SCHOOL OF LAW
CASE WESTERN RESERVE UNIVERSITY

Case Western Reserve Journal of International Law

Volume 46 | Issue 1

2014

Operational Responses to Piracy -- A First Principles Approach

Mark Sloan

Follow this and additional works at: https://scholarlycommons.law.case.edu/jil

 Part of the International Law Commons

Recommended Citation

Mark Sloan, *Operational Responses to Piracy -- A First Principles Approach*, 46 Case W. Res. J. Int'l L. 375 (2013)
Available at: https://scholarlycommons.law.case.edu/jil/vol46/iss1/17

This Article is brought to you for free and open access by the Student Journals at Case Western Reserve University School of Law Scholarly Commons. It has been accepted for inclusion in Case Western Reserve Journal of International Law by an authorized administrator of Case Western Reserve University School of Law Scholarly Commons.

Case Western Reserve Journal of International Law

Volume 46 Fall 2013 Issues 1 & 2

Operational Responses to Piracy—A First Principles Approach

Mark Sloan

OPERATIONAL RESPONSES TO PIRACY—A FIRST PRINCIPLES APPROACH

Mark Sloan[*]

There is a widely held consensus that maritime piracy is best prevented by addressing its root causes, but this article builds on an assumption that operational responses will also continue to play a key role in disrupting the pirates' business model on land and at sea. To consider those operational responses from first principles, it employs the risk management approach used in critical infrastructure protection to analyse the mission of the shipping industry, identify the critical assets, consider the threat, and assess the vulnerabilities of those critical assets. It uses these steps to identify the risk and the management action necessary to mitigate that risk, while also considering incident response, consequence management, and steps to restore mission success. This analysis highlights the relevance of operational responses to countering opportunity and means in particular, and highlights the fact that reducing opportunity is a shared responsibility between security forces and the shipping industry.

CONTENTS

* Mark Sloan is a Research fellow at Dalhousie University's Centre for Foreign Policy Studies and team leader for the Operational Responses Theme of the Dalhousie University's Marine Piracy Project.

I. INTRODUCTION

A. Developing an Operational Response Framework

There seems to be little disagreement among academics and practitioners alike, that the best way to counter existing outbreaks of piracy, and to prevent future outbreaks, is to address the root causes, which inform the motive elements of individual crimes. Furthermore, this consensus also points to the fact that solutions to the root causes generally, but not exclusively, lie in the socioeconomic sphere. Nevertheless, whatever the stage at which the problem is identified and countered, discouraging, deterring, disrupting, or defeating piracy requires enforcement of the rule of law on land and at sea, and the application of appropriate operational responses.[1] Moreover, to be successful, such responses must be coordinated with socioeconomic and other initiatives, and be accompanied by, and must support, the related legal and governance structures and processes that bound operational responses.

The continued need for operational responses provides the underlying assumption for this article. Moving forward from the assumption, the issue becomes identification of a suitable framework for the development of the appropriate operational responses, responses that must be tailored to the specifics of an actual or potential outbreak of piracy. Working from first principles in this process is essential in order to avoid the risk of deciding on the solution before the true nature of the problem has been defined. This brief analysis uses a risk management methodology to support this first principles approach, the model selected being that used in critical infrastructure protection. But why choose critical infrastructure protection as the framework, when shipping itself is not generally considered to be critical infrastructure? Even the concept of Maritime Global Critical Infrastructure focuses on key choke points and international maritime hubs, rather than on shipping itself.[2] The

1. *See* M. SLOAN & D. GRIFFITHS, DALHOUSIE MARINE PIRACY PROJECT: OPERATIONAL RESPONSES FOR THE DISCOURAGEMENT AND SUPPRESSION OF MARINE PIRACY (MARINE AFFAIRS PROGRAM TECHNICAL REPORT #3) 17 (2012), *available at* http://marineaffairsprogram.dal.ca/Publications (defining operational responses as those actions taken to counter a potential or actual outbreak of piracy that are neither targeted at the root causes of piracy, nor address the related legal and governance issues).

2. *See* RISK GOVERNANCE COUNCIL, RISK GOVERNANCE OF MARITIME INTERNATIONAL GLOBAL CRITICAL INFRASTRUCTURE: THE EXAMPLE OF THE STRAITS OF MALACCA AND SINGAPORE 9, 12 (2011), *available at* http://www.irgc.org/IMG/pdf/irgc_mgcireport_2011.pdf (considering the Straits of Malacca and Singapore as Maritime Global Critical Infrastructure because they are two of the most strategic chokepoints for world oil transport).

challenge here is not to argue whether shipping should be considered critical infrastructure, but rather to use the principles of critical infrastructure protection as a means of drawing out some of the key aspects associated with the identification and application of operational responses to piracy.

B. Definitions and Assumptions

Before proceeding further, it is necessary to clarify the definition of piracy, as it is used in this article, and to set out the principles of critical infrastructure protection. In a recent study conducted at Dalhousie University,[3] it was proposed that the definition of piracy should include acts committed both inside and outside territorial waters. This proposal was based on three considerations. First, the broader definition allows the identification of potential low-level precursors to larger outbreaks of piracy. These precursors often occur inside territorial waters, and such attacks are equally threatening to commercial shipping, fishing vessels, and private marine craft as attacks conducted on the high seas. Second, in order to make appropriate recommendations for operational and other responses, the full extent of attacks must be recorded. And, third, this definition helps the development of a holistic maritime security strategy, whether nationally, regionally, or internationally, since piracy is but one of a number of challenges to maritime security. The Dalhousie study also recommended that robbery (armed or unarmed) from ships that are berthed alongside in a port should be excluded from the definition because dealing with such incidents should be a routine national policing issue.[4] The Dalhousie study's definition of piracy therefore falls between that of the U.N. Convention on the Law of the Sea (UNCLOS)'s definition of piracy as acts on the high seas,[5] and the "piracy and armed robbery" definition established by the International Maritime Organization (IMO) and used by the International Maritime Bureau (IMB).[6] For these reasons, this analysis uses the revised definition of piracy:

---

3. *See* L. FANNING, M. SLOAN, S. WHITMAN, H. WILLIAMSON, & S. DOUGLAS, DALHOUSIE MARINE PIRACY PROJECT: EXPLORING AN INTEGRATED APPROACH TO THE SUPPRESSION AND PREVENTION OF MARINE PIRACY (MARINE AFFAIRS PROGRAM TECHNICAL REPORT #4) (2012) [hereinafter INTEGRATED APPROACH]. Details of the Dalhousie Marine Piracy Project are available at http://dmpp.management.dal.ca/.

4. *Id.* at 15.

5. U.N. Convention on the Law of the Sea art. 101, *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 (entered into force Nov. 16, 1994) (defining piracy as "any illegal acts of violence or detention, or any act of depredation, committed for privates ends . . . on the high seas . . .").

6. Int'l Maritime Org. [IMO], *Code of Practice for the Investigation of Crimes of Piracy and Armed Robbery Against Ships*, Annex ¶¶ 2.1, 2.2,

> The participation, planning and support of attempted or actual deliberate (violent) criminal interference with the rights and freedoms of the seas, which target marine craft (vessels) and persons for personal economic gain.[7]

The Dalhousie study also made the assumption that piracy will never be eradicated completely, even though it may cease to be a meaningful risk in a particular region. That assumption remains valid in this analysis as well.

The principles of critical infrastructure protection are simple. One must start by analyzing the mission; then identify the critical assets; consider the threat; assess the vulnerabilities of the critical assets; use these steps to identify the risk; and then take management action to mitigate that risk while also planning incident response, consequence management, and steps to restore mission success.

II. Mission and Critical Asset Analysis

When applying this approach to the problem of countering marine piracy, defining the mission of seafarers and their vessels is relatively straightforward.[8] Simplistically, this includes the safe, timely and legally compliant passage of the designated cargo, passengers, and crew from their place of loading to the required point of offload. Also quite simply, the critical assets under consideration are the vessels, their crews, passengers, and cargos. Given this mission and critical assets, it immediately becomes apparent from the critical infrastructure protection framework that the risk of a successful pirate attack will be minimized by one or both acts of reducing the threat or the reducing the vulnerability of the critical assets.

III. Threat Analysis

In order for efforts to reduce the threat of piracy to be effective, threats must first be recognised and then understood. Although its general nature is encapsulated in the definition of piracy, the detail is more complex, and not only varies from one piracy area to another, but also changes. The different business models used by pirates in the Indian Ocean and in the Gulf of Guinea, and their evolution over time, are a clear illustration of these variations.

However, recognising a threat and understanding it are two separate challenges. In an ideal world, the early, localised,

IMO Assemb. Res. A. 1025 (26) (Dec. 2, 2009) (covering both the UNCLOS definition of piracy as well as "armed robbery at sea").

7. INTEGRATED APPROACH, *supra* note 3, at 6.

8. Vessels refer to privately owned leisure as well as commercial vessels of all types.

opportunistic, subsistence type precursors to a significant outbreak of piracy will be reported and recognised for what they are, with actions then being taken to curb the crime before it takes on a more organised and challenging form. The theory is simple, but there are a number of reasons why nations may be unable or reluctant to acknowledge that they have a piracy problem. To start with, in the absence of an effective incident reporting and recording process, they may fail to recognise the threat. Even if such a problem is recognized, it may not be acknowledged for several reasons, including the perceived impact on a country's international standing and on the willingness of vessels to use its waters and ports when faced with such a threat, or the lack of national laws recognising the crime of piracy. Nevertheless, early identification of a potential piracy problem is essential for the development of appropriate operational responses.

In the case of the Somali piracy outbreak, many Somalis claimed that the early piracy attacks were a response to their need to counter illegal, unreported, and unregulated fishing in their waters.[9] If this concern had been recognised earlier, and if steps were taken by the regional and international community to address the problem in the absence of any effective government in Somalia, it would have removed the claim of legitimacy for the pirates' actions. Additionally, such efforts may have prevented or slowed the development of the much wider threat.

Understanding the pirates' business model, and therefore the threat, is as complex now as historically. However, amidst these complexities, there has been a constant in the piracy formula—it occurs where motive, means, and opportunity combine to the extent that the potential financial gains outweigh the risk and fear of arrest, injury, or death. Without a motive, means to conduct the crime will not be sought, and opportunities will not be exploited. Each of these three factors is shaped by the context of the particular region and leads to the development of differences in the business models. Motive may be as simple as greed, or as complex as gang or tribal loyalties/rivalries, revenge, and social retribution. Opportunity arises from a flawed maritime security environment, weak rule of law on land, and the availability and vulnerability of potential targets. Means include the availability of the organisation, finances, material,

9. *See, e.g.*, Tristan McConnell, *Somali Pirates' Rise Linked to Illegal Fishing and Toxic Dumping*, GLOBAL POST (Mar. 16, 2012), http://www.globalpost.com/dispatch/news/regions/africa/120306/pirates-Somalia-how-it-started%20 (stating how illegal fishing, which costs the Somali economy hundreds of millions of dollars, gave rise to piracy); U.N. Secretary General, *Rep. of the Secretary-General on the Protection of Somali Natural Resources and Waters*, ¶ 44, U.N. Doc. S/2011/661 (Oct. 25, 2011) (discussing how the piracy surge has led to a decrease in illegal fishing on the Somali coast).

information, and personnel necessary to support the activity. As with any form of crime, countering any or all of this trinity will render the piracy business model unsustainable, thereby reducing or negating the threat, and the risk.

A. Motive

Comparing modern with historic outbreaks of piracy, motive is perhaps the least changed of the factors. However, it is not unreasonable to suggest that, as the gap between rich and poor has become more transparent to those at the poor end of the spectrum, the growing awareness of their plight has created increased motive to address the imbalance. While socioeconomic solutions are at the heart of countering motive, and thereby reducing the threat, operational responses also have a role—for example, when the rule of law is used to deal with tribal loyalties or rivalries, revenge or social retribution.[10] In contrast, addressing opportunity and means are heavily dependent on operational responses.

B. Opportunity

Opportunity for pirates arises when effective rule of law is weak or absent, thus allowing them to operate with relative impunity. Additionally, it stems from vulnerabilities among potential targets. Ineffective rule of law where piracy is concerned therefore includes both a flawed maritime security environment and weak rule of law on land. Overcoming this requires political will and, in the case of maritime security, recognition of the importance of the territorial waters and adjacent high seas to the state's security and economy. Even in July 2011, the Commander of the Benin Naval Training Center stated that "[c]ountries like mine do not realize what they are losing at sea by not conducting security."[11] An associated and equally important need exists for states to enact national legislation establishing piracy as a crime, and therefore providing the legal foundation for practical counter-piracy actions and subsequent prosecutions.

If piracy emanates from more unstable or less developed nations or regions, capacity building may be required in order to develop a state's ability to enforce the rule of law. In the context of piracy and other organised crime, it is important that such capacity building is

10. *See* Brett D. Schaefer, *Piracy: A Symptom of Somalia's Deeper Problems*, HERITAGE FOUND. (Apr. 17, 2009) (noting how tribal factions in Somalia have deprived the state of proper governance and legitimacy, thereby creating a climate ripe for piracy).

11. *Seminar Focuses on Maritime Safety and Security in West and Central Africa*, AFR. CTR. FOR STRATEGIC STUDIES (July 25, 2011), http://africacenter.org/2011/07/seminar-focuses-on-maritime-safety-and-security-in-west-and-central-africa/.

not just focused on national development, but also considers the regional and international security dimension in order to improve interoperability, situational awareness, and situational understanding between agencies and nations. The need for such an approach in the Gulf of Guinea has been recognized by the European Commission,[12] among others, and was also the driver behind the formation of the Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia (ReCAAP).[13] The European Union led project "Critical Maritime Routes in the Gulf of Guinea Programme (CRIMGO)" focuses on training for coastguards and establishing a network to share information between countries and agencies.[14] That is not to say that the approach has to be complex, and progress made developing information sharing centres under the Djibouti Code of Conduct,[15] for example, is clear evidence of what can be achieved relatively simply.

In terms of the availability of potential targets, there are certainly more now than historically because of the greater number of ships and tonnage of cargo moved by sea, the number of ports in operation, and the increase in the number of leisure craft. According to figures compiled by Clarksons, a shipping information provider,[16] the world's fleet of commercial vessels over 100 tons numbered 86,300 ships at the end of 2012, and in 2013 there were 57,400 ships actually carrying cargo. However, it is not the *availability* of potential targets that

12. CRISTINA BARRIOS, EU INST. FOR SECURITY STUDIES, FIGHTING PIRACY IN THE GULF OF GUINEA OFFSHORE AND ONSHORE 3 (2013), *available at* http://www.iss.europa.eu/uploads/media/Brief_20.pdf (describing the European Commission's initiatives in the Gulf of Guinea that are focused on maritime security, surveillance, and information sharing).

13. Regional Cooperation Agreement on Combating Piracy and Armed Robbery Against Ships in Asia, Nov. 11, 2004, 2398 U.N.T.S. 199 (entered into force Sept. 4, 2006).

14. Press Release, European Commission, New EU Initiative to Combat Piracy in the Gulf of Guinea (Jan. 10, 2013), *available at* http://europa.eu/rapid/press-release_IP-13-14_en.htm.

15. *See* Int'l Maritime Org. [IMO], *Code of Conduct Concerning the Repression of Piracy and Armed Robbery Against Ships in the Western Indian Ocean and the Gulf of Aden*, Djibouti Meeting Res. 1 (Jan. 29, 2009), *available at* http://www.imo.org/OurWork/Security/PIU/Documents/DCoC%20English.pdf; Loukas Kontogiannis, *Info Sharing & Maritime Situational Awareness: Status of Implementation Efforts & Future Plans*, INT'L MAR. ORG., http://ipsc.jrc.ec.europa.eu/fileadmin/repository/mare/vescosur/pmar_wks/IMO_presentation.pdf (last visited Mar. 27, 2014).

16. *Too Many Ships in the World Merchant Fleet*, HELLENIC SHIPPING NEWS (Apr. 8, 2013), http://www.hellenicshippingnews.com/News.aspx?ElementId=984ef639-7f94-4d62-88a9-f80b3ecc6fb9.

contributes to opportunity so much as their *vulnerability*, hence the importance of considering the vulnerability analysis.

C. Means

The final threat driver is means, and the analysis of means and ways to counter them have been significantly advanced by recognition of the fact that piracy in all but its subsistence form employs a business model. Previous efforts to end piracy outbreaks have put great emphasis on actions taken at sea, thereby operating to suppress criminal acts that are often simply symptoms of a greater problem on land. In contrast, looking at piracy from the perspective of the business model highlights the fact that its support functions are generally based on land. This helps in the identification of those parts of the model that are most vulnerable, or the disruption of which will have most effect on the operation of that model. However, as was the case in Somalia, for example, and to an extent the way it remains so today, the lack of a secure environment on land meant that actions at sea were almost all that was possible until conditions ashore improved. Actions at sea should therefore not be discounted as an option.

Disruption to the business model may be short term, thereby allowing more permanent measures to be put in place in order to counter any or all of opportunity, motive, and means. Alternatively, disruption may be a longer-term solution in itself if it disrupts the model to the extent that it cannot evolve, thereby impacting the ability to conduct piracy at all. Different agencies will focus on different parts of the model, and working to counter the business model therefore emphasises the essential need for a truly inter-agency approach. Achieving such a coordinated inter-agency approach is another area where capacity building has a role to play, as recognized by the IMO's current work with the Gulf of Guinea nations.[17] The fact that many of these and other points raised have parallels with lessons learned in Iraq and Afghanistan emphasizes the need to identify and learn lessons from efforts to counter other forms of organized crime. The specific nature of these crimes may differ, but similarities between the business models provide good opportunities to transfer lessons learned from one "campaign" to another.

One element of the means factor that does not receive much attention is the availability of information. As with almost all walks of life, the plethora of widely available open source information has brought a new dimension to organized crime, including piracy, and

17. *IMO Strategy for Implementing Sustainable Maritime Security Measures in West and Central Africa*, INT'L MAR. ORG. (Mar. 18, 2014), http://www.imo.org/OurWork/Security/WestAfrica/Pages/WestAfrica.aspx (describing a Code of Conduct for West African states to promote regional cooperation in the fight against piracy).

this is reflected in the pirates' knowledge of shipping movements and of the measures being taken to counter their attacks. For example, if the European Union Naval Force (EU NAVFOR) deployed to the Indian Ocean changes its posture, or if it experiences a reduction in the number of assets allocated by contributing nations, the pirates will learn of these changes through the media and other sources very quickly. As another example, access to Automatic Identification System (AIS) tracking is easy to achieve.[18] With this access, a plethora of information about shipping movements is readily available, as is information that can be used to identify potential victims. It is too late to turn off the "information tap," but an awareness of what can be learned from open source information, and reducing some information availability, is another way in which vulnerability can, and is being reduced.

IV. VULNERABILITY ANALYSIS

Government security forces such as naval and coastguard units, as well as police and security forces on land, have a significant role to play in reducing vulnerability of the critical assets. So too does the willingness of the shipping companies, owners, operators, and charterers of vessels to implement appropriate ship protection measures. The importance of the latter has been widely debated in recent years, particularly with respect to the need and desirability of embarking armed security guards, whether Privately Contracted Armed Security Personnel (PCASP) or the Vessel Protection Detachments (VPDs) provided from armed forces personnel. Despite the ebbs and flows of this particular debate, shipping industry recognition of their role in reducing vulnerability has been reflected in the development of Best Management Practices[19] for use in the Indian Ocean. More recently Interim Guidelines for Owners, Operators, and Masters for protection against piracy in the Gulf of Guinea region[20] were produced at the end of 2012.

18. *See AIS Transponders*, INT'L MAR. ORG., http://www.imo.org/OurWork/Safety/Navigation/Pages/AIS.aspx (last visited Mar. 25, 2014) (stating how the AIS is designed to automatically provide ships with information).

19. BMP 4: BEST MANAGEMENT PRACTICES FOR PROTECTION AGAINST SOMALI BASED PIRACY (2011), *available at* http://www.mschoa.org/docs/public-documents/bmp4_low_res_sep_ 5_2011.pdf.

20. INTERIM GUIDELINES FOR OWNERS, OPERATORS AND MASTERS FOR PROTECTION AGAINST PIRACY IN THE GULF OF GUINEA REGION 2 (2012), *available at* https://www.bimco.org/en/News/2012/12/%7E/media/Security/Piracy/Gulf_of_Guinea/2012-12-20_RT_agreed_GoG_anti-piracy_guidance.ashx (stating that "these interim Guidelines aim to bridge the gap between the advice currently found in BMP4 and the prevailing situation in the Gulf of Guinea region").

The classic vulnerable vessel has a low freeboard, and travels slowly. A study in 2011[21] identified that the average speed of the ships seized in the Indian Ocean was 13 knots, while the average freeboard was only 4.5 metres. That study also stated that there had been no successful attacks reported on vessels with a service speed of more than 18 knots and with more than 8 metres freeboard.[22] Conversely, this indicates that reducing transit speeds in order to save fuel will increase certain vessels' vulnerability to attack if a piracy threat is present. It also means that some vessels should simply not be at sea in the threat area. This might be a difficult case to make economically when the actual risk of being attacked is low (and in the Indian Ocean, even at the height of the piracy threat, it was less than 1 percent),[23] but if economics are not a factor, it is a very effective way of reducing vulnerability.

Measures to reduce vulnerability are therefore at the core of preventing successful attacks, and they should be mandatory rather than discretionary when the threat level dictates such measures to be appropriate. The fact that there are already legal mechanisms in place that require vulnerabilities to be reduced, and also mandate monitoring the extent to which those requirements are being met, is sometimes overlooked or ignored because compliance is inconvenient.

Key among such mechanisms is the International Ship and Port Facility Security Code, under which ships are expected to identify critical areas and to conduct a ship security assessment.[24] However, differing interpretations of this code have led to a lack of clear direction, which has been interpreted by some states as allowing an administrative approach to security that tends to apply only when the ship is in port or well inside territorial waters. Even though flag state responsibilities are established in UNCLOS and subsequent additional guidance and legislation, there is still more work to be done to ensure that suitable, common standards are achieved, and to discourage the use of any flag that does not meet its international obligations.

---

21. CATLIN ASSET PROTECTION, PIRACY 2011: A GROWING MENACE 8 (2011), *available at* http://www.catlin.com/en/UnitedKingdom/Insurance/War-Political-Risk/~/media/Downloads/UK/Thought%20leadership/Catlin-report-Piracy-a-growing-menace.ashx.

22. *Id.*

23. *Horn of Africa Piracy Activity Update – 8 Jul*, OCEANUSLIVE (July 8, 2011), http://www.oceanuslive.org/main/viewnews.aspx?uid=00000286.

24. Int'l Maritime Org. [IMO], *Consideration and Adoption of the International Ship and Port Facility Security (ISPS) Code,* ¶¶ 7.2, 8.5, IMO Conf. Doc. SOLAS/CONF.5/34 (Dec. 17, 2002), *available at* http://www.infrastructure.gov.au/transport/security/maritime/isps/files/resolutions_2_9.pdf (outlining the necessary elements of a ship security assessment).

Despite the important role of the Port State Control Regime,[25] various studies have indicated shortcomings in its effectiveness in some parts of the world. Although seldom commented on in relation to countering piracy, the regime has a role to play in reducing the number of ships at sea with key vulnerabilities, and therefore, deserves continued attention.

Armed with an understanding of the specific nature of the threat in an area, and the vulnerabilities of any particular vessel, it is therefore relatively simple to assess the degree of risk. Once that is complete, it is possible to identify appropriate mitigating action, whether that action is required by or for specific vessels in build or already in operation, or nationally, regionally or internationally by a range of agencies.

V. INCIDENT RESPONSE, CONSEQUENCE MANAGEMENT, AND RESTORATION OF MISSION SUCCESS

In addition to providing a framework to support identification of the levels of threat, vulnerability, and risk, the critical infrastructure protection process also requires consideration of incident response, consequence management, and restoration of mission success. As with much of what has already been discussed, this will require a multi-agency approach and a range of actions, some of which include the need for operational responses. Actions to free pirated ships and hostages, or to pay ransoms, are the obvious examples, but others, such as dealing with an environmental disaster (e.g., a major oil spill or a collision at sea), are also likely, and will require an operational response. Each situation will require a well exercised response if their impact is to be contained. The environmental issue is perhaps particularly relevant in the current piracy outbreak in the Gulf of Guinea, where the business model commonly involves the hijack of a

25. Port State Control is the inspection of foreign ships in national ports to verify that the condition of the ship and its equipment comply with the requirements of international regulations and that the ship is manned and operated in compliance with these rules. IMO has encouraged the establishment of regional Port State Control organizations and agreements on Port State Control. Memoranda of Understanding (MoUs) have been signed covering all of the world's oceans: Europe and the North Atlantic (Paris MoU); Asia and the Pacific (Tokyo MoU); Latin America (Acuerdo de Viña del Mar); Caribbean (Caribbean MoU); West and Central Africa (Abuja MoU); the Black Sea region (Black Sea MoU); the Mediterranean (Mediterranean MoU); the Indian Ocean (Indian Ocean MoU); and the Riyadh MoU. *See Port State Control*, INT'L MAR. ORG., http://www.imo.org/blast/mainframe.asp?topic_id=159 (last visited Mar. 26, 2014).

tanker, followed by transhipment of its cargo to another vessel for subsequent resale.[26]

Underpinning all of this effort is the need for an effective incident reporting process. All of the agencies who maintain statistics about piracy attacks openly acknowledge that they are only showing what is reported, and that a significant number of attacks are not reported, and thus absent from the databases. Part of the challenge is certainly an unwillingness to report incidents, but another aspect is the multiplicity of reporting channels. As one analyst noted, "[i]t seems clear that the problem is both simple, in that we need to effectively capture data on pirates, but at the same time it is exquisitely complex, in so far as shipowners don't want to report, security companies are accused of scaremongering if they do report, and the agencies charged with collecting and collating, aren't sure what they are meant to be gathering, for whom and for what purpose."[27] If formal reporting mechanisms are not capturing all piracy incidents in a region, measures should be implemented that will improve the ease of access to a reporting hub for those making the report, encourage incidents to be reported (by changing the culture), and establish national and/or regional reporting systems that combine in a seamless manner. Only then will counter-piracy activities be targeted to best effect, and a more complete record of piracy activity identifying the true extent of the problem be established.

VI. CONCLUSION

In conclusion, this brief analysis uses the critical infrastructure protection framework to illustrate how a systematic risk management approach works from first principles to help develop the operational responses to piracy, and to plan for incident response and restoration of mission success. It also provides a framework against which the various options might be validated, and it aids development of an understanding of the wider cross-domain issues associated with countering the problem. This includes furthering the coordinated inter-agency, stakeholder-wide approach that is essential to effectively counter piracy, whether preemptively or reactively.

26. *See* Freedom C. Onuoha, *Oil Piracy in the Gulf of Guinea*, CONFLICT TRENDS 28, 31 (2012) (explaining the modus operandi of pirates in the Gulf of Guinea).

27. *Doesn't Add Up: A Look at the Real Facts Behind the Drop in Piracy Attacks in the Indian Ocean*, INS. BULL. (SEACURUS Ltd., Gateshead, U.K.), Apr. 2013, at 11 www.seacurus.com/newsletter/Seacurus_Issue_24.pdf.


SCHOOL OF LAW
CASE WESTERN RESERVE
UNIVERSITY