The Nautical Institute

Maritime Security

A practical guide for mariners

by

Steven Jones MA MSc BSc (Hons) AFNI FRSA

Maritime Security
A practical guide for mariners

by

Steven Jones MA MSc BSc (Hons) AFNI FRSA

Published by The Nautical Institute
200B Lambeth Road, London SE1 7JY, UK
Tel: +44 (0)20 7928 1351 Fax: +44 (0)20 7401 2817 Web: www.nautinst.org

Although great care has been taken with the writing of the book and production of the volume, neither The Nautical Institute nor the author can accept any responsibility for errors and omissions or their consequences. The opinions expressed are those of the author alone and should not be taken as necessarily being the policies or views of any organisation with which he has any connection.

The book has been prepared to address the subject of maritime security. This should not, however, be taken to mean that this document deals comprehensively with all of the concerns that will need to be addressed or even, when a particular need is addressed, that this document sets out the only definitive view for all situations.

Cover image: Alamy
Design and layout by Phil McAllister Design
Printed and bound in the UK by Short Run Press

ISBN 978 1 915488 01 5

Contents

Dedication

To my family and friends, without whom every success does seem a failure.

Acknowledgements

Thanks to:

Bridget Hogan
Captain John Lloyd
Captain Mike Powell
Captain Tom Brown
Captain Terry Ogg
Captain Stu Nicholls
Dariusz Goździk
Dr Phil Anderson
Emma Ward
Mike Williams
Steven Gosling

Foreword

by **Heike Deggim**
Director, Maritime Safety Division, IMO

Maritime transport is the lifeblood of global economic growth and prosperity. The overwhelming majority of goods, around 80%, are transported by ship. New technologies, digitalisation and automation mean that the maritime industry is undergoing seismic change. There is no better example of this than the design and construction of maritime autonomous surface ships, with both the international shipping and port sectors increasingly reliant on new and emerging technology.

Along with growth and opportunities to enhance the speed and efficiency of commercial operations come significant challenges. The inter-connected modern maritime domain faces new and emerging trans-national security threats on an unprecedented scale. Piracy and armed robbery remain of concern, as do terrorism; serious and organised crime; illegal, unreported and unregulated (IUU) fishing; and security vulnerabilities related to stowaways and irregular migration, to name but a few. We are also seeing increasing and worrying trends in collateral damage resulting from state and civil conflicts. We are witnessing the growing use of cyber attacks and unmanned aerial vehicles as well as the increasing sophistication of water-borne improvised explosive devices and other forms of attack unique to the maritime domain. It is at these moments when a good knowledge of maritime security issues and responses, as covered in this guide, becomes invaluable.

In *Maritime Security – A Practical Guide for Mariners*, Steven Jones has woven together the many and diverse strands that make up the context, theory and best practices of maritime security. He offers practical, experience-led advice in clear language, designed to equip seafarers with essential and potentially life-saving knowledge. The information he so insightfully provides is equally relevant for littoral states and ship and port operators who require a thorough knowledge of the security measures and legislation intended to protect ships, crews, passengers, cargoes and the facilities and supply chain that serve them.

The book leads us through the evolution of maritime security, the development of the ISPS Code and modern shipboard security procedures, explaining why they matter and how they are applied in dealing with the increasingly diverse threats to the maritime sector. Each chapter lays out relevant security issues, legislation and solutions in language that is accessible to seafarers across the spectrum of experience and training. Security is everybody's business. I commend this book to seafarers, maritime security professionals, government officials and academics, and also to the casual reader who wishes to understand, why and how maritime security can, and does, make such a vital contribution to safeguarding this critical sector.

Preface

The first guide on maritime security for The Nautical Institute was published more than 20 years ago. Since then, much has changed. The technological landscape has evolved, new challenges have emerged and threats to seafarers, ships, ports and cargoes are constantly appearing and shifting.

Cybersecurity is arguably the single biggest change. When the ISPS Code was introduced, shipping was about a decade behind society and businesses ashore in its adoption of IT. However, it has since become hugely data- and connectivity-driven. This presents both threats and opportunities. Enhanced communication links to systems ashore have brought new hazards and risks, which all have to be managed.

We have also had to cope with a rising tide of piracy. From Somalia to Nigeria, crews have been subjected to waves of violence from pirate gangs who see human capital and ransoms as their reward. These despicable acts have brought suffering to many seafarers. Although that particular threat has, at the time of writing, abated somewhat, only vigilance can really protect seafarers. Piracy and armed attacks are still taking place, so it is clear that there is more to do.

Terrorism at sea has been declining, but it remains a risk. It only takes a change of mindset, a new, energised terrorist organisation to emerge or the old guard to return to their ways, and the maritime industry can fall victim once more.

The issue of stowaways and rescue of migrants at sea also remains troubling. Desperate people who feel compelled to make dangerous choices frequently cross paths with marine traffic. Stowaways find ships to be attractive targets; when they are found aboard, they present massive logistical and cost implications for ship operators.

In some waters, ships have to run a gauntlet of perilously overloaded and potentially dangerous small boats. These are packed to the waterline with people looking to escape war, terror and poverty, all seeking to start new lives in other countries. Often, they find only danger and death. Ships are legally and morally bound to act, thereby finding themselves in complex rescue operations. It is clear that more support is needed to solve these problems to keep our seas safe.

Crime is an ever-present problem at sea, just as it is ashore. From theft to smuggling, fraud to violence, seafarers can unwittingly find themselves caught up in criminal activities. Sadly, when seafarers raise problems or report crimes, they often find themselves made the scapegoat, suffering as a result. This is a harsh reality that needs to change.

These are some of the topics addressed in this new practical guide. It pulls together the themes of three best-selling maritime security books, now fully updated with new content added. It aims to provide the rules, checks, balances and insights that make maritime security work and will, I hope, spark a wider, deeper interest in the subject.

Steven Jones

List of abbreviations

AID	automated intruder detection
AIS	Automatic Identification System
AMS	(US) area maritime safety (committee)
AMS	(US) automated manifest system
APPS	(US) Act to Prevent Pollution from Ships
APT	advanced persistent threat
BIMCO	Baltic and International Maritime Council
BMP	Best Management Practices
CBP	(US) Customs and Border Patrol
CCTV	closed-circuit television
CSI	(US) Container Security Initiative
CSO	company security officer
CSR	continuous synopsis record
C-TPAT	(US) Customs-Trade Partnership Against Terrorism
CVSSA	(US) Cruise Vessel Safety and Security Act
DDoS	distributed denial of service
DHS	(US) Department of Homeland Security
DOE	(US) Department of Energy
DOJ	(US) Department of Justice
DoS	declaration of security
DP	dynamic positioning
DPA	designated person ashore
ECDIS	electronic chart display and information system
FAL	(IMO) Facilitation Committee
FCPA	(US) Foreign Corrupt Practices Act
GISIS	(IMO) Global Integrated Shipping Information System
GPS	Global Positioning System
HRA	(piracy) High Risk Area
IACS	International Association of Classification Societies
ICJ	International Court of Justice
ICS	International Chamber of Shipping
ICT	information and communication technology
IED	improvised explosive device
ILO	International Labour Organization
IMB	International Maritime Bureau
IMCA	International Marine Contractors' Association
IMO	International Maritime Organization
IOM	International Organisation for Migration
IoT	internet of things
ISM	(IMO) International Safety Management (Code)
ISPS	(IMO) International Ship and Port Facility Security (Code)
ISSC	international ship security certificate
ISWAN	International Seafarers Welfare and Assistance Network
ITF	International Transport Workers Federation
ITLOS	International Tribunal for the Law of the Sea
LLAR	low-level armed robbery
LNG	liquefied natural gas
LRIT	long-range identification and tracking

MACN	Maritime Anti-Corruption Network
MARPOL	(IMO) International Convention for the Prevention of Pollution from Ships
MARS	(NI) Mariners' Alerting and Reporting Scheme
MCB	maritime security capacity building
MCH	major criminal hijack
MDA	maritime domain awareness
MG	maritime governance
MIP	maritime infrastructure protection
MLAR	medium-level armed robbery
MLC	(ILO) Maritime Labour Convention
MRCC	maritime rescue co-ordination centre
MSO	maritime security operations
MTSA	(US) Maritime Transportation and Safety Act 2002
NI	The Nautical Institute
NNSA	(US DOE) National Nuclear Security Administration
OFAC	(US) Office of Foreign Assets Control
OFSI	(UK) Office of Financial Sanctions Implementation
OPRC	International Convention on Oil Pollution Preparedness, Response and Cooperation
OSS	on-scene security survey
OWS	oil-water separator
PAA	piracy-affected area
PCASP	privately contracted armed security personnel
PFSO	port facility security officer
PFSP	port facility security plan
PPE	personal protective equipment
PSC	port state control
PSI	(US) Proliferation Security Initiative
RAM	restricted in ability to manoeuvre
ReCAAP	Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia
RPG	rocket-propelled grenade
RSO	recognised security organisation
SAR	(IMO) International Convention on Maritime Search and Rescue
SFI	(US) Secure Freight Initiative
SID	seafarer's identity document
SMS	safety management system
SOLAS	(IMO) International Convention for the Safety of Life at Sea
SSA	ship security assessment
SSAS	Ship Security Alert System
SSO	ship security officer
SSP	ship security plan
STCW	(IMO) International Convention on Standards of Training, Certification and Watchkeeping for Seafarers
SUA	(IMO) Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation
TAPA	Transported Asset Protection Association
UN	United Nations
UNCLOS	(UN) Convention on the Law of the Sea
UNHCR	UN High Commissioner for Refugees
UNTOC	(UN) Convention Against Transnational Organised Crime
VTS	vessel traffic services
WCO	World Customs Organization
WMD	weapon of mass destruction
WTO	World Trade Organization

Chapter 1

The pillars of maritime security

This practical guide to maritime security aims to inform and support seafarers in aspects related to the safety and security of people, ships, ports, cargoes and the marine environment. It covers the following topics.

Threats and risks: The threats and risks associated with maritime security, such as piracy, terrorism, armed robbery and smuggling. This section aims to help seafarers to take appropriate measures to protect their vessels, crew, cargo and the marine environment.

Global trade and transportation: The impact of disruptions to maritime security on global trade and transportation, which will help seafarers understand the link between the global economy and the importance of safeguarding the smooth flow of goods and services.

Stakeholder collaboration: The importance of collaboration, intelligence-sharing, law enforcement measures and co-operation among stakeholders, which will help to prevent and mitigate security threats.

Cybersecurity: Insights into maritime cybersecurity, including best practices that will help with the prevention, detection and response to cyber threats in the maritime domain.

Compliance with international maritime security codes: An overview of security codes, such as the ISPS Code, that set out mandatory security requirements for ships and port facilities. Implications of non-compliance include security risks, legal and financial penalties, trade disruption, loss of customer confidence and potential environmental damage.

Implementation of security measures: Guidance on onboard security measures, such as controlling access, monitoring surroundings, reporting suspicious activity, enhancing shipboard security and protecting against security threats.

Inspections, audits, drills and exercises: The guidance stresses the importance of actively participating in inspections, audits, drills and exercises in accordance with maritime security measures, such as the ISPS Code. This includes being prepared to demonstrate compliance with security measures to ensure the safety and security of their vessels and operations.

Maritime security

Maritime security describes malicious threats posed to seafarers, ships, ports and cargoes and also the wider menace posed to countries and trade. It covers the actions taken to mitigate and manage risks and threats, as well as maritime issues that are often related to national security, the marine environment, economic development and human security.

Among the most common and significant maritime security threats are piracy, terrorism and armed robbery, and issues around stowaways and criminality also have to be addressed. To keep the maritime domain safe, these all require continuous effort and co-operation, while remaining legally compliant.

Maritime security involves co-ordination between different stakeholders, including national governments, law enforcement agencies, port authorities, shipping companies and organisations. These all play a key role in the smooth functioning of global trade and transportation, in addition to protecting human lives and the environment.

The concept has evolved since the introduction of the International Ship and Port Facility Security Code on 1 July 2004. The ISPS Code represented a significant change in the approach of the maritime community to security and its evolution within the industry. In the decades since then, we have seen many changes to the way that maritime security is understood and managed, and in shipping's ability to balance the complex demands placed on it by people, ships, ports and cargoes.

Starting from an assessment of the many threats facing shipping and ports, and the problems associated with particular vessel types and cargoes, this guide covers the ISPS Code and the implications of its rules, providing valuable insights into maritime security and contingency planning. It also explores the wider maritime security issues of piracy, cybersecurity and criminality at sea, along with stowaways and migrant rescue at sea.

Decades of maritime security

Over the past 20 years, the field of maritime security has undergone significant change. The shipping industry has learned several important lessons:

Increased awareness of security risks: Since the terrorist attacks on New York of 11 September 2001, there has been a heightened awareness of security threats that ships and ports may face, including piracy, terrorism and smuggling.

Importance of security planning and training: Effective security planning and training are critical for preventing security incidents and responding to them if they occur.

Adoption of technology: The shipping industry has increasingly adopted technology to improve security, such as tracking systems, surveillance cameras and access control measures. Electronic systems make it easier to monitor ships, cargo and ports, and to identify potential security risks.

Collaboration and communication: Sharing information and intelligence between governments, organisations and stakeholders is essential for identifying potential threats and responding to incidents quickly.

Development of international regulations: The International Maritime Organization (IMO) has developed regulations and conventions to promote maritime security. These regulations have helped to standardise security practices across the shipping industry.

Piracy can have a devastating impact on seafarers, shipping and global trade, and it remains a threat, despite all the security rules and plans that are in place. While there has been much progress in stemming the problems, when piracy does take root somewhere – as it has done in past years in Somalia and West Africa – seafarers are reliant not just on their own knowledge of what to do, but also on the support and assistance of others.

Innocent seafarers who become caught up in security issues can sometimes find themselves facing serious consequences. After reporting smuggling, for example, seafarers have sometimes been wrongly implicated in the crime. In certain countries, seafarers can be held without charge to act as witnesses in alleged pollution cases. Rules do exist to safeguard the fair treatment of seafarers, but they are not universally applied.

Many seafarers work tirelessly to enhance security. In this guide we explore the elements of good practice on board and in ports. To be effective, maritime security requires a combined effort by global governments, military and law enforcement bodies to deal robustly with those who threaten the security of global shipping.

Maritime security pillars and overview

Five pillars combine to provide a comprehensive overview of maritime security-related concerns, issues, risks, threats and countermeasures:

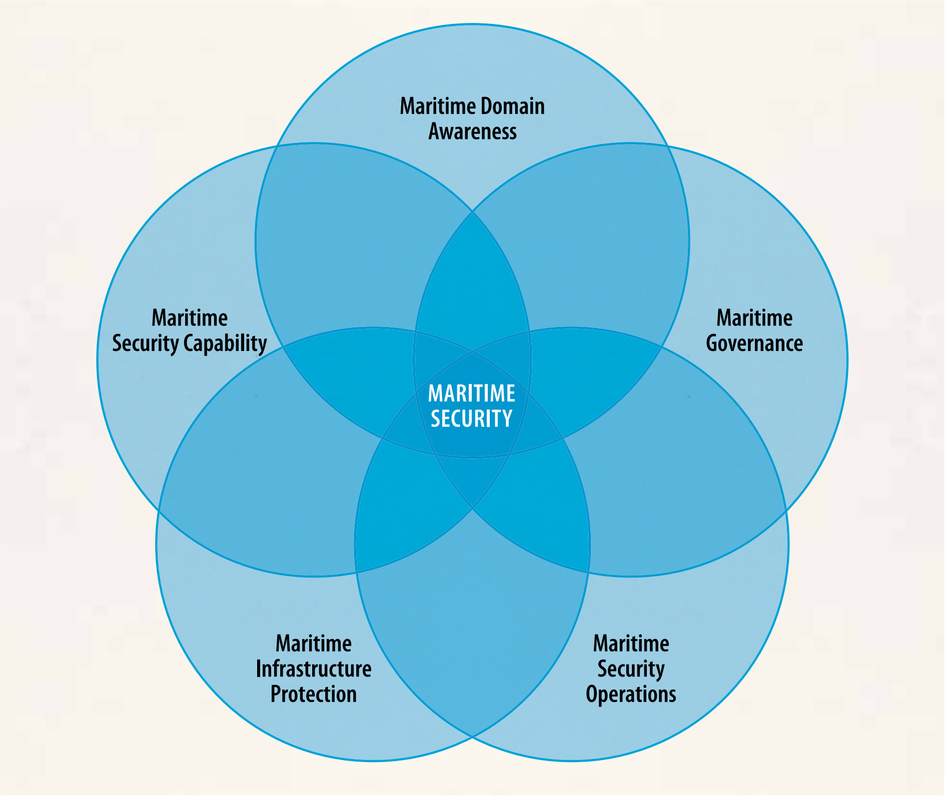
Maritime domain awareness (MDA): monitoring and understanding activities in the maritime environment, such as vessel traffic, potential threats and asset/resource identification.

Maritime governance (MG): legal and regulatory frameworks, policies and international co-operation among maritime stakeholders.

Maritime security operations (MSO): practical responses and mitigation measures taken to prevent and respond to maritime threats, such as piracy, terrorism and smuggling. These are the actions, management processes and physical responses on a vessel.

Maritime infrastructure protection (MIP): safeguarding the physical assets and infrastructure of the maritime industry, such as ports and terminals, cables and pipelines.

Maritime security capacity building (MCB): the human and institutional resources needed to ensure effective maritime security, including training and education programmes, technology transfer and partnerships between governments, industry and civil society.


Maritime Domain Awareness
Maritime Security Capability
Maritime Governance
MARITIME SECURITY
Maritime Infrastructure Protection
Maritime Security Operations

Maritime domain awareness (MDA)

The main tools and services for maritime domain awareness include:

- Satellite-based monitoring systems
- Radar and other sensor technologies
- Vessel traffic services (VTS)
- Maritime patrol aircraft and vessels
- Geospatial data and analysis tools
- International and regional maritime information-sharing networks.

MDA makes use of advanced technologies and expertise to improve maritime security and safety:

- **Maritime surveillance:** Advanced maritime surveillance solutions, including vessel tracking, satellite imaging and drone technology, are used to monitor and track vessels and detect potential security threats.
- **Data analytics:** Machine learning is employed to analyse maritime data, identify patterns and support decision-making in areas such as maritime risk assessment and environmental monitoring.

- **Port security:** Access control, cargo screening and threat detection technologies can help ensure the safety and security of ports and their facilities.
- **Maritime communication:** Advanced communication and information-sharing systems help to improve co-ordination and collaboration among maritime stakeholders, including ports, shipping companies and law enforcement agencies.
- **Environmental monitoring:** Advanced technologies, such as remote sensing and satellite data, are used for monitoring and tracking environmental factors such as oil spills, marine debris and water quality.

Risk and threat assessment is another important part of MDA. Ways that maritime security risks and threats can be identified include:

- **Intelligence gathering:** Collecting and analysing information about potential threats from sources such as government agencies and law enforcement and intelligence services. This information can be used to identify patterns and trends that may indicate the presence of security threats.
- **Surveillance and monitoring:** Using technology, such as radar, cameras and satellite imagery, to monitor the maritime environment and detect any suspicious activity.
- **Risk assessments:** Assessing security risks associated with maritime operations, such as cargo-handling or port operations. By identifying potential vulnerabilities and impacts, security measures can be put in place to reduce, mitigate or transfer the risk of security incidents.
- **Physical inspections:** Physically inspecting vessels, cargo and port facilities to identify any suspicious activity or potential security threats.
- **Security alerts:** Sharing information about potential security threats with other stakeholders, such as law enforcement agencies, port authorities and shipping companies.

One important conceptual aspect and focus of MDA in its widest sense is the 'blue economy'. This refers to the sustainable use and management of the world's oceans and coastal resources for economic growth, social wellbeing and environmental sustainability. The term highlights the importance of the oceans and seas, which cover more than 70% of the Earth's surface, as a source of economic opportunity, innovation and wealth. It encompasses a wide range of sectors and activities, including fisheries, aquaculture, maritime transport, tourism, renewable energy and biotechnology. 'Blue economy' also describes the protection and restoration of marine ecosystems, which are essential for maintaining the health and productivity of the ocean and its resources.

Maritime security is essential for the success of the blue economy by:

- **Protecting shipping and ports:** Maritime transport is a critical component of the blue economy, with ships carrying more than 80% of the world's trade. Ensuring the security of ships and ports is crucial for the safe and efficient movement of goods.
- **Combatting illegal activities:** The blue economy is vulnerable to illegal activities, including piracy, smuggling and illegal fishing, which can damage both the environment and local and national economies; they can also threaten the safety of people and goods. By creating a secure and stable environment, maritime security measures can help the blue economy thrive.

- **Protecting the marine environment:** Maritime security measures, such as oil spill response and prevention, can help protect the marine environment from pollution and other negative impacts.
- **Attracting investment:** A secure and stable maritime environment is attractive to investors and can encourage investment in the blue economy. This, in turn, can lead to job creation, economic growth and social development.

Maritime governance

Maritime governance considers the seas as one of the 'global commons' – areas and resources that are essential for human wellbeing and economic development.

There are four traditional types of global commons:

1. **Atmosphere:** The atmosphere comprises the layer of gases surrounding the Earth that is essential to sustain life. It is considered a global common because it is not subject to national jurisdiction and any changes to it, such as greenhouse gas emissions, affect all countries and individuals.
2. **Oceans:** The world's oceans cover more than 70% of the Earth's surface. They are important for transportation, trade, fisheries and other economic activities, as well as supporting biodiversity and regulating the global climate.
3. **Antarctica:** Antarctica is not subject to national jurisdiction, as it is governed by the Antarctic Treaty System. It is important for scientific research and serves as a model for co-operation and governance.
4. **Outer space:** Outer space is not subject to national jurisdiction and is essential for space exploration and research, as well as supporting telecommunications and satellite systems.

The four global commons require co-operation and governance to ensure their sustainable use and preservation. International shipping affects or touches on each one, so maritime security must be taken into account when considering them.

The concept of global commons is significant because vessels often operate in seas and oceans that are beyond the jurisdiction of individual countries or authorities. If such seas are seen as part of the wider global commons, a focus on maritime governance and diplomacy is key and must be managed through various legal frameworks, treaties and organisations. Pivotal to this approach is the United Nations Convention on the Law of the Sea 1982 (UNCLOS), which sets out the legal framework for maritime governance, including rules on maritime boundaries, navigation and marine environmental protection.

Diplomacy has a vital role in managing maritime disputes and promoting co-operation among countries. When things go wrong, dispute resolution can solve issues, such as conflicts over maritime boundaries, resources and other issues that have major economic and security implications. Not all states are signatories of UNCLOS, but as the convention is now considered to reflect customary law, it can be considered binding for non-signatories.

Specific examples of dispute resolution mechanisms in the maritime context include:

- **International Court of Justice (ICJ):** The principal judicial organ of the United Nations with jurisdiction over disputes between states, including those related to maritime boundaries.
- **International Tribunal for the Law of the Sea (ITLOS):** An independent judicial body established under UNCLOS to settle disputes related to the interpretation and application of the convention.
- **Arbitration:** A means by which countries can resolve maritime disputes, using a neutral third party to arrive at a binding decision.
- **Negotiated settlements:** Many maritime disputes are resolved through direct negotiations between the parties involved, often with the assistance of a mediator or facilitator.
- **Confidence-building measures:** In some cases, countries may use confidence-building measures, such as joint patrols, shared fisheries management or scientific co-operation, to build trust and prevent disputes from escalating.

Maritime security operations

Maritime operations can include patrols, inspections, intelligence gathering, law enforcement and interdiction efforts carried out by naval, coast guard or law enforcement agencies. Their ultimate goal is to ensure the safety and security of maritime transportation, commerce and people at sea. Responses are constantly evolving in response to new threats and changing security environments.

Maritime infrastructure protection

Maritime infrastructure protection includes the following elements:

- **Physical security measures:** These include physical solutions such as perimeter fencing, access controls and security cameras to deter or detect intruders.
- **Security personnel:** Ports may employ security personnel, such as guards or law enforcement officers, to monitor access to the facility and respond to security incidents. More serious incidents may involve responses from state agencies such as police forces, coast guards and potentially even military.
- **Surveillance and monitoring:** Surveillance technologies, such as CCTV cameras, lighting or drones, can monitor activity in and around the facility.
- **Regulatory frameworks:** Many countries have established regulatory frameworks for the protection of maritime infrastructure.
- **Collaborating with other stakeholders:** Collaboration between ports, shipping companies and other stakeholders can also help protect maritime infrastructure. This can involve sharing information, conducting joint risk assessments and co-ordinating responses to security incidents.

Maritime security capacity building (MCB)

One of the key elements of the fight against Somali-based piracy was capacity building. While the actions of seafarers and shipping companies played a vital role, along with the patrols and responses of many countries' navies, successful MCB approaches have thus far managed to contain the threat from this part of the world.

Some of the key elements needed for effective maritime security capacity building include:

- **Human capacity building:** Developing skills and knowledge of individuals working in the maritime security sector, including law enforcement officials, coast guards and naval personnel, via training and education programmes and opportunities for professional development and exchange.
- **Institutional capacity building:** Strengthening the institutions responsible for maritime security, including coast guards, port authorities and maritime law enforcement agencies. This also encompasses improvements in governance, management and resource allocation.
- **Technology transfer:** Transferring technology and equipment to support maritime security operations, such as vessels, communications equipment and surveillance systems. This can help enhance the effectiveness of maritime security operations, while promoting economic development.
- **International partnerships:** These are essential for building maritime security capabilities, as many threats are transnational, such as piracy. Partnerships can include information-sharing, joint training exercises and co-ordinated law enforcement operations.
- **Policy and regulatory frameworks:** The development of policy and regulatory frameworks promotes effective governance and encourages co-operation among relevant stakeholders.