to stop there. A standardised score is a prioritisation tool, not an oracle, and anyone who uses one should be clear about three limits.

It is not attribution. A cluster of AIS gaps near a cable route says that something is worth watching, not who is responsible. Attribution needs evidence that open data rarely provides.

It is not prediction. A "High" reading means current exposure is high on the method's scale, not that an incident will happen. Forecasting is a different discipline, and a responsible methodology must diligently separate the two. This is a measurement of an asset's exposure to hybrid threats and disruptive activity, akin to measuring a cyber attack surface.

It is only as good as its sources and only as honest as its gaps. This is why traceability and the rule that

"unknown is not clear" matter more than any single algorithm. A score that hides its uncertainty is worse than no score at all, because it invites confidence it has not earned.

Used within those limits, a MHTES score does something no additional feed can do: it gives everyone in the organisation the same starting point for a decision that can be easily understood by everyone.

Closing the seams

Hybrid actors are good at finding seams: between agencies, between jurisdictions, between the team that watches AIS and the team that reads sanctions lists. The Mediterranean now has plenty of them, from the GNSS-degraded waters off the Levant to the contested seabed east of Crete, where a single cable survey has become a test of who sets the rules. Operators cannot close every seam in the region, but they can close those that exist inside their own organisation.

One place to see the threats, one methodology to read them and one audit trail to show what was done: that is not really a technology argument. It is the discipline protective work has always relied on. Decide what matters most, act on it first, and be able to explain why.



James Davies

FOUNDER AND CEO, SENTINELLA GLOBAL

James Davies is the founder and CEO of Sentinella Global, which develops Mare, a hybrid threat exposure platform for ports, subsea cables and vessels in the Mediterranean. His background is in federal law enforcement and all-source intelligence.

The crew remembers. Does the industry?

Why the welfare lessons of the first piracy era must not be lost

Dr Jessica Simonds · Assistant Professor, Rabdan Academy, United Arab Emirates

EXECUTIVE VIEW

Somali piracy is re-emerging, and crews now face it alongside attacks on merchant shipping in the Strait of Hormuz, regional instability and prolonged detentions. The systems of care built between 2008 and 2012 were learned at great human cost during the peak of Somali piracy. This article asserts that the mechanisms established to support seafarers belong inside voyage risk management and not simply something to ponder in the aftermath of an incident. It further contends that a hijacked vessel should not be retaken by force until responders have confirmed where every member of the crew is and that they are safe.

Lessons paid for

Between 2008 and 2012 the shipping industry was forced to learn something it had never needed to know at scale. When hundreds of ships are hijacked and thousands of seafarers are held for months, the human response matters as much as the commercial one.

An alliance of owners, unions, managers, manning agents, insurers and welfare bodies came together to build a humanitarian response programme. Nearly 5,000 seafarers had by then been hijacked and detained, often in appalling conditions. The programme organised its work around three phases, before, during and after an incident. That structure remains sound, but should not be forgotten or trivialised as a bygone era.

The difficulty is that institutional memory in shipping is short. Attention moves quickly to the next crisis, of which we often learn through trial and error in how to respond. Knowledge that was built under intense pressure often ends up held by a handful of organisations and experienced individuals, and it fades as they move on and is rarely institutionalised in the same sense as guidance like the Best Management Practices (BMP) series. The weakness of the current edition, BMP Maritime Security, is the broad direction it gives to stakeholders, which allows those at the least compliant end of the spectrum (such as vessels operating under weak shipowners or flags of convenience) to tick boxes without full consideration of the operational picture as it is being experienced in practice.

The harm that outlasts the hijack

The research that followed the first era is sobering. A survey of 101 former hostages and 363 seafarers with no known exposure to piracy found that roughly a quarter of the former hostages showed symptoms consistent with post-traumatic stress disorder. The same study found that trauma influenced career decisions. The damage does not end at release. It follows people ashore, into the workforce and affects who stays at sea.

Smaller clinical studies point the same way. Italian seafarers held for seven to ten months were assessed five months after release, and three of the four received a diagnosis of post-traumatic stress disorder. Bulgarian survivors examined within weeks of release reported detachment from those close to them,

nightmares, sleep disturbance and heightened startle responses. These samples are small and should be read with care, but they are consistent with the larger survey.

Perhaps the most uncomfortable finding concerns what happened next. Research on Filipino seafarers after captivity found that many received no systematic attention or treatment for psychological problems. The ransom had been paid and the ship had sailed, and for many the industry regarded the matter as closed.

Families on shore

The burden does not fall on seafarers alone. In one study of the relatives of the Italian hostages, 42 per cent showed pathological anxiety scores five months after release and a third showed signs of depression. When the group was reassessed against updated diagnostic criteria, seven of twelve relatives showed symptoms within the post-traumatic stress spectrum.

Again, the sample is small, but the implication is clear. A hijacking is a family event. Support that ends at the gangway leaves much of the harm untouched.

This is why family liaison mattered so much in the first era. Someone had to tell relatives the truth, in plain language and on a schedule they could rely on, through months of silence and rumour. That is skilled work and it cannot be improvised on the day.

Communication under pressure

Analysis of 173 recorded exchanges between a master and a negotiator during a real hijacking offers a rare window into how crews cope. The study found that the master's coping changed when the negotiator's responses became too minimal.

The point is a practical one. How shore-side teams speak to a crew in captivity is part of their welfare. Honest information, brief acknowledgement and psychological support help people hold together. The author urged that pre-piracy training should include practical examples of these dynamics, and that is worth rehearsing between crews and managers well before any transit.

Overlapping pressures

The seafarer of 2026 faces a more crowded threat picture than the seafarer of 2010. Hijackings have resumed in the Gulf of Aden and the Indian Ocean. In August the tanker Sibu 1 became the sixth commercial vessel seized by Somali pirates since April, taken by six armed men east of Al Mukalla in Yemen. Puntland's maritime police recovered it in late September after a 48-hour operation, and all 20 crew were unharmed. Five of the six vessels held by Somali pirates in late August have since been released, but the pace of seizures this year shows how quickly the threat has returned.

The conflict between Iran and the United States, which began on 28 February, has now placed merchant seafarers directly in the line of fire. By the end of September the International Maritime Organization had recorded 24 seafarers killed across 85 incidents involving commercial shipping in the Strait of Hormuz and the wider Middle East since the war began. On 23 September the bulk carrier Cape Dao, with 28 crew on board, was reportedly struck by two torpedoes off Oman's Musandam peninsula. Suraj Yadav, a 23-year-old wiper who had joined the ship barely a month earlier, was killed and a second seafarer was injured, while the remainder of the crew were rescued by the Oman Navy. A seafarers' union official who spoke with the survivors reported that they escaped only because of where they happened to be on the ship, and observed that in the attacks he has followed, the bridge, the accommodation and the engine room are the areas most often struck. Neither Iran nor the United States has claimed responsibility for the strike.

Mr Yadav spoke to his family two hours before the attack and showed them footage of his cabin and workplace. At the time of writing his family were still waiting for his body to be repatriated so that the final rites could be observed. For those of us who work on seafarer welfare, this is what the agenda looks like in practice. It is not a policy statement or a helpline number. It is the treatment of a family who

need accurate information, prompt repatriation and a named person to speak to, and it is the kind of support the humanitarian programmes of 2008 to 2012 sought to provide.

Each of these is a welfare problem as well as a security or legal one. A crew that has endured a hijacking, a drone strike and a long detention in a single contract has been asked to absorb a great deal.

The wider evidence on seafarer mental health tells us the baseline is already fragile. Social isolation, distance from families, fatigue and long working hours are the main drivers of mood disorders at sea. Researchers have argued that the industry leans too heavily on reactive, behaviour-based remedies and needs proactive employer investment instead.

The pandemic offered a useful lesson here. A survey of 817 seafarers, alongside interviews with 26 stakeholders, found that the most effective support measures were not exotic. They included communication with family, timely crew changes and a positive, collegial atmosphere on board. These measures are inexpensive and they work.

The moment of boarding

Of all the welfare decisions taken during a hijacking, the decision to retake the vessel by force is among the most consequential, and it is one that the shipping industry has yet to discuss openly enough.

Recent events off Somalia illustrate what is at stake. The tanker MT Honour 25 was seized on 21 April by six armed men with 17 crew on board, and it has since been retaken by Puntland forces. Five crew, three Pakistani nationals, one Indian and one from Myanmar, were killed by the pirates, four others were injured and 16 suspected pirates have been captured. These appear to be the first crew deaths at the hands of Somali pirates in more than a decade. Accounts of when the killings took place differ. Puntland's information ministry has said the crew were killed before regional forces boarded. A statement from the Puntland Maritime Police Force, as reported in Pakistan, indicated that the pirates opened fire on the hostages during the operation, and two surviving Pakistani sailors have said the pirates killed their crewmates while fleeing the maritime police. It would be unsafe to attribute the deaths to the responders themselves. What the episode does demonstrate is the danger that armed men on board pose to the seafarers they hold and how narrow the margin for error becomes once a recovery is under way with crew still exposed. After five months in captivity, the survivors now face the recovery process described earlier in this article, and the families of the dead are spread across at least three countries.

The contrast with the attempted hijacking of Golden Arsenal on 1 July is instructive. Pirates got aboard, but the crew reached their citadel, naval forces coordinated a response and the vessel continued on its voyage. The outcome differed because the seafarers were secure while others acted.

The principle that follows is straightforward. A forced boarding places armed criminals, armed responders and unarmed seafarers within the same confined space, and the seafarers are the only party unable to protect themselves. Where the crew have reached the citadel, a forced boarding should not proceed until every one of them has been confirmed as secure inside it. Confirmation is the operative word. An assumed headcount is not a headcount, and a plan that depends upon the crew being safe should not be launched in the hope that they are.

The recovery of Sibu 1 shows that a forced operation can also end well when crew have been held for weeks and no citadel is available. Where a vessel has been in pirate hands for some time, the same logic holds in a different form. Responders should know where every member of the crew is, and in what condition, before they act.

This is not an argument for inaction. Prolonged captivity carries its own toll, as the research above demonstrates, and a citadel is a temporary refuge and not a place in which to wait out a siege. The pressure to act quickly is understandable, particularly for coastal authorities and naval forces operating in

difficult circumstances. But the sequence matters. Establishing where the crew are, and that they are safe, comes first. The decision to intervene follows.

The Cape Dao offers a related lesson. A citadel protects against boarders, but it offers no defence against a torpedo, and the survivors owed their lives to where they happened to be when the ship was struck. In both cases the location and condition of the crew at the decisive moment determined who lived, and that is something owners, managers and responders can plan for in advance and not leave to chance.

Welfare is risk management

A prepared vessel is a difficult target. Citadel drills, watchkeeping and access control all reduce the chance that an attack succeeds. However, those measures depend on people who are trained, rehearsed and confident enough to act under pressure. Preparing a crew psychologically is part of preparing the ship.

The same is true after an incident. The humanitarian sector offers a useful model. The International Committee of the Red Cross developed a seven-phase care model for staff taken hostage. It combines coordination between the actors involved, long-term peer and organisational support, guided reintegration into work and specialist counselling where needed. Recovery is treated as a process managed over months and planned in advance. Shipping can adopt the same logic. Welfare should be assessed alongside geography, vessel speed, freeboard and cargo when a voyage through an exposed area is being planned.

The crews who were held between 2008 and 2012 remember what happened to them and what help did or did not arrive. The question for the coming months is whether the rest of the industry remembers it too.



Dr Jessica Simonds

ASSISTANT PROFESSOR, RABDAN ACADEMY, UNITED ARAB EMIRATES

Dr Jessica Simonds is Assistant Professor in Defence and Security at Rabdan Academy. Her research covers counter-piracy, risk governance and management, and maritime insurance. She is the author of a Routledge monograph on maritime insurance and piracy in the Indian Ocean.

SOURCES & FURTHER READING

- Abila, S. S. and Tang, L., Trauma, post-trauma, and support in the shipping industry: The experience of Filipino seafarers after pirate attacks, Marine Policy, 46, 132–136, 2014. https://doi.org/10.1016/j.marpol.2014.01.012
- Aebischer Perone, S. et al., Psychological support post-release of humanitarian workers taken hostage: the experience of the International Committee of the Red Cross (ICRC), British Journal of Guidance & Counselling, 48(3), 360–373, 2018. https://doi.org/10.1080/03069885.2018.1461193
- Aleksandrov, I. et al., On psychological and psychiatric impact of piracy on seafarers, Journal of IMAB, 21(4), 2015. https://doi.org/10.5272/jimab.2015214.991
- Badam, R. T., 'Leave our children alone,' says family of Indian sailor killed in Strait of Hormuz, The National, 30 September 2026. https://www.thenationalnews.com/news/uae/2026/09/30/indian-sailor-killed-cape-dao-family-question-iran-us/
- Dimitrevich, A. and Torskiy, V., Maritime Piracy Humanitarian Response Programme (MPHRP), TransNav, 8(3), 419–421, 2014. https://doi.org/10.12716/1001.08.03.13
- Froholdt, L. L., Coping with Captivity in a maritime hijacking situation, WMU Journal of Maritime Affairs, 16, 53–72, 2017. https://link.springer.com/article/10.1007/s13437-016-0101-0
- Nittari, G. et al., Factors affecting mental health of seafarers on board merchant ships, Reviews on Environmental Health, 2022. https://doi.org/10.1515/reveh-2021-0070
- Osman, N., Somali pirates killed oil tanker crew before rescue, official tells BBC, BBC News, September 2026. https://www.bbc.com/news/articles/crjw5jp2de7go
- Sampson, H. and Ellis, N., Stepping up, the need for proactive employer investment in safeguarding seafarers' mental health and wellbeing, Maritime Policy & Management, 48(8), 2021. https://doi.org/10.1080/03088839.2020.1867918
- Seyle, D. C., Fernandez, K. G., Dimitrevich, A. and Bahri, C., The long-term impact of maritime piracy on seafarers' behavioral health and work decisions, Marine Policy, 87, 23–28, 2018. https://doi.org/10.1016/j.marpol.2017.10.009
- Simonds, J., Maritime Insurance, Risk, and Seafarer Security: Navigating Piracy in the Indian Ocean, Routledge, 2025.
- Somali Guardian, Puntland forces free hijacked oil tanker Sibu 1 off Somalia's coast, all 20 crew safe, September 2026. https://www.somaliguardian.com/news/somalia-news/somalia-puntland-forces-free-hijacked-tanker-sibu-1-crew-safe/
- Splash247, First Somali piracy crew deaths in over a decade, September 2026. https://splash247.com/first-somali-piracy-crew-deaths-in-over-a-decade/
- Tang, L. et al., Seafarers' mental health during the COVID-19 pandemic, Marine Policy, 145, 2022. https://doi.org/10.1016/j.marpol.2022.105276
- The Express Tribune, Govt to bring home bodies of slain sailors: FO, October 2026. https://tribune.com.pk/story/2632354/govt-to-bring-home-bodies-of-slain-sailors-fo
- The Week, How Indian Navy stopped pirates from boarding Tamil Nadu-bound cargo ship 'Golden Arsenal', 2 July 2026. https://www.theweek.in/news/maritime/2026/07/02/how-indian-navy-stopped-pirates-from-boarding-tamil-nadu-bound-cargo-ship-golden-arsenal.html
- Ziello, A. R. et al., Psychological consequences in victims of maritime piracy, the Italian experience, International Maritime Health, 64(3), 2013. https://pubmed.ncbi.nlm.nih.gov/24072540/
- Ziello, A. R. et al., Psychological distress in families of victims of maritime piracy, International Maritime Health, 65(1), 2014. https://pubmed.ncbi.nlm.nih.gov/24677125/
- Ziello, A. R. et al., Sea piracy sequelae, assessment according to the DSM-5, International Maritime Health, 65(4), 2014. https://pubmed.ncbi.nlm.nih.gov/25522708/

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.