Legal questions arising from maritime security considerations in the energy and cyber domains

LCDR Kelly A. Mosteller, USA-N
Combined Joint Operations from the Sea Centre of Excellence (CJOS COE)
Norfolk, VA, USA

Introduction

Several news-worthy events this year have highlighted the intersections of the energy sector and the cyber domain with maritime security. Maritime criminals in the Gulf of Guinea specifically target vessels carrying crude oil, impacting production costs and regional security. In October, it was revealed that cyber-attacks on the system controlling the location and movement of shipping containers had allowed criminals to smuggle tons of cocaine and heroin through the Port of Antwerp over a two-year period. Doomsday scenarios envision criminal or terrorist organizations taking control of a chemical tanker’s e-navigation system and remotely piloting the ship for use as an instrument of destruction.

Despite certain drawbacks, the energy industry and cyber technologies can also enhance safety at sea and improve maritime security. Novel legal issues arise from the place where maritime security considerations overlap the energy sector and cyber domain, and these issues should be considered carefully by militaries, policy-makers, and intergovernmental bodies when crafting solutions to twenty-first century maritime security challenges.

Energy

The economic implications of the intersection of energy and maritime security are widely explored. Legal issues; however, continue to arise, and many remain unsettled. Some of these issues are definitional, and might be resolved through stakeholder conferences aimed at reaching consensus on the meaning or application of key terms. However, some legal issues arise from social or political deficiencies. Experts note the frequent coincidence of large natural resource stores and weak governance systems; this complicates the relationship between extractive companies and their host nations and muddies the legal waters when issues arise.

The extractive industry is often named as a catalyst of maritime security challenges in the Gulf of Guinea. Issues of resource distribution and disenfranchisement give rise to social unrest and crime that often spills over into the maritime domain. Data from the International Maritime Bureau indicates that maritime criminal organizations based in Nigeria specifically target vessels associated with the extractive industry: crude carriers are hijacked and their cargoes stolen, oil platforms require constant security to protect their crew and suppliers, and illegal bunkering is rampant throughout the Niger Delta.

Legal questions that arise from this situation revolve around definitions of piracy, jurisdiction over maritime crime, and the strength (or existence) of domestic laws governing maritime crime. International efforts to develop better means of bringing maritime criminals to justice, such as task forces to aid in the development of domestic laws and the establishment of the Regional Anti-Piracy Prosecution and Information
Coordination Centre (RAPPICCC) in the Seychelles, have met with some success, but these efforts and similar initiatives merit additional attention.

The environmental impacts of oil and gas extraction can contribute to threats against maritime security. Oil spills or leaks from extraction sites, and pollution from rigs or vessels have led some communities to resort to what they see as vigilante justice, particularly if the community was heavily dependent upon the maritime environment for their livelihoods. In these environments, the question of how communities can recover against extractive companies for damage caused to the living resources is often challenging, particularly in countries lacking effective legal institutions.

In regions where new offshore deposits of oil and natural gas have recently been discovered, countries may choose to commit a substantial portion of their maritime defense capabilities to protecting those lucrative assets. This leaves the rest of their maritime territory undefended from threats such as illegal fishing or pollution, or rendering an effective response impossible in the event of a maritime disaster such as a ferry sinking. This presents a legal and policy challenge regarding a government’s duty to protect its people through effective legislation and regulation of public services like transportation and national resources like fish stocks.

A growing area of concern, as evidenced by the many competing claims over vast portions of the South China Sea, involve territorial disputes over offshore “features” such as rocks, sea mounts, and islands. The classification of these features determines the extent of the rights that attach to that feature: while islands capable of supporting human habitation and economic life are entitled to their own 200nm Exclusive Economic Zones (EEZs), uninhabitable rocks only merit a 12nm territorial sea. Therefore, most of the disputes over seemingly valueless chunks of land are really driven by a desire for control over the highly valuable natural resources that may lie beneath the sea floor. These issues take years to resolve through the international tribunals established for that purpose; in the meantime, not only is resource exploration and production untenable, but maritime security itself is threatened as sovereign states seek to maintain a fragile peace. Similar issues of territorial rights are arising in the arctic regions as countries seek to stake their claims on resources that are, for now, still trapped beneath the ice.

Despite its role in exacerbating maritime insecurity, the energy sector could, and arguably does, contribute to greater maritime security, though this also raises some legal issues. Increased exploration of offshore formations results in a higher number of vessels and rigs in many areas. This can contribute to a greater awareness of what is taking place in the maritime domain, as well as greater importance being placed on maritime security. Indeed, discoveries of oil and gas offshore have contributed to a reduction in “sea blindness,” or the lack of concern that many countries show for the issues affecting their territorial waters and exclusive economic zones, as these countries begin to recognize the lucrative resources under their waters and the need to protect those resources in order to reap the economic benefits.

Private armed security teams onboard vessels have been credited with the dramatic reduction in successful pirate attacks off the east coast of Africa. But the presence of these armed guards raises legal issues in regard to when a vessel is engaging in innocent passage. A vessel must be aware of the laws of each country whose waters it sails, as most countries restrict the presence of armed vessels in their territorial waters.
Many of the countries blessed with abundant energy resources are also burdened with ineffective governance institutions. Thus, when it comes to the intersection between the energy sector and maritime security, the legal issue that emerges most clearly is the need for international cooperation to strengthen the regulatory, legal, and law enforcement systems of oil-rich countries.

**Cyber**

The cyber domain both enhances maritime security and creates vulnerabilities in the maritime sector. Understandably, mariners want to be cautious about sharing information in order to protect themselves from potential exploitation, but national militaries and international bodies often seek greater information sharing as a means of enhancing their maritime domain awareness (MDA) and developing a Recognized Maritime Picture (RMP). Balancing these interests has created new legal and policy questions.

The cyber domain facilitates information sharing that can contribute to maritime security. MDA systems can improve early warning capability for threats and response capability for disasters, improving the ability of national maritime authorities to secure their waters and maritime infrastructure. Digital and internet-based technology also enables the coordination of multinational forces in international waters.

Legal issues of privacy arise when discussing the type and extent of the information being shared, with whom the information is shared, and under what parameters it is shared. Ship and cargo tracking can be accomplished more easily in using digital technology, but issues of privacy and intellectual or commercial property arise in these realms also.

Despite the benefits cyber-based technologies can bring to maritime security, the prevalence of cyber-based control systems has also created some weaknesses in critical maritime areas. The Port of Antwerp, Belgium uncovered a drug smuggling operation that had been underway for approximately two years beginning in June, 2011. In October 2013, it was revealed that the smugglers were using hackers and other cyber-theft methods to redirect the containers in which the contraband was shipped, and steal them from the port. Legal issues may arise if a country’s laws have not been updated or are not broad enough to encompass the cybercrime that can threaten the maritime infrastructure.

Always seeking greater efficiency, some shipping companies are turning to e-navigation. The International Association of Lighthouse Authorities (IALA) defined e-navigation as the “harmonised collection, integration, exchange, presentation and analysis of marine information onboard and ashore by electronic means to enhance berth to berth navigation and related services, for safety and security at sea and protection of the maritime environment.” Some have raised concerns whether e-navigation opens control of ships to hackers, but a more important legal question may involve the apportioning of liability in the event that a ship relies on the e-navigation concept to its detriment.

The mandatory use of Automatic Identification System (AIS) raises legal issues as well. AIS allows other ships as well as coastal authorities to see information about the ship, including its identity, type, position, course, speed, navigational status, and other
safety-related information. Many mariners, however, are concerned that using AIS can facilitate criminals and pirates targeting their vessel, and frequently turn AIS off when they are transiting through higher-risk waters. Failing to use AIS can open a vessel to civil penalties in certain countries.

Placing greater control of maritime assets -- whether containers, charts, or ships -- in the cyber domain demands commensurate increases in cyber security. In February 2013, President Obama signed an Executive Order assigning responsibility for critical infrastructure cybersecurity to various executive agencies. The order contemplated issues such as enforcement, intellectual property rights, and privacy concerns of affected parties. Significant milestones provided in the Order will be complete by May 2014, and it would be prudent for international maritime bodies to adopt best practices from the U.S. process to their own consideration of maritime cybersecurity issues.

**Conclusion**

Maritime security has long posed unique challenges to the national and international legal systems that seek to address it. New discoveries and the growing importance of offshore energy sources have added to the complexity of governance over these areas, and opened new geographic regions to maritime security threats. Rapid advances in cyber applications have helped to improve awareness of the maritime domain, but they have also created certain vulnerabilities in the maritime sector that could facilitate smuggling, terrorism, or attacks on a nations’ critical infrastructure. The legal environment has not been able to keep pace with these changes in the maritime security environment, leaving gaps in the current international and national legal responses. National and international bodies must develop clear legal guidance so that those organizations charged with maintaining global maritime security can do so with the confidence that their enforcement actions will be in support of the law, not against it.

LCDR Mosteller is a Reserve Staff Officer at CJOS COE in Norfolk, VA. For further information, she may be contacted at kelly.mosteller@navy.mil. For further information about CJOS COE, please see the CJOS COE web page at www.cjoscoe.org.
Sources:


