Redrawing the ‘mental map’ of maritime risk

George Mangos, co-founder, SOKANA

For generations, maritime risk was shaped by factors that could be predicted. From weather and machinery to piracy and war; risks that had flags, borders, and in most cases, precedents. It was orderly, chartered and insurable. However, it is a world that is fast changing and being reshaped by unflagged drones, stateless code and trade routes that are not being altered by monsoons, but by tweets, tariffs and airstrikes. While geography is still important, politics, ambiguity and data matter more.

Within this dynamic, as an industry, we are now not just redrawing shipping lanes, we are having to redraw the very mental maps by which we navigate uncertainty and risk.

The evidence of this is plain to see. The Red Sea, which was once a vital artery of global trade, is now effectively a combat zone, with over 130 attacks on commercial vessels in the past 18 months; not from conventional navies, but irregular actors deploying cheap weapons such as drones. The Panama Canal, which was a marvel of engineering, is now a hostage to nature, with droughts forcing the authorities to slash vessel transits by one third. In the Arctic, as climate change forces the ice to retreat, it is now becoming a new international trade frontier and central stage for the Great Power Competition between Russia, China and the US as they compete for the opportunities of untapped oil reserves and natural gas.

And on top of all this, the narrow passages through which the vast majority of global trade must pass – the chokepoints – be it Gibraltar, the Bosphorus or the Malacca Strait, are not just becoming tools of leverage in regional rivalries. They are becoming the levers of regional dominance and the fault lines of global economic power that determine who controls the movement of oil, food and raw materials; where the threat of blockades, disruption and slowdowns will be the currency of choice, potentially leaving nations at the mercy of whoever controls specific lanes of transit.

Despite all this, the most dangerous risks that the maritime industry faces are not always visible on a map. Instead, they are coded in ambiguity, often hidden and don’t arrive with a warning shot, but in silence. They are risks without attribution. We now have to question who actually launched the drone that hit a vessel; was it a militia? A state proxy? Or a state in disguise? Who spooked the AIS signal: a prank or a prelude?

When it comes to sanctions, what was once a tool of diplomacy to instigate change has now created oceans of uncertainty, with additional complexities and increased risks. Ship owners now need to be intelligence analysts, scanning every detail, every route and every manifest. As the list of nations, individuals and organisations subject to sanctions continues to grow, they are faced with uncertainty over what exactly they’re allowed to carry, what ports they can legally call at, or whether it will be called into question in the future. Cargo origin is no longer obvious. And with ship-to-ship transfers and obfuscated ownership structures, due diligence now operates at DEFCON 1. Critically, the cost of error, which can be financial, reputational and even legal, could be catastrophic.

On top of all this, cyber adds another layer of risk that the industry has to deal with. In 2024, one in five shipping companies faced a cyber attack. Over the last few years, the majority of the top ten container lines have publicly admitted to being cyber victims at a significant cost. Of course, some of last year’s attacks were tests and not malicious. But many were as a result of criminal activity by global syndicates using cybercrime as a significant source of revenue. And some were also state-backed sabotage cloaked in plausible deniability, using wiper malware to destroy networks and intelligence, sometimes indiscriminately. But, unlike piracy, there is no emergency call for a malware breach. There is no navy that will respond to a corrupted server. The irony is that as we further digitalise the industry, which will continue at pace, we are also exposing it. And despite this, cyber risk remains one of the least standardised – and most opaque – elements in maritime insurance today. This is the paradox; the industry has never had more visibility, but the uncertainty within it has also never been greater.

Digitalisation is fundamentally changing the industry, enabling it to become faster, smarter, more efficient and sustainable. We can now use machine learning to anticipate vessel movements, track cargoes in real-time, and

even forecast arbitrage opportunities. Predictive maintenance, robotic ports, autonomous navigation — these aren't theories. They are prototypes, pilots, and in some cases, policy. However, this is also creating a double-edged sword.

Speed compresses certainty, and the faster we move, the less time we actually have to evaluate risk. For example, we don't just need to know if a fixture is profitable; we also need to ensure it is legal, safe, and insurable. Not in one month, but in 48 hours. Within this new world, the role of relationships grows even more important. Ultimately, trust and human signal will cut through the fog of algorithmic noise. However, in spite of this, the reality is that no shipowner, broker or underwriter has yet built or created a system that combines real-time geopolitical risk, cargo intelligence and live coverage into one integrated platform. This is where the white space exists, and it is here where the future of maritime insurance must take root.

Right now, this leaves us in an age and a place where risk cannot be avoided, but it must be adapted to. And this adaptation begins with asking the right questions.

- What does a route-based insurance model look like when routes are redrawn daily?
- Can we build live intelligence-sharing ecosystems between shipowners and insurers, so we're not just reacting to events, we're predicting them?
- Do our coverage models account for drone attacks without declarations, or cyber sabotage without signatures?
- Can we make insurance responsive to region-specific volatility without pricing out resilience itself?
- And critically, are we building an industry fit for today's risks, or only yesterday's threats?

Within this, we must also remember that fewer than half of the world's merchant vessels are part of P&I clubs. All the real-time data, intelligence, daily updates on sanctions, weather-related systems, natural disasters and other security risks that the clubs provide its members are only seen by 50% of the global commercial fleet. The rest do not have access to this level of intelligence, insight and protection. In effect, there are tens of thousands of vessels navigating blind. This isn't just a market gap; it's a systemic vulnerability.

The history of maritime is engulfed in a story of bold navigation across oceans, empires and eras. And with every new frontier that had to be crossed, there was also a transformation in how we understood and priced risk. Today, we must do the same. We are no longer navigating a sea of 'knowns', but rather a sea of continually shifting risks. Some are geopolitical, some technological, and some are invisible, hiding in the shadows until they are not.

However, the greatest risk we now face is not war, but the weather of digital code. It is 'assumption'. Assuming the maps that we once used still apply. Assuming that the old frameworks will survive new shocks. They won't. It's not about redrawing trade routes, it's about working together to redraw the mental maps we use to navigate uncertainty; maps that are dynamic, collaborative and built not just to survive volatility, but to actually lead through it.