Maritime Security, Port Protection, and International Trade

Posted on September 22, 2018

Michael McNicholas's *Maritime Security: An Introduction* surveys the commercial systems, infrastructure, legal frameworks, and threats that shape modern maritime transport. The original article selected twenty-five topics from the first nine chapters and briefly recorded what was learned from each. That numbered structure is preserved here, but each topic is expanded to explain why it matters for port protection and international trade. Maritime security is not limited to guarding ships against pirates. It includes the protection of people, cargo, vessels, ports, waterways, information systems, supply chains, and national economies from terrorism, organized crime, smuggling, cyberattack, accident, and disruption. Because most international merchandise trade by volume travels by sea, a local port incident can affect manufacturers, consumers, energy supplies, and food security far beyond the coastline (McNicholas, 2016; International Maritime Organization, 2021).

1. Functions of Major Seaports

Major seaports connect maritime transport with roads, railways, pipelines, warehouses, customs systems, and inland distribution centers. They load and unload containers, vehicles, fuel, grain, minerals, machinery, clothing, food, and other goods used in everyday life. Ports also provide pilotage, tug assistance, repair, bunkering, waste reception, crew services, inspection, and emergency response. Their security value arises from concentration: enormous quantities of cargo, passengers, information, and infrastructure pass through limited gateways. A disruption can delay production and create cascading losses, so security must support continuity rather than merely prevent unauthorized entry (McNicholas, 2016).

2. Forms of Seaports

Ports differ according to geography, cargo, ownership, and function. Container ports handle standardized boxes transferred between ships, trucks, and trains. Bulk ports handle unpackaged commodities such as coal, ore, grain, or petroleum. Roll-on/roll-off terminals serve vehicles and wheeled cargo. Cruise terminals process passengers, baggage, supplies, and hospitality services. Fishing, naval, ferry, and specialized industrial ports face different risks. Security plans should reflect the facility rather than apply one identical model. An oil terminal emphasizes fire, sabotage, and hazardous materials, while a cruise terminal emphasizes passenger screening, crowd management, and identity control (McNicholas, 2016; International Maritime Organization, 2021).

3. Changes in the Panama and Suez Canals

The Panama and Suez canals shorten major trade routes and therefore function as strategic chokepoints. Expansion of the Panama Canal allowed larger vessels and influenced port dredging, crane investment, and shipping patterns. The Suez Canal has also been expanded and remains essential to trade between Europe and Asia. Blockage, conflict, accident, or attack in either canal can redirect ships around longer routes, increasing time, fuel cost, insurance, and congestion. Security planning must consider canal traffic management, salvage, navigation, cyber systems, and geopolitical risk. The 2021 grounding of the *Ever Given* in Suez illustrated that disruption need not be an intentional attack to create global effects (McNicholas, 2016).

4. Evolution of Modern Ships

Ships have evolved in size, propulsion, specialization, automation, and cargo handling. Containerization reduced loading time and theft by standardizing cargo units. Tankers, liquefied-gas carriers, car carriers, cruise ships, and offshore-support vessels are designed around specific missions. Larger ships provide economies of scale but create concentrated risk: an accident involving a megaship may overwhelm local salvage and port capacity. Increased automation improves efficiency while expanding dependence on software, sensors, satellite navigation, and shore-based communication. Security must evolve with design (McNicholas, 2016).

5. Types of Modern Ships

Container ships carry standardized intermodal units; bulk carriers transport dry commodities; tankers carry petroleum or chemicals; LNG carriers transport liquefied natural gas; roll-on/roll-off vessels carry vehicles; general-cargo ships handle varied loads; and passenger vessels transport travelers. Each type creates distinct vulnerabilities. Tankers present pollution and fire risks, container ships conceal millions of possible cargo combinations, and passenger ships involve large populations in confined environments. Ship-security assessments should consider cargo, route, flag, crew, port calls, and the consequences of loss (McNicholas, 2016).

6. Development of Greener Ships

Environmental pressure and regulation are encouraging more efficient hulls, engines, fuels, routing, and port operations. Greener ships may use LNG, methanol, biofuels, batteries, wind assistance, shore power, or future low-carbon fuels, although each option has trade-offs. Environmental technology also creates security needs. New fuels may be toxic, flammable, or difficult to handle; charging and digital energy-management systems may be vulnerable; and unfamiliar emergency procedures require training. Decarbonization and security should be designed together rather than treated as separate

goals (International Maritime Organization, 2021).

7. Ocean Cargo Transportation

Ocean transport begins before cargo reaches the port. A seller and buyer agree on goods, price, responsibilities, insurance, and delivery terms. Freight is booked, cargo is packed and documented, inland carriers deliver it to a terminal, customs information is submitted, and the shipment is loaded according to vessel planning. At the destination, it passes through discharge, inspection, clearance, and inland delivery. Security gaps can occur at any stage, including fraudulent booking, tampered containers, false seals, insider access, or manipulation of electronic records. Supply-chain security therefore depends on trusted partners and traceability (McNicholas, 2016; United States Coast Guard, 2024).

8. Import and Export Documentation

Common documents include the commercial invoice, packing list, bill of lading, certificate of origin, customs declaration, insurance certificate, permits, and dangerous-goods documentation. The bill of lading can serve as a receipt, evidence of the carriage contract, and in some cases a document of title. Accurate documentation supports customs, payment, safety, and cargo release. False descriptions can conceal contraband, evade tax, or create hazardous stowage. Digital documents improve speed but require authentication, access control, and protection against alteration (McNicholas, 2016).

9. Maritime Transportation Terms

Maritime trade uses specialized terms concerning chartering, freight, laytime, demurrage, manifests, consignees, carriers, ports of loading, and delivery responsibility. Incoterms allocate costs and risks between buyer and seller but do not replace the contract of carriage or determine ownership automatically. Security professionals need this vocabulary because responsibility changes across the transaction. Confusion about who packed, sealed, carried, or received cargo can delay investigation and create opportunities for fraud (McNicholas, 2016).

10. The ISPS Code

The International Ship and Port Facility Security Code was adopted through the International Maritime Organization after the attacks of September 11, 2001. It establishes a risk-management framework for ships and port facilities engaged in international voyages. Contracting governments set security levels, while companies and facilities conduct assessments, develop plans, appoint security officers, control access, monitor restricted areas, and maintain communication. The code does not eliminate

threat; it creates a common minimum structure that can be adapted to local risk (International Maritime Organization, 2021).

11. The Maritime Transportation Security Act

The United States enacted the Maritime Transportation Security Act of 2002 to strengthen security at ports and waterways. It requires security assessments and plans for regulated vessels and facilities, supports identification and access controls, and gives the Coast Guard major responsibilities. The act interacts with customs, immigration, intelligence, and state and local agencies. Compliance should not be treated as paperwork. Plans require exercises, updates, and integration with actual emergency capabilities (United States Coast Guard, 2024).

12. Maritime Terrorist Attacks

Attacks on the *USS Cole*, the tanker *Limburg*, passenger vessels, ports, and coastal infrastructure demonstrate varied methods and targets. Terrorists may seek casualties, economic disruption, symbolic effect, environmental damage, or publicity. Ships can be targets, delivery platforms, or sources of dangerous cargo. Risk depends on intent, capability, protective measures, and consequence. Security should avoid assuming that the last method used will define the next attack (McNicholas, 2016; International Maritime Organization, 2021).

13. Security Measures

Measures include perimeter control, identity verification, patrols, lighting, surveillance, screening, restricted areas, container seals, intelligence sharing, cybersecurity, drills, and emergency plans. Layered security is stronger than dependence on one checkpoint. Personnel should know how to report anomalies without profiling people solely by race, nationality, or religion. Personal awareness matters, but responsibility rests with organizations to create systems, staffing, and equipment that support safe action (International Maritime Organization, 2021; United States Coast Guard, 2024).

14. History of Piracy

Piracy has accompanied maritime trade for centuries, but its form changes with commerce, governance, and technology. Modern piracy may involve opportunistic theft at anchor, hijacking for cargo, kidnapping for ransom, or prolonged control of a vessel. Weak coastal governance, economic exclusion, corruption, and valuable shipping routes can create enabling conditions. International law distinguishes piracy on the high seas from armed robbery within a state’s territorial waters, affecting jurisdiction and response (McNicholas, 2016; United Nations Office on Drugs and Crime, 2023).

15. Methods of Piracy

Pirates may use small fast boats, ladders, firearms, insider information, false distress signals, or mother ships. Attacks may occur while vessels are moving, anchored, or in port. Protective measures can include routing, speed, watchkeeping, physical barriers, citadels, alarms, lighting, and naval coordination. The relationship among piracy, terrorism, and organized crime should not be assumed. They may share methods or networks, but motives and legal categories differ. Accurate classification supports an appropriate response (United Nations Office on Drugs and Crime, 2023; McNicholas, 2016).

16. Origins and Transportation of Illicit Drugs

Cocaine, heroin, cannabis, synthetic drugs, and precursor chemicals move through complex global routes using containers, fishing vessels, yachts, commercial ships, and concealment within legitimate cargo. The original list focused on three drugs, but synthetic substances and chemicals have become increasingly important. Maritime transport is attractive because trade volume is enormous and inspection of every container is impossible. Law enforcement uses intelligence and risk targeting rather than universal physical search (United Nations Office on Drugs and Crime, 2023).

17. Drug-Trafficking Routes

Routes change in response to enforcement, conflict, market demand, and criminal opportunity. A route map can become outdated quickly. Traffickers may use transshipment ports, altered documents, semi-submersible craft, or “rip-on/rip-off” methods in which drugs are inserted into a legitimate container without the shipper’s knowledge. Effective response requires international cooperation, financial investigation, port integrity, and protection against corruption (United Nations Office on Drugs and Crime, 2023).

18. Front Companies

Front companies can provide apparently legitimate bookings, invoices, warehouses, vessels, or trade transactions that conceal criminal activity. Trade-based money laundering may use mispriced or fictitious shipments. Beneficial-ownership transparency, customer due diligence, financial intelligence, and cross-border information sharing help identify misuse. Authorities should distinguish suspicious patterns from legitimate business and protect due process (United Nations Office on Drugs and Crime, 2023).

19. Maritime Smuggling Tactics

Smuggling can involve concealment inside cargo, false compartments, altered seals, corrupted workers, unreported transfers at sea, fraudulent manifests, and misuse of small craft. Human smuggling and trafficking present additional humanitarian and legal issues. Technology such as non-intrusive inspection, tracking, data analysis, and electronic seals can help, but criminals adapt. Security culture and worker integrity remain crucial (United Nations Office on Drugs and Crime, 2023).

20. Attacks Near North Africa

Historical analysis of attacks near North Africa and adjacent waters can reveal patterns involving conflict, piracy, smuggling, and strategic chokepoints. The region includes approaches to the Mediterranean, Suez, Red Sea, and Atlantic routes. Past incidents help planners identify vulnerable vessel types and political conditions, but historical analogy must be used cautiously. Contemporary threats may involve drones, missiles, cyber systems, or armed groups with capabilities different from earlier pirates (McNicholas, 2016).

21. Awareness of Terrorist Tactics

Security training may examine surveillance, small-boat attack, vehicle-borne devices, insider assistance, document fraud, cyber intrusion, and attacks on energy or navigation. Awareness should focus on observable behavior and system vulnerabilities rather than stereotypes. Excessive publication of operational detail can itself create risk, so training must balance specificity with protection of sensitive information. Exercises help personnel translate awareness into coordinated response (International Maritime Organization, 2021; United States Coast Guard, 2024).

22. Terrorist and Criminal Networks

Terrorist and criminal groups may cooperate transactionally in smuggling, document acquisition, weapons, finance, or transport, but their relationships vary. Criminal organizations usually seek profit, while terrorist organizations pursue political or ideological goals, although both may use coercion and secrecy. Assuming a permanent alliance can distort intelligence. Investigators should follow evidence, money, logistics, and personal networks (McNicholas, 2016; United Nations Office on Drugs and Crime, 2023).

23. Impact of Cyber Threats

Cyberattacks can disrupt terminal operating systems, navigation, cargo booking, customs data, cranes, gates, fuel systems, and communication. Consequences include delay, unsafe movement, theft, ransom, data loss, and physical damage. The 2017 NotPetya incident caused major disruption to Maersk and demonstrated how malware outside a port can affect global shipping. Cyber risk is operational risk, not only an information-technology problem (International Maritime Organization, 2021).

24. Cyber Threats to Ports and Ships

Ships rely on bridge systems, electronic charts, satellite links, machinery control, and administrative networks. Ports depend on interconnected public and private systems. Weak passwords, unsupported software, vendor access, phishing, removable media, and poor separation of networks can create entry points. Controls include asset inventories, patching, backups, network segmentation, access management, incident response, crew training, and safe manual alternatives. Cybersecurity should be incorporated into safety and security management (International Maritime Organization, 2021; United States Coast Guard, 2024).

25. Major Targets at Ports and on Ships

Potential targets include passengers, crews, hazardous cargo, fuel terminals, bridges, cranes, navigation systems, communications, data, and chokepoints. Attackers may seek theft, ransom, sabotage, espionage, coercion, or disruption. Target analysis should assess attractiveness, vulnerability, and consequence. Protection should prioritize critical functions and recovery capability, since no system can eliminate all risk. Resilience—maintaining or restoring trade after an incident—is therefore a core part of maritime security (McNicholas, 2016; International Maritime Organization, 2021; United States Coast Guard, 2024).

Conclusion

The twenty-five topics from McNicholas's text reveal that maritime security combines commerce, engineering, law, intelligence, environmental management, and international cooperation. Seaports and ships enable daily life but concentrate valuable goods and essential systems. The ISPS Code and MTSA establish formal security frameworks, while piracy, terrorism, trafficking, fraud, and cyberattack continually adapt. Effective protection is layered and risk-based. It depends on trained people, reliable documents, secure technology, trusted supply-chain partners, lawful enforcement, and plans for recovery. The objective is not to stop maritime trade in the name of security; it is to keep trade moving safely while reducing opportunities for harm (McNicholas, 2016; International Maritime

Organization, 2021; United Nations Office on Drugs and Crime, 2023; United States Coast Guard, 2024).

References

International Maritime Organization. (2021). *Guide to maritime security and the ISPS Code*.

McNicholas, M. (2016). *Maritime security: An introduction* (2nd ed.). Butterworth-Heinemann.

United Nations Office on Drugs and Crime. (2023). *Global maritime crime programme*.

United States Coast Guard. (2024). *Maritime Transportation Security Act and regulated facility guidance*.