Siren
Powering investigations

SIREN PERSPECTIVE

Fortifying Maritime Security With Advanced Strategic Intelligence

Author - John Randles
Contributor - Bob Griffin

Author: John Randles
CEO of Siren

John Randles has been working with organisations all over the world solving Law Enforcement, Public Safety and Intelligence challenges with technology since 2017. John is the Chief Executive Officer at Siren, based in Dublin, Ireland. John has been in the Global Data Management space for over twenty years and played a leading role in a number of well-known technology success stories. John was CTO of Eontec, later acquired by Siebel in 2004, and CEO of Polarlake, later acquired by Bloomberg in 2012. John spent five years as CEO of Polarlake for Bloomberg after the acquisition. John has a degree in Computer Engineering from the University of Limerick in Ireland.

Contributor: Bob Griffin
Chairman of Siren

Bob Griffin has been a key player in the software industry for Law Enforcement, Public Safety and Intelligence for more than 25 years. He sold his company, i2/COPLINK, to IBM, where he remained as the General Manager for the Safer Planet and Smarter Cities brand until February 2017. Bob is a distinguished alumnus of the Naval Post Graduate School's Center for Homeland Defense and Security's Executive Leadership Program in Monterey, California. Bob has addressed the World Economic Forum on the use of technology for critical infrastructure protection, and the World Conference on International Telecommunications on the topics of defense, disinformation, and cyber warfare.

Maritime trade is the backbone of international trade and the global economy accounting for in excess of 80% of traded goods. UNCTAD figures for 2021 show shipments reached 11 billion tons[1] globally. Container shipping is the dominant mode of transport for physical goods and volumes through major container shipping ports such as Shanghai, Singapore and Hong Kong simply cannot be subjected to sufficiently thorough physical checks without bottlenecking trade. According to World Shipping Council statistics[2], seven of the top 10 ports by shipping volume are controlled by China, accounting for in the region of 200 Million TEU (Twenty-foot Equivalent Units) annually. China also "owns, co-owns or operates a further 96 foreign ports" around the world[3] and requires Chinese companies overseas to report intelligence on foreign entities to the Chinese government[4].

Maritime security intelligence plays a pivotal role in safeguarding this global trade, ensuring the safety of vessels and preventing maritime crimes and terrorist activities. In an era where international waters are increasingly vulnerable to various threats, the need for accurate, timely, and actionable intelligence is paramount. This Siren Perspective delves into the world of modern maritime security intelligence, exploring the challenges and the evolving strategies to counter maritime threats effectively.

Shipping and port facilities take their security responsibilities seriously and evincing their response to modern-day threats with the implementation of The International Shop & Port Facility Security Code (ISPS), thereby adapting their security stance to reflect the changing terrorist threat after 9/11 and the bombing of the French oil tanker Limburg in 2002. But the risks at sea are ever evolving and in an era of constant technological change, the necessary vigilance must take a more holistic look at the threats faced by vessels and ports but also by nations, security forces and commercial entities.

Given the heightened political tensions in recent years, it's evident that maritime security is now intrinsic to Great-power competition (GPC)[5] as state actors jockey for dominance through economic disruption and nefarious intelligence gathering operations. This radically alters the focus of maritime security which has historically directed available resources towards narcotics smuggling by transnational crime gangs.

Disruptions to the orderly operation of a large scale supply chain can have a devastating impact on global trade, interfering with carefully planned logistics schedules. The closure of a single supply route can "cause a knock-on log jam that affects the world economy at the rate of billions of dollars every day" according to one UK-based maritime analyst[6].

The sheer number of personnel involved in protecting our oceans from different yet related domains underpins the need for data oversight and collaboration through multi-agency security groups. Security roles span Navy departments, Coast Guard and border patrols, maritime criminal intelligence & security specialists and data analysts, as well as port and vessel security personnel. Vigilance, cooperation and preparedness are vital.

1 https://unctad.org/rmt2022#:~:text=Riding%20on%20the%20surge%20in,recorded%20in%20all%20developing%20regions.

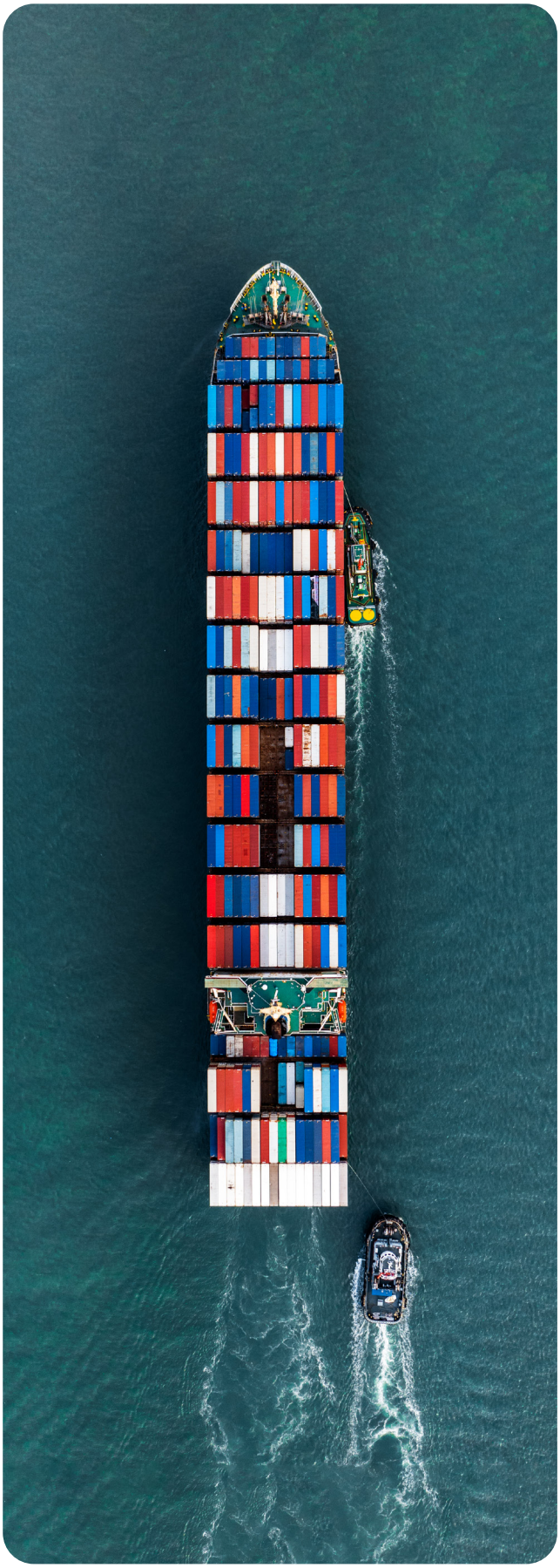
2 https://www.worldshipping.org/top-50-ports

3 https://direct.mit.edu/isec/article-abstract/46/4/9/111175/Pier-Competitor-China-s-Power-Position-in-Global?redirectedFrom=fulltext

4 https://foreignpolicy.com/2023/09/20/china-shipping-maritime-logistics-lanes-trade-ports-security-espionage-intelligence/

5 https://www.cna.org/reports/2020/06/DOP-2020-U-025085-Final.pdf

6 https://www.securityweek.com/vulnerable-maritime-supply-chain-threat-global-economy/



The threat at sea now also includes global communications via undersea cables totalling in excess of 1.2 million kilometres in length and energy sources including offshore wind farms and oil & gas pipelines.

The scale of this multilayered maritime threat demands a proportionate, proactive security posture that can reduce vulnerabilities, thereby safeguarding energy and communications assets and facilitating continuous maritime trade with minimal reactive measures. While tactical responses are vitally important, the absence of adequate data-driven foresight hinders the success rate of such interventions.

The large number of potential attack scenarios and respective control options make it difficult to evaluate the effects of security measures. A strategic outlook requires a comprehensive approach comprising satellite imaging, remote sensing, AI, machine learning and data analytics working in conjunction with the traditional interventions of maritime law enforcement.

UNDERSTANDING MARITIME SECURITY INTELLIGENCE

Law enforcement departments need to collect maritime security intelligence. It is the collection, analysis, and dissemination of information related to maritime activities, threats, and vulnerabilities. It encompasses a wide range of data sources including satellite imagery, radar systems, vessel tracking, electronic charts & traffic monitoring, weather visualisation and human intelligence (HUMINT). The scope of maritime security covers both state and non-state actors involved in countering activities such as piracy, smuggling, terrorism, and illegal fishing.

Importance of Maritime Security Intelligence

The importance of reliable, accessible and timely intelligence to maritime security cannot be overemphasised. It serves multiple purposes:

Mitigating geopolitical vulnerabilities:

China's global maritime prowess is growing and with most global seaborne trade encountering CCP-controlled assets, the associated risks are profound - counterintelligence is vital.

Safety of Vessels: Timely, reliable security information enables Coast Guard officials to guide ships to avoid dangerous areas, navigate safely, and respond to emerging threats effectively.

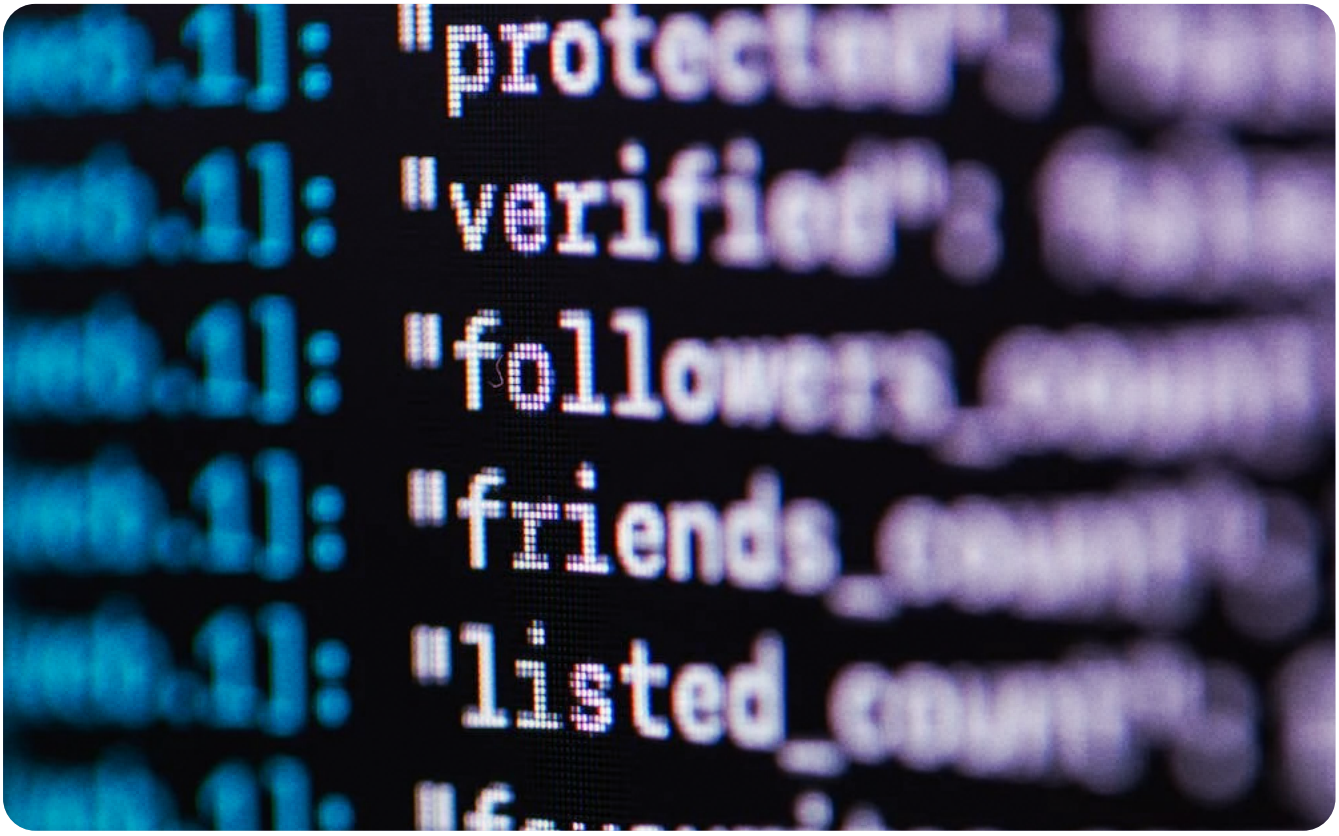
Counter-Piracy Operations: Intelligence helps security forces to understand the capabilities of pirate groups; identify piracy-prone regions and track the movements of pirate vessels, enabling naval forces to plan and execute effective counter-piracy operations.

Safeguarding Supply Chains: Port executives face a myriad of challenges including weather, terminal accessibility, labour shortages and continuity in land transport. Vessel quality, freight volatility and increased regulation pose additional problems. Disruptions are costly, making time intelligence critical to the supply chain operations.

Anti-Terrorism Efforts: Up-to-date data assists Navy surveillance and reconnaissance efforts by effectively monitoring and thwarting terrorist activities, such as the smuggling of weapons or explosives via maritime routes.

Resource Protection: Intelligence helps combat illegal, unreported, and unregulated (IUU) fishing, safeguarding marine ecosystems and food security.

Border Security: Real-time data helps Coast Guard and border patrols in upholding law & order at sea by enforcing maritime borders, deterring human trafficking efforts and mitigating against the illicit movement of contraband weapons and drugs.



SECURITY LEVELS

The International Ship and Port Facility Security (ISPS) Code requires that signatory governments, local administrations, shipping and port industries co-operate in detecting security threats and taking preventive measures against security incidents. The code.applies to commercial ships and offshore drilling entities and details the security responsibilities for vessels and ports. For related vessels, a Ship Security Officer (SSO) has responsibility for implementing the Ship Security Plan, ensuring shipboard personnel are trained, reporting security incidents and proposing amendments and continuous improvements to the Ship Security Plan.
Maritime security is categorised into three bands - SL1 to SL3 with the latter being the most severe threat level.

Security level (SL1): This is the normal threat level. SL1 is the level at which the minimum protective and security measures are in permanent effect.
Security level 2 (SL2): This is the heightened threat level. SL2 is the level at which, as a result of a heightened threat of a security incident, additional protective security measures are maintained for the duration of the threat.
Security level 3 (SL3): The exceptional threat level, SL3 is the level at which, when a security incident is probable or imminent, further specific protective security measures are initiated and maintained for a limited period.

With appropriate security intelligence software in place, the minimum protective standard is raised significantly as awareness of risks and potential threats are increased. This preventative approach to managing maritime risk ensures that key decision-makers are proactively informed of relevant risks and the need to escalate to SL2 is thereby reduced.

CHALLENGES IN MARITIME SECURITY INTELLIGENCE

The threat to security at sea is not limited to the visible, physical danger which already stretches available resources. The composition of the threat has altered radically and has in itself become a sophisticated[6], strategic supply chain with input from state intelligence or criminal enterprises before an attack is executed.

Vastness of the Maritime Domain

One of the primary challenges in maritime security intelligence is the sheer vastness of the maritime domain. Covering over 70% of the Earth's surface, it poses difficulties in monitoring and surveillance. This surveillance is made all the more difficult by the use of submarines and 'narco torpedoes' to distribute contraband.

Diverse Threats

Maritime threats are multifaceted, ranging from piracy and smuggling to environmental disasters and the growing challenge that is Great-power competition. The diversity of threats requires intelligence agencies to adapt and stay ahead of evolving tactics.

Considering that "virtually all of the world's seaborne goods" pass through or near Chinese infrastructure, China's commercial leverage is a potentially critical advantage in the ongoing geo-political struggle[8].

Maritime threats don't solely manifest physically at sea or on vessels. Increased regulation, inflation, labour shortages, volatile cargo, rail & road network disruptions and land-based extreme weather events all have the potential to cause significant port congestion, bottlenecking supply chains and creating havoc in maritime trade.

Limited Resources

Resource constraints, both in terms of personnel and technology, can hinder effective intelligence gathering and analysis. Some analysts suggest elements of the maritime industry are up to 20 years behind the pace in terms of cyber security[8].

Information Sharing

International cooperation and information sharing among nations, agencies, and organisations are crucial. OSINT data sources are advantageous but concerns about data security and sovereignty in uncertain political times can hinder international collaboration.

Technological Advancements

As technology evolves, increasingly sophisticated maritime criminals are able to exploit new tools and methods, necessitating continuous innovation in intelligence capabilities to keep ahead of emerging threats.

Intelligence Gathering Methods

Available data relating to maritime security is wide and varied - combining these datasets and cross-referencing with proprietary data can be a mammoth manual endeavour. Outlined below are methods of data collection currently in use in maritime security - scaling the data gathering effort to enable efficient analysis requires a specialist solution, such as Siren.

Satellite Imagery

Satellites now provide very high resolution (VHR) optical imagery which is a valuable source of information for monitoring vessel movements, identifying suspicious activities, and tracking

7 https://press.un.org/en/2019/sc13691.doc.htm

8 https://foreignpolicy.com/2023/09/20/china-shipping-maritime-logistics-lanes-trade-ports-security-espionage-intelligence/

9 https://maritime-zone.com/en/news/view/how-new-maritime-technologies-will-change-the-shipping-industry

environmental changes, such as oil spills and harmful algal blooms which can have a devastating impact on the fishing industry. Recently, the European Maritime Safety Agency (EMSA) awarded a two-year contract to European Space Imaging (EUSI) and Airbus to deliver VHR imagery aimed at improving monitoring and reactivity in maritime security[9].

AIS (Automatic Identification System)

AIS transponders on vessels transmit real-time data, including ship location, speed, and cargo information. This data is instrumental in tracking ships and their activities and the International Maritime Organisation require large ships and other commercial vessels to broadcast data such as their position, course and speed via AIS[10]. This is a key piece of data in real-time risk assessment.

Radar Systems

Coastal radar systems help detect vessels in proximity to the coastline, including detecting smaller vessels such as trawlers and dinghies thus aiding in surveillance and response efforts.

HUMINT (Human Intelligence)

Human intelligence sources, such as informants and undercover agents, play a crucial role in gathering information about illicit maritime activities and criminal organisations.

Open Source Intelligence (OSINT)

Information available in the public domain, including social media and news reports, maritime traffic and weather data can provide valuable insights into maritime threats, likely behaviours and trends.

10 https://spacewatch.global/2023/05/eusi-and-airbus-to-provide-emsa-with-satellite-imagery-service/

11 https://www.navcen.uscg.gov/automatic-identification-system-overview

12 https://edition.cnn.com/2023/10/03/asia/us-philippines-naval-exercise-sama-sama-intl-hnk-ml/index.html

KEY PLAYERS IN MARITIME SECURITY

International Naval Forces

Naval forces of coastal states are instrumental in maritime security. They conduct patrols via ships, submarines, aircraft and satellite, responding to threats, and sharing intelligence with international partners. Naval forces also engage in co-operative multilateral training events including Maritime Partnership Exercise (MPX) conducted by the Indian Navy. While co-operative efforts are welcome, it's hard to ignore the threat to stability of the maritime industry in the South China Sea with the Philippines, US and other Western naval forces conducting military drills[11] - the latest development in a long-running territorial dispute between China and other South China Sea nations.

National Intelligence Agencies

Intelligence agencies play a key role in gathering intelligence related to maritime threats and sharing it with relevant authorities. The National Maritime Intelligence-Integration Office (NMIO) is responsible for ensuring intelligence and information is shared with partners - this office is run by the US Navy.

International Law Enforcement & Peacekeeping Organisations

Organisations like INTERPOL, the United Nations and the International Maritime Security Construct (IMSC) support global efforts to combat maritime crime by facilitating information exchange and coordinating anti-piracy operations. The IMSC is concerned with maintaining order in the Persian Gulf, Gulf of Oman, Gulf of Aden and Southern Red Sea - with a particular focus on deterring state-sponsored maritime criminality and ensuring safe navigation for oil tanker shipping.

Private Security Firms

Private security companies provide services like vessel protection and risk assessment to safeguard shipping interests. Private Maritime Security Companies (PMSC) have risen to prominence in response to modern piracy threats and provide a range of services including risk assessment, armed & unarmed security at ports and on vessels and crisis response services. These entities come with their own risks where jurisdiction and licencing issues come to the fore - as seen in July 2023 when the UK suspended the licences of floating armouries in the Indian Ocean[12].

Specialist Software Providers

Software systems such as Siren have a critical role to play in staying one step ahead of security threats. By aggregating data from many sources into a single interface, Siren's maritime solution hones risk assessment efforts, breathing confidence into security decisions. Artificial Intelligence (AI) can play an important role in maritime security by analysing real-time data to identify suspicious activities and predict potential threats. This 'big picture' approach takes cognizance of the wide array of datasets involved in the end-to-end supply chains of the maritime trade ecosystem without stifling decision making processes.

13 https://lloydslist.com/LL1146018/UK-licence-suspension-of-Indian-Ocean-floating-armouries-leaves-3000-weapons-in-limbo

14 https://www.dhs.gov/sites/default/files/2023-09/23_0913_ia_23-333-ia_u_homeland-threat-assessment-2024_508C_V6_13Sep23.pdf

CASE STUDIES IN MARITIME SECURITY INTELLIGENCE

The imperative for a strategic, data-driven approach to maritime security is best evidenced by recent data as detailed in the below examples. Maritime intelligence personnel across defence and law enforcement operations must leverage best in class technology to keep abreast of these developments and the potential impact on oceanic security.

Weaponizing Maritime Trade

The growing influence of the Chinese Communist Party in maritime affairs shows no signs of abating. The Department of Homeland Security specifically highlighted the expanding of Beijing's physical and technological logistics capabilities as an area of increased risk in their 2024 Threat Assessment[13].

Counter-Piracy Operations in the Gulf of Aden

The piracy epidemic in the Gulf of Aden and Gulf of Guinea regions - hotbeds of piratical activity - exemplifies the importance of strategic security intelligence for the maritime world. International naval coalitions, such as Combined Task Force 151, successfully utilised intelligence to curb piracy in the region. The UN estimates financial losses relating to Gulf of Guinea piracy alone at $1.9bn annually[14] with the International Chamber of Commerce reporting a surge in maritime piracy in the region in the first half of 2023[15].

IUU Fishing in the South China Sea

The South China Sea witnesses rampant illegal, unreported and unregulated (IUU) fishing activities, threatening marine ecosystems and regional political stability. The US Coast Guard has stated that many Chinese-flagged fishing vessels are members of the People's Armed Forces[16] Military Militia - a component of the Chinese armed forces, illustrating how escalating Great-power competition is manifesting on the ground (or in the seas).

Countering Drug Trafficking

According to the United Nations Office on Drugs & Crime (UNODC), drug trafficking is estimated to be worth in excess of US$650 billion[17] globally. Data from the European Monitoring Centre for Drugs & Drug Addiction (EMCDDA) and EUROPOL states that "most of the cocaine seized in the EU is transported by sea, primarily in maritime shipping containers"[18] which demonstrates the covert logistical capabilities of transnational crime gangs.

Reports from Bloomberg in 2022 suggested shipping giant MSC had been infiltrated by a Balkan drug cartel[19] - the company has strenuously denied these accusations but the tale does serve to illustrate the diverse nature of the maritime security challenge when legitimate, large scale commercial entities can be exposed to such a potentially fatal risk.

15 https://press.un.org/en/2022/sc15113.doc.htm

16 https://iccwbo.org/news-publications/news/mid-year-imb-report-reveals-rise-in-maritime-piracy-and-armed-robbery/

17 https://www.usni.org/magazines/proceedings/2023/february/fishing-trouble-chinese-iuu-fishing-and-risk-escalation

18 https://www.unodc.org/e4j/zh/organized-crime/module-16/key-issues/terrorism-and-drug-trafficking.html

19 https://www.emcdda.europa.eu/publications/eu-drug-markets/cocaine/europe-and-global-cocaine-trade_en

20 https://www.bloomberg.com/news/features/2022-12-16/how-world-s-top-shipping-company-became-hub-for-drug-trafficking

EMERGING TRENDS AND FUTURE PROSPECTS

The future of effectiveness of maritime security can be greatly enhanced through a strategic outlook, collaborative engagement and appropriate deployment of the latest technology.

According to a 2017 Core research paper, updating a risk-based framework for maritime security is dependent on effective monitoring and therefore it is necessary to construct .... "a "live" database, which can record and store a large amount of observable information associated with threats, vulnerabilities, the corresponding criticality analysis and countermeasures. By doing so, the stakeholders can continuously assess their system security performance against the boundaries in the AHARP (As High As Reasonably Practical) scheme. A sound performance measurement loop in the security quality control process will be formed. The information in the database will be processed and regularly updated with more data obtained."

In essence, this is what Siren does through automation. Siren provides the world's largest investigative dataset comprising multiple data sources (with 27 datasets specific to maritime intelligence), enterprise analytics, all backed by domain experience.

Use of Artificial Intelligence (AI)

AI and machine learning algorithms are being deployed to process vast amounts of data quickly, identify anomalies, and predict maritime threats. Through the use of AI, the Chinese government already enhanced the capabilities of its naval maritime integrated surveillance system[20] by deploying BZK-005 UAVs (Unmanned Autonomous Vehicles).

Space-Based Surveillance

Advancements in satellite technology are enhancing global maritime surveillance capabilities, allowing for real-time tracking of vessels and suspicious activities. As mentioned earlier, the European Maritime Safety Agency (EMSA) recently awarded a contract for very high resolution (VHR) optical imagery. Microsatellite innovation makes high quality imagery, daily change detection and persistent monitoring accessible, thereby informing risk mitigation strategies and targeted tactical responses.

Cybersecurity in Maritime Intelligence

As digitalisation in the maritime industry grows, the vulnerability to cyberattacks increases. Cybersecurity measures are becoming integral to protecting maritime intelligence systems.

Cyber criminals can hack electronic systems responsible for controlling vessels, resulting in severe and costly ramifications. In response, Cyber Intelligence Threat (CTI) Analyst roles, domain expertise and specialist tools are in high demand in both commercial and government settings.

21 https://www.airuniversity.af.edu/JIPA/Display/Article/2980879/artificial-intelligence-technology-and-chinas-defense-system/

22 https://www.militaryaerospace.com/sensors/article/14299148/signals-intelligence-sigint-unmanned-maritime-patrol

23 https://www.cna.org/reports/2020/06/DOP-2020-U-025085-Final.pdf

Autonomous cargo ships trials are ongoing and unmanned aerial vehicles (UAVs) for maritime patrol have been ordered by the US Navy[21]. While unmanned systems bring advantages, a CNA study[22] stresses the importance of having "humans in the loop". Context-appropriate decision-making requires discernment but also requires timely access to data - this is where human decision-makers leveraging available datasets in real-time facilitate a more proactive dimension to maritime security that unmanned machines cannot match.

International Collaboration

Efforts to overcome information-sharing barriers and promote international cooperation promise to deliver more effective responses to maritime threats but reactive measures are slow to impact the risk of a recurring threat - a proactive and strategic stance is required.

RECOMMENDATIONS

In response to the complex maritime threats, it is crucial to adopt a proactive security strategy that matches the scale of the challenge. Such an approach aims to minimise economic vulnerabilities; ensure the protection of energy and communication assets, and maintain smooth maritime trade with fewer reactive measures. While tactical responses are important, their effectiveness is hindered by the absence of data-driven foresight. A successful strategy should incorporate the latest proven technology across satellite imaging, remote sensing, AI, machine learning, and data analytics alongside traditional maritime law enforcement methods to provide a comprehensive solution.

In particular, the dominance of China in maritime logistics and the scale of their intelligence gathering footprint demands well-informed mitigation strategies from Western allies. The following five recommendations are key to maritime security into the future:

- **Risk assessment measures** must avail of a suite of up-to-date data sources in order to conduct thorough investigations of potentially bad actors and illicit entities across the entire maritime supply chain ecosystem including ports & terminal operators, vessels & cargo, freight forwarders, land-based logistics operators and relevant regulations & governance.

- Using appropriate visualisation tools to **detect suspicious activity** (loitering, blocking sea lanes, breakdown trends) to thwart TCOs and politically motivated trade interference.

- Greater reliance on **network graphs** to map links between people (e.g. TCO members) and ship and port ownership & associated business transactions.

- **Routine monitoring** of activity around critical energy and communications infrastructureas a Great-power competition counter-intelligence measure.

- **Link data** to criminal activity on darknet, cellphones, crypto currency trading and also to identify foreign intelligence activity for critical investigative insights.

Without such a comprehensive data-driven approach, maritime criminal intelligence investigators can get lost in a sea of disconnected data. This allows transnational crime to continue to successfully use the seas for distributing contraband around the world and there will be a persistent risk of maritime trade being weaponized for geopolitical gain.

CONCLUSION

Maritime security intelligence is an indispensable component of safeguarding the global maritime domain. Its significance lies in mitigating geopolitical manipulation, ensuring the safety of vessels, countering piracy, terrorism, and illegal activities, and protecting vital marine resources. Despite the challenges it faces, advances in technology and international cooperation offer hope for a more secure maritime future. As threats evolve, so too must our methods of gathering and utilising intelligence to preserve the freedom and security of the world's oceans.

The opportunity to rapidly and succinctly synergise the disconnected data produced by vast human and technological resources from different maritime domains is a boon to the security of the world's oceans. For security personnel across multi-agency security groups, Navy departments, Coast Guard and maritime criminal intelligence & security specialists this represents a critical real-time asset in the face of ubiquitous maritime threats.

Through an all-in-one platform, Siren provides a strategic solution to maritime intelligence challenges by complementing established physical solutions, effectively providing overarching data-driven acumen to better inform strategic decision-making and improve tactical security measures. The single user-experience is applicable across multiple contexts and provides access to a wide range of pre-integrated datasets.

WEB
WWW.SIREN.IO

EMAIL
INFO@SIREN.IO