METIS INSIGHTS

DRYAD® GLOBAL

OLD TOOLS VS NEW THREATS?

The ISPS Code and Modern Maritime Security

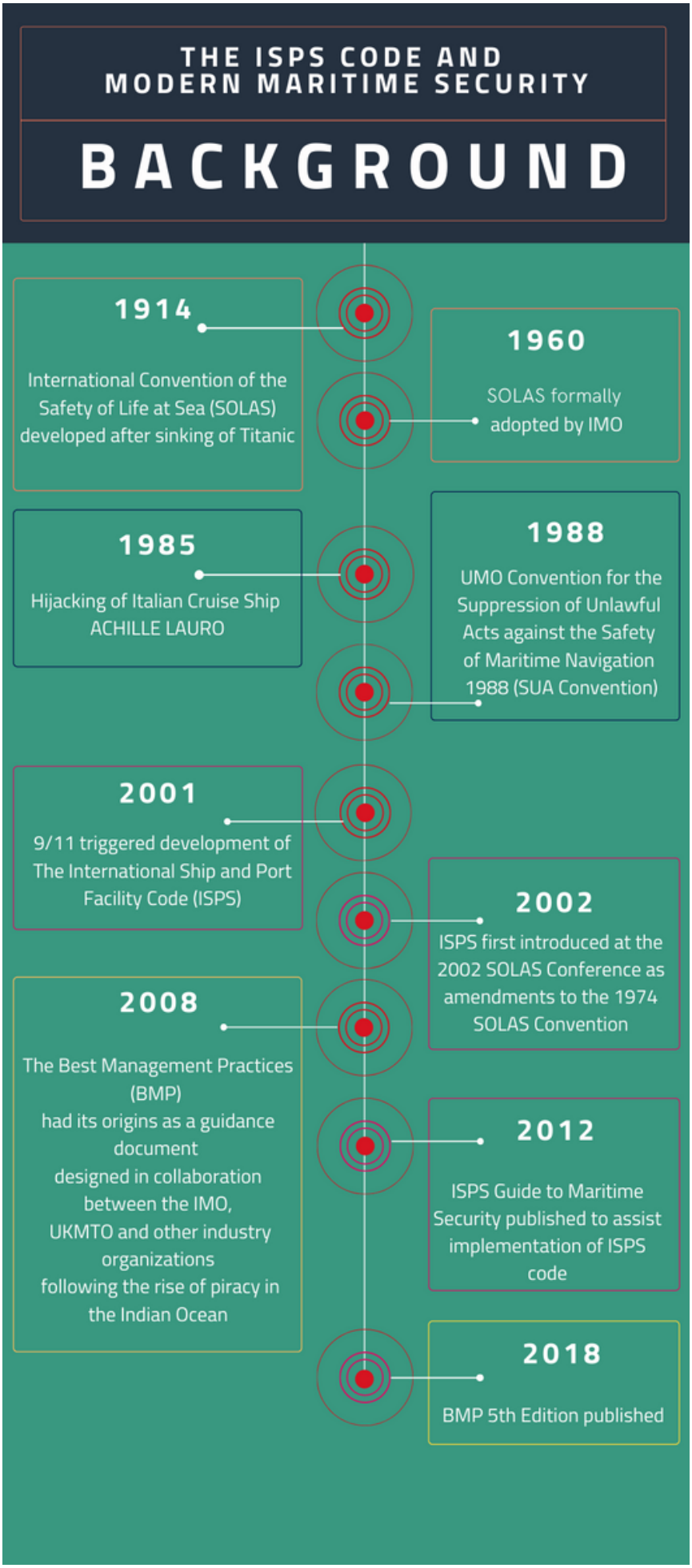
Introduction

Historically, maritime security guidelines and best practise have evolved in response to incidents or issues that have resulted in a clear gap in the provision of the procedural core function, security. The timeline of the implementation of significant maritime security legislation and conventions illustrates this pattern of development.

Post 9/11, the US raised concerns about the maritime domain potentially becoming a target for international terrorism. The ISPS Code provides a framework for the assessment and detection of possible security threats to ships or port facilities. It applies to vessels engaged in international voyages including passenger vessels, cargo vessels of 500 gross tonnage and above, mobile offshore drilling units, and port facilities.

Analysis by
Shannon McSkimming
Dryad Global

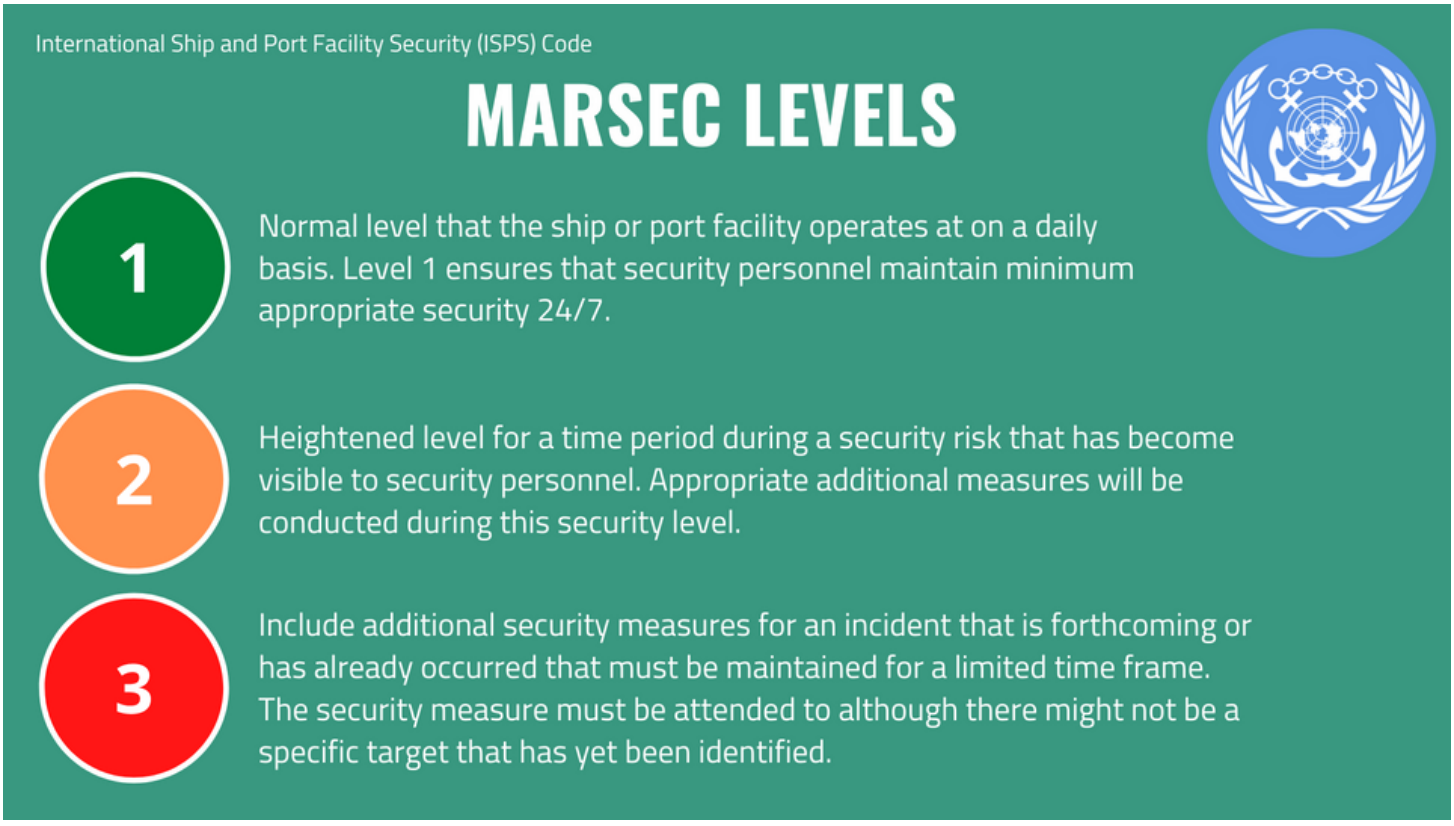
Analysis by
Casper Goldman
Dryad Global



The 5 core objectives of the ISPS Code are:

1. To facilitate cooperation between all parties involved in assessing and detecting security threats and implementing preventative security measures.
2. To determine the roles and responsibilities of all parties concerned with safeguarding maritime security.
3. To ensure collation and exchange of maritime security- related information
4. To provide methodology for ship and port security assessments
5. To ensure adequate and proportionate maritime security measures are in place on board ships and in ports.

There are 3 MARSEC levels in the ISPS Code, reflecting increasing levels of security measures and varying operational roles and responsibilities between parties and operational procedure at each level.



The IMO published the 'Guide to Maritime Security' and the ISPS Code in 2012 to assist in the implementation of the code. However, there have been difficulties with implementation and recent debate about continuing relevance and keeping the code dynamic and adaptable.

Putting the Code to Use

The ISPS Code has given effect to several legal responsibilities for SOLAS contracting governments, as well as vessels operating under their flags and within ports of their jurisdictions.

These include but are not limited to:

- The mandatory appointment of a PFSO (port facility security officer)
- The mandatory appointment of a CSO (company security officer)
- The mandatory appointment of an SSO (ship security officer)
- The development of a SSP (ship security plan)
- A PFSP (port facility security plan)
- The setting of ISPS security levels for ports by relevant authorised persons.

> *"The code does not specify what knowledge and training nor how individuals in these positions are certified."*

According to the ISPS Code, those in the key security positions outlined above should "have knowledge and have received training". However, the code does not specify what knowledge and training nor how individuals in these positions are certified.

Instead, there is a set of additional non-mandatory guidelines that provide more detail:

- Guidance on training and certification for key security personnel outlining required competencies
- Required knowledge, understanding and proficiency
- Methods for demonstrating competence
- Criteria for evaluating competence

However, this section is non-mandatory and therefore the degree to which these are implemented fully relies on the contracting government. Whilst contracting governments are technically not required to adopt these additional guidelines, the three largest flag states (Marshall Islands, Panama & Liberia – with flagged vessels totalling approximately 40% of global shipping) have all published a list of approved training courses in line with these guidelines for security personnel certification. This means that the code is widely and thoroughly implemented. Also, like the training of ISPS mandated security officers, all flag states have a list of recognised security organizations (RSOs) or a dedicated government authority that are authorised to audit the ship security plan and subsequently issue an international ship security certificate, which verifies compliance with the mandatory section (part A) of the ISPS Code. This further emphasises the extent to which the code is implemented and the subsequent impact it has on maritime security.

Where to Adapt?

The strength of the ISPS Code lies in the clarity and uniformity it has brought to maritime security. A common understanding of security levels, roles and responsibilities of different security officers, and security procedures has brought together contracting governments, government agencies, local administrations, shipping and port industries, and other stakeholders in identifying and tackling security threats. This common language facilitates powerful cooperation that is guided by a common methodology for ship and port security assessments for each security level. However, this methodology is where the core challenge of the code lies.

The ISPS Code is currently limited in its capacity to pre-emptively identify emerging threats because the code is focused on mitigation measures and post-event response.

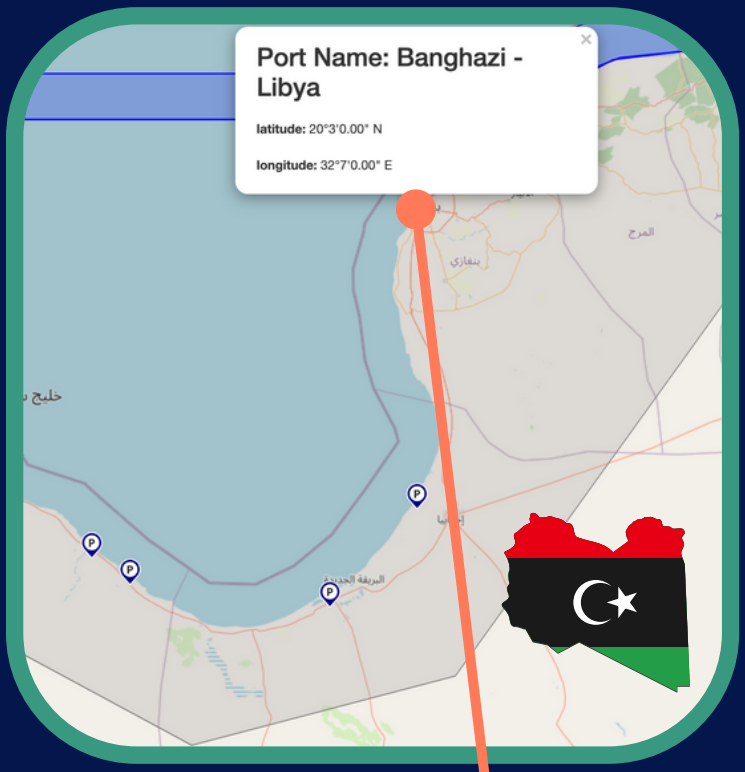
The **primary example** of a developing maritime security threat is cybersecurity. In the nearly 20 years since the implementation of the ISPS Code, the technology utilised in all commercial industries has changed drastically. While increased capacity, connectivity, monitoring and improved security measures have doubtlessly led to improvements across the shipping industry, they also present new threats. Due to the inherent interconnected nature of the maritime industry, the ISPS Code for both ports and vessels has to be workable in a space with a wide variety of potential spill-over risks from industries and companies co-operating with them. This was seen most notably in cyberspace in the NOT PETYA attack which originated in a small Ukrainian software company whose tax filing software serviced a large number of Ukrainian businesses.

The attack spilled over into Maersk through their Ukrainian branch which had the software on one of their computers and simultaneously infiltrated every connected device in their network, severely impacting Maersk's systems worldwide, including their 76 ports and 800 vessels. The ISPS Code is intended to improve security of vessels and port facilities, limiting the impact of a security incident if it happens and to maintain functionality of systems in the event of an incident. A cyber-attack now has the potential to severely compromise both physical security and operability of ports and vessels. To address this vulnerability, the International Association of Ports and Harbours (IAPH) in cooperation with World Bank has recently submitted cybersecurity guidelines to the IMO for consideration. Whilst this is a step in the right direction for the industry to self-implement improvements, it highlights the importance of introducing a more formal process that continuously assesses whether the ISPS Code is up to date and coherent with emerging risk factors, such as cybersecurity.

A **further opportunity** for the ISPS Code to adapt is to account for greater reactivity when faced with certain traditional threats, such as interactions with hostile foreign militaries and/or state backed hostile groups.

The port MARSEC levels of the code are determined by the authority of the country they are in, with visiting vessel masters either matching the port ISPS security level or, if the vessels ISPS security level is higher than the ports, issuing a Declaration of Security. This process can be hindered or compromised in countries without a functioning government or designated authorities, as was seen during the Libyan Civil War.

An example of this occurred in 2014, when Libya's Port of Benghazi was assessed to be non-compliant and continued to operate during significant onshore violence, recent airstrikes to the port, and the stated intent by General Haftar to shell ships that entered the port. Despite the clear and imminent threat to operations and personnel, the Port authority were unable to implement adequate and proportionate maritime security measures in port to protect facilities and visiting vessels, as militias had taken over control of the port.



Benghazi Port, Libya 2014

A **third limitation** of the ISPS Code connects to how the code treats the security impacts of goods in ports. The ISPS Code mandates that the port security assessment accounts for the identification of potential targets and weaknesses relating to the transport of goods, including explosive and dangerous material, which may be located and/or stored in a port at some point. It highlights the importance of recognising and implementing security measures around threats to and from dangerous materials, however it also emphasises the responsibility of ports and contracting governments to ensure adequate implementation.

Despite the requirement for constant assessment of security measures and risks, it is not feasible for holistic port security to be reassessed every time new cargo arrives. This explains why the security assessment of transiting cargo predominately accounts for stationary risk, rather than transitory and adaptive threats.

A **fourth limitation** is that the three levels of ISPS do not adequately account for the nuance of the multidimensional and varying nature of risk that ports and vessels face.

For example, there have been several tit-for-tat incidents involving explosions with UAVs and WBIEDs in the Persian Gulf and the Gulf of Oman between Iran and Israel, and whilst this may prompt a higher ISPS level, vessels that are not affiliated with Israel and Iran have no reason to operate at a higher risk posture.

Source: Conflict Armament Research

Similarly, when entering a high-risk area and implementing a higher level of ISPS onboard, vessels would implement hard lockdown measures, and whilst this partially mitigates the risk of piracy, this is not an effective deterrent for WBIED and UAV attacks. This highlights the importance of considering the nature of the threat a vessel might face. Vessels operate under ISPS levels set by their Flag States when underway, and whilst these three levels provide useful baseline threat mitigation, their one-size-fits-all nature is ill-equipped to holistically assess and mitigate the risk during a transit. Individual ISPS certifications cannot account for every security scenario that a vessel may encounter at ports around the world without supplementary advice about the local situation prior to transit.

The final limitation of the ISPS Code relates to its core objective of supporting the "early and efficient collation and exchange of maritime security-related information at national, regional and international levels". Without centralised and accessible information regarding the current ISPS levels in ports, the ability for all parties to adequately prepare and implement the appropriate security measures onboard visiting vessels is limited, with ISPS only being advised on approach to the port.

Security in Practice

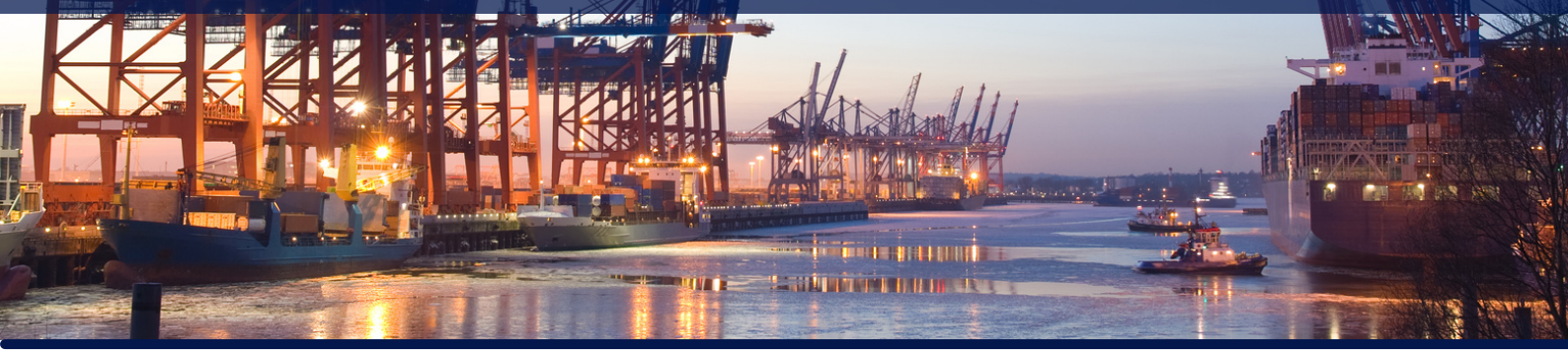
The ISPS Code has made a significant, positive difference to maritime security, bringing about formalised and standardised maritime security for ships and ports with clear enforcement systems and extensive guidelines for implementation, regulation, and designation of responsibility. However, in its current form, the code does not adequately account for the nuance of the multidimensional, varying, and evolving nature of risk in the maritime industry. This is less the result of inadequate planning, but reflective of the ever-evolving nature of risk.

Informed parties would be hard pushed to debate the legitimacy of the ISPS Code, however increasingly there are questions regarding its relevance within the contemporary security environment.

Centralised and accessible documentation of the current ISPS level at ports internationally could, for example, assist the IMO in including all parties involved in maritime security concerns, including vessel owners and companies to ensure the safety of planned operations and transits.

Given the significance of the ISPS Code in being the central tenet around which much of today's maritime security framework is based, it remains vital for the document to continue to reflect the contemporary security environment that it seeks to mitigate against. It has been nearly 20 years since the ISPS Code was adopted, and in that time significant changes have occurred in the maritime industry, particularly with respect to cybersecurity concerns giving rise to legitimate questions as to the contemporary relevance of this framework.

With a reformed, reflexive, and up-to-date ISPS Code, all actors can play their part in ensuring that global maritime shipping is a safer place for all those involved.



WAR RISK COVER

LEVERAGE A WINNING WAY

Dryad Global have married deep knowledge of maritime risk with insurance expertise to offer you a competitive and tailored war risk premium.

Why pay more if you have done more to reduce your risk exposure?

Dryad has partnered with an approved Lloyd's of London broker with over 70 years market experience and knowledge! Cambiaso Risso, branded in London as CR international, is one of the largest European players for retail business insuring more than 9,500 vessels. CR affirmed its brand in the market thanks to the excellent servicing in providing the most suitable insurance arrangements combined with an impeccable assistance on claims. CR has an international network of offices acrossn Norway, Italy, France, Greece, Turkey, Singapore, UK, US and South Korea.

Place war risk separately to Hull and Machinery cover

The days of getting the best deals in bundles have passed- with H&M rates climbing (irrespective of whether you combine war risks) the best deals for war risks can be found with a specialist provider.

Peace of mind for owners

Owners can rest assured that cover operates back-to-back with the existing H&M as the War clauses are automatically amended to match or follow the basis of the H&M conditions such as ITCH, Nordic Plan, American Institute clauses etc.

Policies can be tailored to fit your individual needs!

FIND OUT MORE

We only work with A-rated markets

By working only with the best underwriters who depend on their reputation, you can rest assured that any claim will be handled efficiently, professionally and with a **customer-first** approach.

Benefit like the large war risk pools

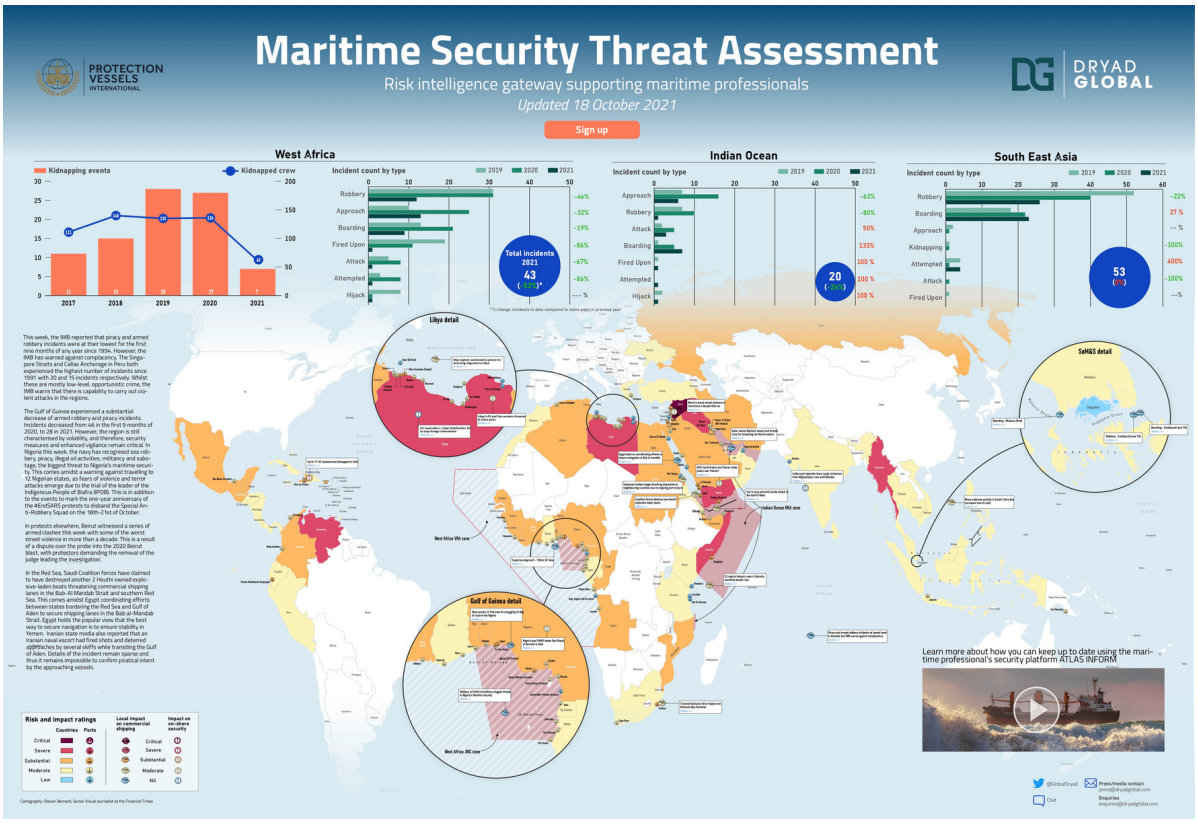
Most large war risk pools are re-insured into the London markets where our providers sit.

NEW

TRITON SCOUT

MARITIME SECURITY THREAT ASSESSMENT

Dryad Global brings you the latest actionable analysis at your fingertips.



FIND OUT MORE

- The macro and the micro in one accessible, intuitive infographic.
- Powered by humans for humans, optimised by the latest AI and tech integrations.
- 360° near real-time reporting and analysis compiled by our team of experts.
- Instant, quick and concise visuals to identify threats against your people and assets.
- Make commercial decisions fast and with confidence 24/7/365.

DRYAD GLOBAL 71-75
SHELTON STREET LONDON
WC2H 9JQ

dryadglobal.com

+44(0)3301 244 344