INTERNATIONAL LAW STUDIES
Published Since 1895
U.S. NAVAL WAR COLLEGE

Maritime Law Enforcement Operations and Intelligence in an Age of Maritime Security

Douglas Guilfoyle

93 INT'L L. STUD. 298 (2017)

Volume 93 2017

Published by the Stockton Center for the Study of International Law

ISSN 2375-2831

Maritime Law Enforcement Operations and Intelligence in an Age of Maritime Security

*Douglas Guilfoyle**

CONTENTS

* Professor of Law at the Faculty of Law, Monash University, Australia. This paper arose from the Maritime Intelligence Law and Law of the Sea Workshop held in Washington DC in October 2016, co-sponsored by the Stockton Center for the Study of International Law, U.S. Naval War College and the Center for Oceans Law and Policy, University of Virginia School of Law. I am grateful to the workshop participants for the opportunity to exchange ideas and to the co-sponsors for the opportunity to participate.

The thoughts and opinions expressed are those of the author and not necessarily of the U.S. government, the U.S. Department of the Navy or the U.S. Naval War College.

I. INTRODUCTION: THE ROLE OF NAVIES AND COAST GUARDS IN MARITIME SECURITY

As a concept maritime security may encompass, and blur demarcations between, a range of traditional threats (military or strategic) and threats from non-traditional actors.[1] Threats to national security in the maritime domain may include "terrorism, weapons proliferation, transnational crime . . . piracy, environmental/resource destruction, and illegal seaborne immigration."[2] The challenge that follows is that navies across the globe are increasingly called upon to carry our maritime security and even law enforcement roles going beyond traditional warfighting capabilities.[3] Indeed, as Till has noted, as the concept of maritime security widens, "the extent of potential overlap" between naval and coast guard activities "is increasing in ways which raise issues over who should be responsible for what."[4] Thus, in an age of maritime security, actionable law enforcement intelligence is no longer an issue for coast guards alone; it is increasingly an issue for navies as well.

There are a number of obvious virtues in maintaining distinct naval and coast guard forces: pragmatically, "lawships" need different tools and capabilities than warships, and conventional "gray painted" naval vessels are sometimes ill-suited to perform law enforcement tasks.[5] This is most apparent in the standards applied to the use of force in differing operations. In general, the military is entitled to use deadly force to overcome "the enemy," but police forces do not have "enemies" and are generally required to remain

1. Christian Bueger, *What is Maritime Security?* 53 MARINE POLICY 159 (2015); Dirk C. Sonnenberg, Maritime Law Enforcement: A Critical Capability for the Navy? 1–3 (Mar. 2012) (unpublished M.A. thesis, Naval Postgraduate School), http://calhoun.nps.edu/handle/10945/6873.

2. Sonnenberg, *supra* note 1, at 1 (quoting COMMANDANT OF THE MARINE CORPS, CHIEF OF NAVAL OPERATIONS & COMMANDANT OF THE COAST GUARD, NAVAL OPERATIONS CONCEPT 2010: IMPLEMENTING THE MARITIME STRATEGY 35 (2010), https://www.uscg.mil/history/docs/2010NOC.pdf.

3. Sonnenberg, *supra* note 1, at 5.

4. GEOFFREY TILL, SEAPOWER: A GUIDE FOR THE TWENTY-FIRST CENTURY 302 (2004).

5. Sam Bateman, *Regional Navies and Coast Guards: Striking a Balance between "Lawships" and Warships*, *in* NAVAL MODERNISATION IN SOUTH-EAST ASIA: NATURE, CAUSES AND CONSEQUENCES 245, 246–47 (Geoffrey Till & Jane Chan eds., 2014); *see also* Andrew Murdoch & Douglas Guilfoyle, *Capture and Disruption Operations: The Use of Force in Counter-Piracy off Somalia*, *in* MODERN PIRACY: LEGAL CHALLENGES AND RESPONSES 147, 167–68 (Douglas Guilfoyle ed., 2013).

within the bounds of reasonable and proportionate force in subduing suspects who are often fellow citizens.[6] There is also a difference in mindset between military and law enforcement operations, with the former typically prioritizing "disrupting or stopping the threat . . . over long-term solutions, and intelligence exploitation . . . over evidence collection and [creating] case packages."[7]

However, not every coastal State has the luxury of maintaining separate maritime services.[8] Even in the United States where there is a policy division between maritime defense and security issues (with the Department of Defense and Coast Guard as the respective lead agencies) there are areas of overlap in which certain maritime threats can be classified as both homeland defense and national security issues. This overlap may create policy challenges.[9] While the United States is perhaps unique in the impediments of law and tradition that restrict the use of naval assets in law enforcement operations,[10] there are nonetheless practical limitations that may restrict the effectiveness of, for example, European navies in conducting constabulary tasks.[11] In reality, most successful maritime law enforcement operations, irrespective of the force conducting them, require both a combination of actionable intelligence and interagency (or international) cooperation based on some degree of intelligence sharing.[12]

The need for intelligence is also a consequence of limited resources. Effective maritime law enforcement requires choices to be made about the deployment of finite assets. Even when maritime patrols are conducted in order to "randomly" intercept crimes such as human or drug smuggling, where such patrols occur is itself based on intelligence. Even the most well-resourced navies and coast guards cannot maintain a "cordon of steel" around a national coastline. There is the now well-known story of a U.S. Secretary of State, startled at the arrival of 220 maritime irregular migrants in Miami,

---

6. Nathan Alexander Sales, *Mending Walls: Information Sharing After the USA PATRIOT Act*, 88 TEXAS LAW REVIEW 1795, 1821 (2010); *see also* Håkan Friman & Jens Lindborg, *Initiating Criminal Proceedings with Military Force: Some Legal Aspects of Policing Somali Pirates by Navies*, *in* MODERN PIRACY: LEGAL CHALLENGES AND RESPONSES, *supra* note 5, at 172.

7. Sonnenberg, *supra* note 1, at 70.

8. Nong Hong, *China's Newly Formed Coast Guard and Its Implication for Regional Maritime Disputes*, 28 OCEAN YEARBOOK 611, 618 (2014).

9. Sonnenberg, *supra* note 1, at 4.

10. *Id.*

11. Friman & Lindborg, *supra* note 6; Douglas Guilfoyle, *Counter-Piracy Law Enforcement and Human Rights*, 59 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 141 (2010).

12. Sonnenberg *supra* note 1, at 52.

demanding to know: "How in the world did they get through?" The answer from the U.S. Coast Guard Commandant was, of course: "Sir, with all due respect, how did they get through what?"[13] In intercepting threats in the maritime domain, intelligence will always be crucial whether the mission is one of national defense or of law enforcement.

II. LAW ENFORCEMENT OPERATIONS AND ACTIONABLE INTELLIGENCE

A. Maritime Domain Awareness as a Form of Intelligence

The first step in considering the role of intelligence in maritime security law enforcement operations is, obviously enough, to consider what is meant by intelligence. Here, Colby's observations remain helpful:

> There are no limits to the types and sources of information which may be useful. The processing of intelligence refers to the treatment accorded the raw data which has been collected. It generally includes appraisal of the relevance of the information, as well as editing and cataloguing in forms useful to decision-makers. These tasks vary enormously in complexity, depending in large measure on the amount and quality of data requested and actually collected.[14]

One topic considered in passing in this article will be the sharing of information between intelligence and law enforcement agencies. However, while such information may—and sometimes does—play a role in real cases where maritime law enforcement action is taken, it is obviously not the only or even necessarily the best source of actionable intelligence in maritime law enforcement. A critical concept remains maritime domain awareness (MDA). The International Maritime Organization (IMO) definition of MDA is "[t]he effective understanding of any activity associated with the maritime

13. Joseph L. Nimmich & Dana A. Goward, *Maritime Domain Awareness: The Key to Maritime Security*, *in* GLOBAL LEGAL CHALLENGES: COMMAND OF THE COMMONS, STRATEGIC COMMUNICATIONS AND NATURAL DISASTERS 57 (Michael D. Carsten ed., 2007).

14. Jonathan E. Colby, *The Developing International Law on Gathering and Sharing Security Intelligence*, 1 YALE STUDIES IN WORLD PUBLIC ORDER 49, 53 (1974) (quoted in NATALIE KLEIN, MARITIME SECURITY AND THE LAW OF THE SEA 211 (2012)).

environment that could impact upon . . . security, safety, economy or [the] environment."[15]

This definition appears to draw heavily on the wording of the 2004 U.S. Maritime Security Policy directive.[16] While MDA is originally a U.S. concept, Australia, Canada, the European Union and the Philippines (among others) all have MDA policies.[17] MDA is basically about knowing who is doing what, where. A simple example is provided by Seychelles efforts to secure their exclusive economic zone (EEZ) (formidably large compared to their land territory) against piracy. By fitting all Seychellois fishing vessels with automatic identification systems, and improving radar coverage across their EEZ, the Seychellois Coast Guard was able to identify vessels in its EEZ that were *not* Seychellois fishing vessels and send one of its limited number of cutters to investigate and verify that the vessel was not a threat.[18] However, MDA is not always this simple.[19]

B. Intelligence Sharing: Problems of National Law and Agency Coordination

In the U.S. context, various impediments have made the sharing of information gathered by military or intelligence agencies with law enforcement especially challenging. Nonetheless, the basic problems relating to the use of intelligence agency products in law enforcement are relatively common to a number of jurisdictions. As Vervaele notes:

---

15. International Maritime Organization, MSC.1/Circ. 1415, Amendments to the International Aeronautical and Maritime Search and Rescue (IAMSAR) Manual 11 (May 25, 2012), http://www.mardep.gov.hk/en/msnote/pdf/msin1242anx1.pdf.

16. President George W. Bush, National Security Presidential Directive NSPD-41/Homeland Security Presidential Directive HSPD-13, at 5 (Dec. 21, 2004), https://fas.org/irp/offdocs/nspd/nspd41.pdf.

17. *See* Transport Canada, *Maritime Domain Awareness*, CANADA.CA, http://www.tc.gc.ca/eng/marinesecurity/initiatives-235.htm (last visited July 19, 2017); *Commission Communication, Towards the Integration of Maritime Surveillance: A Common Information Sharing Environment for the EU Maritime Domain*, COM (2009) 538 final (Oct. 15, 2009), http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52009DC0538&from=EN; ANGEL RABASA & PETER CHALK, NON-TRADITIONAL THREATS AND MARITIME DOMAIN AWARENESS IN THE TRI-BORDER AREA OF SOUTHEAST ASIA: THE COAST WATCH SYSTEM OF THE PHILIPPINES 21 (2012). Australia is discussed below.

18. The author observed this system on a visit to the Seychelles Coast Guard headquarters in 2011.

19. *See infra* Part III.

> That such information can be used as a lead for initiating criminal investigations is hardly contested. Much more of a problem is, however, whether this information per se is able to give rise to reasonable suspicion or form a sufficient basis for the use of coercive measures under criminal law . . . [or] can be used as legal proof in criminal proceedings.[20]

There is also the risk that if law enforcement agencies are allowed routinely to use information derived from intelligence agency surveillance (usually conducted under more permissive standards than those required of law enforcement) a situation may evolve where ordinary restraints on law enforcement surveillance are circumvented through surveillance activities being de facto "outsourced" to intelligence agencies.[21] U.S. discussion of this question has centered on the role of intelligence gathered under the Foreign Intelligence Surveillance Act (FISA). FISA prohibited direct sharing of intelligence gathered under the Act with law enforcement agencies, and required—in addition to certain statutory requirements—the permission of the Attorney General for such sharing to take place in a particular case.[22] The USA PATRIOT Act of 2001 substantially reformed the law concerning information sharing between defense, intelligence and law enforcement agencies to facilitate, *inter alia*, efforts to combat crimes of terrorism. The principal reform was a change to FISA introduced by section 218 of the Act, under which FISA investigatory powers could be used if "a significant purpose" of surveillance was the collection of foreign intelligence information (as opposed to the previous standard of "primary purpose").[23] This change was intended to more readily allow, for example, a wiretap to proceed not only if the purposes of intercepts was to "turn a suspected spy into a double agent (a classic counterespionage technique), but also to prosecute that spy for espionage (the textbook law enforcement move)."[24]

While changes to FISA may have loosened some rules-based restrictions around interagency intelligence sharing, they have not necessarily removed

---

20. John A. E. Vervaele, *Terrorism and Information Sharing between the Intelligence and Law Enforcement Communities in the US and the Netherlands: Emergency Criminal Law?*, 1 UTRECHT LAW REVIEW 1, 2 (2005).

21. Sales, *supra* note 6, at 1810–11.

22. Vervaele, *supra* note 20, at 6–7; Foreign Intelligence Surveillance Act of 1978 §§ 106, 305 (codified as amended at 50 U.S.C. §§ 1806, 1825 (2012)).

23. USA PATRIOT Act of 2001, Pub. L. No. 107-56, § 218, 115 Stat. 272 (1971) (codified at 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (2012)).

24. Sales, *supra* note 6, at 1812.

all possible firewalls. Principal remaining barriers include the National Security Act 1947, which continues to place a broad and ambiguously worded prohibition on the Central Intelligence Agency's exercising any "police, subpoena, or law enforcement powers or internal security functions,"[25] and especially the Posse Comitatus Act of 1878, which makes it an offense for anyone to use "any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws" of the United States (except as otherwise authorized by the Constitution or statute).[26] As a matter of policy, the general prohibition on law execution by military forces has been extended to the U.S. Navy, despite an express textual reference authorizing these activities in the Act.[27] As Sales notes, "it remains unclear to what extent Posse Comitatus allows law enforcement officials and military officers to share information with one another. Indeed, in part because of the Act, military brass appear to be exceedingly reluctant to share information with their colleagues in law enforcement agencies."[28]

While these are obviously U.S.-specific problems, they highlight the kind of difficulties that may and do exist in other jurisdictions, as well as where multiple government agencies have had traditionally distinct functions and legislative mandates, but that are now expected to cooperate to deliver greater maritime security. In Australia, for example, it was once estimated that, in addition to responsibility "for securing Australia's maritime approaches [being] spread widely between agencies of both [the federal Commonwealth government and the states]," that "about twelve Commonwealth agencies" have some involvement in questions of maritime security.[29] While the creation of the Australian Border Force (ABF) in 2015 might be thought to have simplified the situation (Australia's border being entirely maritime), the ABF notes that it "regularly engages with partner agencies,"[30] including the Attorney-General's Department, the Australian Antarctic Division, the Australian Communications and Media Authority, the Australian Crime

25. National Security Act of 1947, Pub. L. No. 80-523, § 102 (codified as amended at 50 U.S.C. § 3036(d)(1) (2012)).

26. Posse Comitatus Act of 1878, 18 U.S.C. § 1385 (2012).

27. Deputy Secretary of Defense, DoD Dir. 5525.5, DoD Cooperation with Civilian Law Enforcement Officials ¶ E4.3 (1986).

28. Sales, *supra* note 6, at 1824.

29. Sam Bateman, *Securing Australia's Maritime Approaches*, 3 SECURITY CHALLENGES 109, 117 (2007).

30. AUSTRALIAN GOVERNMENT, DEPARTMENT OF IMMIGRATION AND BORDER PROTECTION, AUSTRALIAN BORDER FORCE, PROTECTING OUR BORDERS, https://www.border.gov.au/australian-border-force-abf/protecting (last visited July 19, 2017).

Commission, the Australian Federal Police, the Australian Fisheries Management Authority, the Australian Maritime Safety Authority, the Australian Security Intelligence Organisation, the Australian Transaction Reports and Analysis Centre, the Department of Agriculture, the Department of Defence, the Department of Foreign Affairs and Trade, the Department of Industry and Science, the Department of Infrastructure and Regional Development, the Department of Infrastructure and Transport, Office of Transport Security, the Department of the Prime Minister and Cabinet, the Department of Environment and the Great Barrier Reef Marine Park Authority. The use of the word "including" to introduce a non-exhaustive list of eighteen partner agencies is telling as to the complexities involved.

This type and level of complexity resulted in the U.S. adoption in 2005 of the Maritime Operational Threat Response (MOTR) Plan to better coordinate the interagency response to particular maritime security operations.[31] Since that time, "the MOTR Plan has been successfully employed for hundreds of routine maritime threats and a number of low-frequency/high risk threats. These cases include drug and migrant interdiction, fisheries violations, bomb threats, radiation/nuclear alarm resolution, and piracy."[32] At least ten States have similarly adopted "whole-of-government processes to improve the interagency response to [maritime] threats" to deal with such challenges of information sharing and coordinated action.[33]

III. MARITIME DOMAIN AWARENESS AND INTERNATIONAL LAW

While MDA is a simple enough concept, delivering it in a manner consistent with international law is not free from difficulty. First, there may be questions regarding the intelligence uses to which information gathered in maritime law enforcement operations may be put. Second, States may desire information about vessels transiting off their coasts that they have no obvious

31. Brian Wilson, *Reshaping Maritime Security Cooperation: The Importance of Interagency Coordination at the National Level*, *in* MODERN PIRACY: LEGAL CHALLENGES AND RESPONSES, *supra* note 5, at 202.

32. Gary L. Tomasulo Jr., Evolution of Interagency Cooperation in the United States Government: The Maritime Operational Threat Response Plan 3 (June 2010) (unpublished M.B.A. thesis, Alfred P. Sloan School of Management, Massachusetts Institute of Technology), https://dspace.mit.edu/bitstream/handle/1721.1/59157/659552377-MIT.pdf?sequence=2.

33. Brian Wilson, *Five Maritime Security Developments That Will Resonate for a Generation*, HARVARD NATIONAL SECURITY JOURNAL (Mar. 11, 2015), http://harvardnsj.org/wp-content/uploads/2015/04/Wilson-NSJ-Artide-PDF.pdf.

power to demand under the UN Convention on the Law of the Sea (UNCLOS) absent further international cooperative mechanisms being established.[34] As a key example of the latter, in 2004 Australia declared its intention to create a 1,000 nautical mile (nm) "Maritime Information Zone" within which it proposed that any passing vessel would be "required to provide details of cargo, destination, crew, port of call, [and] likely arrival [time] at port."[35] The Australian Prime Minister was further reported as saying the Defence Force "will be able to intercept and board ships and do 'whatever it takes' to get the information they need."[36] Though clearly able to make the provision of such information a condition of entry for vessels intending to enter an Australian port,[37] Australia had no obvious authority to demand such information from vessels merely transiting within 1,000 nm, let alone intercept them using defense personnel to demand information. In addition, the Australian government declared an intention "to identify all vessels, other than day recreational boats" upon their entry to its EEZ.[38] Within months protests from Indonesia and New Zealand saw Australia rebrand its initiative the "Australian Maritime Information System" and stress that information would be sought from shipping on "a wholly voluntary basis" underpinned by "cooperative international arrangements."[39]

Unsurprisingly, Australia was already actively involved in efforts to establish a cooperative international system for greater exchange of shipping information at the IMO.[40] In 2006 after four years of work, and in an initiative largely spearheaded by the United States and the United Kingdom, the IMO Maritime Safety Committee reached agreement on a long-range identification and tracking (LRIT) system, to be implemented as Regulation 19-1 of the International Convention for the Safety of Life at Sea (SOLAS). Its

34. The following section draws substantially on research previously published. *See* Douglas Guilfoyle, *Maritime Security*, *in* LAW OF THE SEA: UNCLOS AS A LIVING TREATY 329 (Jill Barrett & Richard Barnes eds., 2016).

35. Catherine McGrath, *Government Boosts Maritime Security*, ABC (Dec. 15, 2004), http://www.abc.net.au/pm/content/2004/s1266082.htm.

36. *Id.*

37. United Nations Convention on the Law of the Sea art. 25(2), *opened for signature* Dec. 10, 1982, 1833 U.N.T.S. 397 [hereinafter UNCLOS].

38. Natalie Klein, *Legal Implications of Australia's Maritime Identification System*, 55 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 337, 337 (2006) (quoting Press Release, Prime Minister John Howard, Strengthening Offshore Maritime Security (Dec. 14, 2004)).

39. NATALIE KLEIN, MARITIME SECURITY AND THE LAW OF THE SEA 227 (2012).

40. *See, e.g.*, Australia, MSC 79/5/12, Measures to Enhance Maritime Security: Long-Range Identification and Tracking of Ships (Sept. 24, 2004), http://merchantmarine.financelaw.fju.edu.tw/data/IMO/MSC/79/MSC%2079-5-12.pdf.

implementation under SOLAS obviously has the effect of making it binding on SOLAS State parties through the tacit acceptance procedure.[41] The regulation entered into force in July 2009. The LRIT system's essential features are as follows:

- [V]essels covered by the regulation must automatically transmit every six hours the ship's identity, position (expressed in latitude and longitude) and "the date and time of the position provided;"[42]
- all covered vessels "must transmit . . . LRIT data to the data centre nominated by its flag State" and the LRIT regulations "allow flag States to receive LRIT information from ships flying their flag" wherever they are worldwide[43] and
- contracting SOLAS governments must "elect either to create a National LRIT Data Centre, or participate in a Regional or Cooperative [LRIT] Data Centre."[44]

LRIT Data Centres may request information of each other through the International Data Exchange. Using this mechanism, port States are "entitled to receive [LRIT] information about ships which have indicated their intention to enter a port facility . . . or a place under the jurisdiction of that [State], irrespective of where such ships [are] . . . provided they are not located" within another SOLAS party's internal waters.[45] Correspondingly, a coastal State is "entitled to receive [LRIT] information about ships . . . navigating within . . . 1,000 nautical miles of its coast provided such ships are not located" within another SOLAS party's internal waters.[46]

Thus, despite the skepticism with which the Australian Maritime Information Zone proposal was initially received, the final LRIT system strongly resembles what Australia had proposed. Nor was Australia alone in seeking

41. JAMES HARRISON, MAKING THE LAW OF THE SEA: A STUDY IN THE DEVELOPMENT OF INTERNATIONAL LAW 161–62 (2011).
42. International Convention for the Safety of Life at Sea ch. 5, reg. 19-1, ¶ 5.3, Nov. 1, 1974, 1184 U.N.T.S. 278 (2007 revision) [hereinafter SOLAS].
43. Chris Rahman, *Maritime Domain Awareness in Australia and New Zealand*, *in* MARITIME SECURITY: INTERNATIONAL LAW AND POLICY PERSPECTIVES FROM AUSTRALIA AND NEW ZEALAND 200, 211 (Natalie Klein, Joanna Mossop & Donald R Rothwell eds., 2010).
44. *Id.* at 210.
45. SOLAS, *supra* note 42, ch. 5, reg. 19-1, ¶ 8.1.
46. *Id.*

information about vessels transiting waters off its coasts. During IMO negotiations in 2005, the United States suggested coastal States should be able to request LRIT information about vessels within 2,000 nm of their coasts.[47] The following year, Norway suggested 1,200 nm.[48]

Nor is the LRIT system effective only on paper. After some delays in its establishment (during which time the United States provided International Data Exchange services on an interim basis), the UN Secretary-General announced in 2012 that

> the International Data Exchange for the [LRIT] system is now in operation. As at [sic] 9 March 2012, 97 out of 161 parties to the International Convention for the Safety of Life at Sea were part of the system and 66 data centres for long-range identification and tracking of ships were connected to the Exchange.[49]

Nonetheless, as an MDA tool the LRIT system is far from perfect. It contains rather "pedantic" restrictions on the ability to request information about ships present within another State party's baselines.[50] More problematically, it permits flag States to opt out entirely from providing information where requests are made on security grounds.[51] Another weakness of the system is that it applies only to passenger ships, cargo ships of at least 300 gross tons and mobile offshore drilling units.[52] It therefore does not apply to cargo ships under 300 tons nor to fishing vessels or small privately-owned recreational craft. It is precisely such small vessels that pose the greater security threat: "While safety, security, and stewardship regimes are increasingly being developed for larger vessels on the sea, many smaller vessels,

47. United States, MSC 80/3/3, Long-range Identification and Tracking of Ships ¶ 5.3 (Nov. 12, 2004).

48. Maritime Safety Committee, MSC 81/25, Report of the Maritime Safety Committee on its Eighty-First Session ¶ 5.84 (May 24, 2006). Note, however, the opposition of China to such information being sought of vessels not intending to call at a State's port. *See* Maritime Safety Committee, MSC 81/25/Add.2, Report of the Maritime Safety Committee on its Eighty-First Session annex 43 (June 1, 2006).

49. U.N. Secretary-General, *Oceans and the Law of the Sea*, ¶ 20, U.N. Doc. A/67/79/Add.1 (Aug. 31, 2012).

50. Rahman, *supra* note 43, at 211 (referring to SOLAS Regulation 19-1, ¶ 8.1.2); *see also* SOLAS, *supra* note 42, ch. 5, reg. 19-1, ¶ 8.1.4 (flag States need not provide information about their own flag vessels present in their own territorial sea).

51. SOLAS, *supra* note 42, ch. 5, reg. 19-1, ¶ 9.1; *see also* KLEIN, *supra* note 39, at 232.

52. SOLAS, *supra* note 42, ch. 5, reg. 19-1, ¶ 2.1.

including most fishing vessels, tugs, and recreational vessels, are not covered by these regimes and remain largely anonymous."[53]

As the U.S. Department of Homeland Security has noted, "Small vessels are . . . readily vulnerable to potential exploitation by terrorists, smugglers of weapons of mass destruction (WMDs), narcotics, aliens, and other contraband, and other criminals. Small vessels have also been successfully employed overseas by terrorists to deliver Waterborne Improvised Explosive Devices (WBIEDs)."[54] Further, the scale of the challenge posed by small boats is immense, as the United States alone has "nearly 13 million registered . . . recreational vessels, 82,000 fishing vessels, and 100,000 other commercial small vessels."[55] LRIT information will thus be of no use in relation to the frequent use of small boats for smuggling (especially of drugs and migrants)[56] and the increasing use of fishing vessels in transnational organized criminal activity.[57] Terrorist organizations may also use small boats in attacks on land targets, as was the case for some of the terrorists involved in the 2008 Mumbai attacks.[58]

53. COMMANDANT OF THE UNITED STATES COAST GUARD, THE U.S. COAST GUARD STRATEGY FOR MARITIME SAFETY, SECURITY, AND STEWARDSHIP 26 (2007), http://www.hsdl.org/?view&did=470382.

54. DEPARTMENT OF HOMELAND SECURITY, SMALL VESSEL SECURITY STRATEGY, at i (2008), http://www.hsdl.org/?view&did=485572.

55. *Id.*

56. *See, e.g.*, DOUGLAS GUILFOYLE, SHIPPING INTERDICTION AND THE LAW OF THE SEA 91, 194–95, 212 (2007).

57. *See generally* EVE DE CONING, UNITED NATIONS OFFICE ON DRUGS AND CRIME, TRANSNATIONAL ORGANIZED CRIME IN THE FISHING INDUSTRY (2011), http://www.unodc.org/unodc/en/human-trafficking/2011/issue-paper-transnational-organized-crime-in-the-fishing-industry.html.

58. Somini Sengupta & Keith Bradsher, *Mumbai Terrorist Siege Over, India Says*, NEW YORK TIMES (Nov. 28, 2008), http://www.nytimes.com/2008/11/29/world/asia/29mumbai.html.

IV. INTELLIGENCE COLLECTION AND VISIT, BOARD, SEARCH AND SEIZURE (VBSS) OPERATIONS

A. VBSS Operations on the High Seas

Useful law enforcement intelligence can be gathered in the course of a VBSS operation.[59] In particular, boarding a vessel suspected of one crime may reveal evidence of another crime. Thus, it was not uncommon for counter-piracy patrols off Somalia during VBSS operations to find that hidden below decks aboard suspect vessels was not a crew of pirates, but a human cargo of irregular migrants seeking to be smuggled into Yemen.[60] The frustrating result was that migrant smugglers were often let go because the counter-piracy missions lacked a mandate to deal with migrant smuggling off the African coast, even though some of the same navies were engaged in interdicting migrant smugglers in the Mediterranean.[61]

While this was ultimately a problem of mandate, not legal authority, it does raise the broader question of whether there are distinct legal limitations on what naval forces and maritime agencies can do with information gathered in the course of VBSS operations. Unsurprisingly, the issue turns on the zone in which one operates. The high seas are for present purposes the most pertinent case (though other zones are discussed briefly below).

In respect of the high seas, a controversy is provided by the extent of authority conferred under UNCLOS Article 110, which governs the conduct of VBSS operations in cases of reasonable suspicion that a vessel is engaged in piracy, the slave trade, unauthorized broadcasting or is without nationality. Such an operation is intended to be conducted in sequence. Under Article 110(3), a warship may "send a boat under the command of an officer to the suspected ship." The boarding party is to first inspect the ship's documents

---

59. For a very useful general overview of the law applicable to VBSS operations, see James Kraska, *Broken Taillight at Sea: The Peacetime International Law of Visit, Board, Search, and Seizure*, 16 OCEAN AND COASTAL LAW JOURNAL 1 (2011), http://digitalcommons.mainelaw.maine.edu/odj/vol16/iss1/2.

60. *See also* UNITED NATIONS OFFICE ON DRUGS AND CRIME, TRANSNATIONAL ORGANIZED CRIME IN EASTERN AFRICA: A THREAT ASSESSMENT 3–4, 11–15 (2013), http://www.unodc.org/documents/data-and-analysis/Studies/TOC_East_Africa_2013.pdf; INTERNATIONAL EXPERT GROUP ON PIRACY OFF THE SOMALI COAST, PIRACY OFF THE SOMALI COAST: FINAL REPORT 22 (2008), http://www.imcsnet.org/imcs/docs/somalia_piracy_intl_experts_report_consolidated.pdf.

61. *European Union Naval Force: Mediterranean Operation Sophia*, EEAS (Sept. 15, 2016), https://eeas.europa.eu/sites/eeas/files/factsheet_eunavfor_med_en_0.pdf.

to "verify the ship's right to fly its flag." Then, "[i]f suspicion remains . . . it may proceed to a further examination on board the ship, which must be carried out with all possible consideration." The question that arises is whether the information found in the course of such an "examination" is limited by the original purposes of the boarding. I shall call this question the "wider use" problem.

The conventional view is that at least some forms of wider use are prohibited.[62] The foundational text relied upon to posit this view is normally the commentaries of the International Law Commission to the 1956 draft Articles on the Law of the Sea. With regard to the equivalent provision to Article 110, the Commission stated:

> If the examination of the merchant ship's papers does not allay the suspicions [giving rise to the rights of boarding], a further examination may be made on board the ship. Such examination must in no circumstances *be used for purposes other than those which warranted stopping the vessel*. Hence the boarding party must be under the command of an officer responsible for the conduct of his men.[63]

The same point is made in the highly regarded Virginia Commentary, which tracks closely to the language used by the Commission:

> If suspicion remains after examination of the ship's papers, the boarding party may proceed to a further examination on board the ship. Such further examination is not to be used for purposes other than those which warranted stopping the ship, and is to be carried out with all possible consideration.[64]

Given that international lawyers normally take the pronouncements of the International Law Commission as authoritative, how is this limitation to be construed? Wendel suggests a potentially broad construction.[65] Consider

---

62. *See infra* notes 63 and 64.

63. *Report of the International Law Commission to the General Assembly*, 11 UN GAOR Supp. No. 9, at 284, U.N. Doc. A/3159 (1956), *reprinted in* [1956] 2 Y.B. Int'l. L. Comm'n. 284 (commentary to Artide 46) (emphasis added).

64. 3 UNITED NATIONS CONVENTION ON THE LAW OF THE SEA 1982: A COMMENTARY 245 (Myron H. Nordquist, Satya N. Nandan & Shabtai Rosenne eds., 1995).

65. PHILIPP WENDEL, STATE RESPONSIBILITY FOR INTERFERENCES WITH THE FREEDOM OF NAVIGATION IN PUBLIC INTERNATIONAL LAW 51 (2007).

the interception of a vessel that displayed no flag or identifying markings.[66] These facts could justify boarding and inspection on grounds of suspected statelessness. Wendel argues, however, that the right to verify nationality in such cases cannot justify inspection of the hold or cargo, as the only relevant material will be the vessel's papers.[67] If the papers resolve the issue, no further search should occur. This, in Wendel's view, raises questions regarding the legality of continuing to conduct a search of the hold in cases such as the *So San* incident in which a vessel suspected of conveying Scud missiles from North Korea to Yemen bore no external markings of nationality, but attempted to claim Cambodian nationality verbally.[68] Setting aside the fact that the *So San* interdiction occurred with the consent of the ostensible flag State (which had authority under international law to authorize the search),[69] Wendel's general point is not unfair. We must return, however, to the text of Article 110(2), which states that "[i]f suspicion remains after the documents have been checked, [the boarding State] may proceed to a further examination."[70] The right of "further examination" appears to be a general one. Even if narrowly construed by reference to the original suspicion, as Wendel would have it, where inadequate papers have been presented and the relevant suspicion is one of statelessness, inspection of the hold may reveal information such as a main beam number capable of assisting in the vessel's identification.[71]

To some, however, all of this is beside the point. The question at hand is not whether a VBSS operation can be conducted on a pretext (i.e., statelessness) in order to conduct a search with an ulterior motive. This would be open to an allegation of abuse of right (UNCLOS Article 300). Rather, the question is what can one do with information uncovered in the course of a legitimate VBSS operation that might be generally relevant to broader questions of maritime security, or indeed that might provide evidence of specific criminal conduct, going beyond the original suspicions giving rise to a right of boarding. I have argued elsewhere in this respect that "it is inconceivable

66. The following discussion draws on analysis in GUILFOYLE, *supra* note 56, at 327–28.
67. WENDEL, *supra* note 65, at 51.
68. GUILFOYLE, *supra* note 56, at 244–45.
69. On the authority of a "presumptive flag State" verbally claimed by the master, see *id.* at 96, 340.
70. UNCLOS, *supra* note 37, art. 110(2).
71. *Id.* at 328. One would have to concede that the introduction of uniform IMO ship identification numbers in 1987 may have reduced the necessity for hold searches.

that [Article 110] would prohibit a State from making use of knowledge of other illicit activities discovered or alerting the vessel's flag State of such."[72]

Indeed, at least one treaty concerning maritime security, the 2005 Protocol[73] to the Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation,[74] imposes such a duty on a boarding State granted flag State permission to board and inspect a vessel at sea.

The Protocol details a range of terrorism offenses, suspicion of which might justify boarding and inspection of a vessel. Generally such a boarding by a "requesting party" may only follow a request for and receipt of flag State consent, unless the flag State has waived that requirement under the treaty.[75] For VBSS operations the Protocol provides:

> When evidence of conduct [prescribed under the Protocol] is found as the result of any boarding . . . the flag State may authorize the requesting Party to detain the ship, cargo and persons on board pending receipt of disposition instructions from the flag State. The requesting Party shall promptly inform the flag State of the results of a boarding, search, and detention conducted pursuant to this article. *The requesting Party shall also promptly inform the flag State of the discovery of evidence of illegal conduct that is not subject to this Convention.*[76]

Admittedly, other than this text there seems to be relatively little positive law dealing with the question of whether wider use can be made of evidence of other illegal conduct discovered aboard. One could attempt to invoke the so-called *Lotus* presumption in support of the conclusion that wider use is permitted in order to argue that anything not expressly prohibited is, in fact, permitted. However, quite apart from the fact that current scholarship tends

---

72. Douglas Guilfoyle, *Article 110*, *in* UNITED NATIONS CONVENTION ON THE LAW OF THE SEA: A COMMENTARY 754 (Alexander Proelss ed., 2017).

73. Protocol to the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation, Nov. 1, 2005, IMO Doc. LEG/CONF.15/21 [hereinafter SUA Protocol 2005].

74. Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation, Mar. 10, 1988, 1678 U.N.T.S. 221.

75. See SUA Protocol 2005, *supra* note 73, art. 8*bis*(5)(d), (e) (setting out provisions for deemed consent after the lapse of four hours from the request in certain circumstances or complete waiver of the consent requirement).

76. *Id.* art. 8*bis*(6) (emphasis added).

to argue that this is not, in fact, what the *Lotus* case stands for,[77] attempts to argue in such terms usually end up in an unproductive cul-de-sac. The proposition, as usually stated, is too broad to be meaningfully applied and presumes international law to consist largely of prohibitions rather than positive or facilitative rules. The better question is whether there any identifiable obligations of international law that would be breached if one were to make wider use of information found during a VBSS operation. It is submitted that such obligations are in practice rather hard to find. One could attempt to argue that wider use of information discovered somehow violates the principle of exclusive jurisdiction of the flag State, but one would have to state the principle at a very high level of generality for that result to follow.

As this author has argued elsewhere,[78] the regulatory jurisdiction (i.e., prescriptive jurisdiction) is by no means completely exclusive and other States remain free to attach consequences to the actions of, for example, their nationals aboard foreign vessels on the high seas. At best, the principle of "exclusive" flag State jurisdiction confers a *prima facie* immunity from physical interference on the high seas (enforcement jurisdiction) subject to exceptions provided by UNCLOS, other treaties or flag State consent. The rule of exclusive flag State jurisdiction is thus heavily qualified, and is by its very nature derogable. This does not seem compatible with the idea that it contains by necessary inference an otherwise unstated blanket prohibition against wider use of information discovered aboard a vessel on the high seas subject to a legal VBSS operation. Indeed, one might argue that positive obligations upon States to cooperate to suppress various illicit activities at sea mitigates in favor of the sharing of information where possible. Such obligations of cooperation exist with regard to, *inter alia*, piracy,[79] maritime drug smuggling,[80] unauthorized high seas radio broadcasting,[81] the enforcement

77. *See* Hugh Handeyside, *The* Lotus *Principle in ICJ Jurisprudence: Was the Ship Ever Afloat?*, 29 MICHIGAN JOURNAL OF INTERNATIONAL LAW 71, 78–80 (2007); An Hertogen, *Letting* Lotus *Bloom*, 26 EUROPEAN JOURNAL OF INTERNATIONAL LAW 901 (2015); Douglas Guilfoyle, SS Lotus, *in* LANDMARK CASES IN PUBLIC INTERNATIONAL LAW (Cameron Miles & Eirik Bjorge eds., forthcoming 2017); OLE SPIERMANN, INTERNATIONAL LEGAL ARGUMENT IN THE PERMANENT COURT OF INTERNATIONAL JUSTICE 254 (2005); *see also id.* at 106–07.

78. Guilfoyle, *supra* note 72; *see also* GUILFOYLE, *supra* note 56, at 101.

79. UNCLOS, *supra* note 37, art. 100.

80. *Id.* art. 108(1).

81. *Id.* art. 109(1).

of internationally agreed fisheries conservation measures[82] and the prevention of migrant smuggling by sea.[83]

B. VBSS in Waters under National Jurisdiction

There are numerous good studies of the practical limitations international law may place upon VBSS operations in waters under national jurisdiction.[84] In the present article, the summary is not intended to be more than indicative of these limitations.[85]

The territorial sea of up to 12 nm is plainly a zone of sovereign jurisdiction over which coastal States have law enforcement jurisdiction, subject to innocent passage. What this means in practice has been debated. Some see innocent passage as conferring an absolute immunity from VBSS, unless "non-innocence" is made out on one of the specified grounds.[86] Others have long pointed to the ambiguity of UNCLOS and the Geneva Convention on the Territorial Sea on this point. Both conventions proclaim that a coastal State "should not" exercise criminal jurisdiction over "a foreign ship passing through the territorial sea" unless one of the categories of non-innocent passage are made out.[87] However, *should not* is generally exhortatory language to be contrasted with a mandatory *shall not*. Churchill and Lowe see the provision as codifying usage: coastal States ordinarily restricted any exercise of enforcement jurisdiction within territorial waters to a limited and generally

---

82. *Id.* art. 20(1). *See also* Agreement for the Implementation of the Provisions of the United Nations Convention on the Law of the Sea of 10 December 1982 relating to the Conservation and Management of Straddling Fish Stocks and Highly Migratory Fish Stocks, *opened for signature* Dec. 4, 1995, 2167 U.N.T.S. 3.

83. Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime art. 7, *opened for signature* Nov. 15, 2000, 2241 U.N.T.S. 507.

84. *See especially* Kraska, *supra* note 59.

85. Ships bound inward to port pose few jurisdictional problems, as conditions of entry to port may be imposed and enforced, induding submitting to inspection or providing information ahead of arrival. This analysis concerns vessels that do not enter a port of the coastal State.

86. Namely, under Artide 21(1) of UNCLOS:

> (a) [I]f the consequences of the crime extend to the coastal State; (b) if the crime is of a kind to disturb the peace of the country or the good order of the territorial sea; (c) if the assistance of the local authorities has been requested by the master of the ship . . .; or (d) if . . . necessary for the suppression of illicit traffic in narcotic drugs or psychotropic substances.

UNCLOS, *supra* note 37, art. 21(1).

87. *Id.*, art. 27; Convention on the Territorial Sea and the Contiguous Zone art. 19, Apr. 29, 1958, 15 U.S.T. 1606, 516 U.N.T.S. 205.

accepted set of grounds.[88] Views differed as to whether that practice evidenced a restriction on powers of enforcement in the territorial sea (i.e., a limitation upon sovereignty) or simply evidenced comity (i.e., plenary sovereignty, usually exercised with restraint).[89] The debate is far from resolved, but the only clear prohibitions on law enforcement in the territorial sea concern sovereign immune vessels and crimes "committed before the ship entered the territorial sea" where the vessel in question is simply passing through the territorial sea without entering internal waters.[90]

Conversely, the extent of law enforcement power in the contiguous zone may provide less authority than commonly thought to conduct VBSS operations. Within a contiguous zone (extending up to a further 12 nm seaward from the territorial sea), "states have limited powers" under UNCLOS Article 33 to enforce "customs, fiscal, sanitary and immigration laws."[91] UNCLOS allows coastal States only to exercise "control" (not sovereignty or jurisdiction) either to prevent infringement of the specified laws within the State's territory or territorial sea or to punish acts already committed within its territory or territorial sea.[92] Shearer argues that the connotations of control limit preventive enforcement action to "inspections and warnings," rather than arresting vessels.[93] Some authorities, and in particular U.S. commentators, treat Article 33 as allowing plenary criminal law enforcement for violations of the specified subject matters up to the outer limit of the zone.[94]

This approach fails to give separate meanings to "prevent" and "punish." The power to "punish" is conditioned upon criminal acts having occurred within a State's territory or territorial sea.[95] By analogy with the doctrine of hot pursuit, this appears to be an express extension of an otherwise impermissible jurisdiction. The condition limiting the exercise of jurisdiction to

88. R. R. CHURCHILL & A. V. LOWE, THE LAW OF THE SEA 95–99 (3d ed. 1999).
89. *Id.*
90. UNCLOS, *supra* note 37, arts. 27(5), 30–33. On the challenge of sovereign immune vessels that violate coastal State law in the territorial sea, see James Kraska, *Putting Your Head in the Tiger's Mouth: Submarine Espionage in Territorial Waters*, 54 COLUMBIA JOURNAL OF TRANSNATIONAL LAW 164 (2015).
91. Ivan Shearer, *Problems of Jurisdiction and Law Enforcement against Delinquent Vessels*, 35 INTERNATIONAL AND COMPARATIVE LAW QUARTERLY 320, 330 (1986).
92. *Id.*
93. *Id.*
94. *See, e.g.*, 2 RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW 30, 49 (AM. LAW INST. 1987); J. ASHLEY ROACH & ROBERT W. SMITH, UNITED STATES RESPONSES TO EXCESSIVE MARITIME CLAIMS 481 (2d ed. 1996).
95. UNCLOS, *supra* note 37, art. 33(1)(b).

"punish" would be redundant if relevant criminal laws were continuously enforceable up to the outer limit of the zone. The claim, for example, that "if the U.S. Intelligence Community levies terrorism threat reporting [i.e., the vessel is allegedly carrying terrorism-related material or personnel] against a ship anywhere within 24 nautical miles of the United States coast, it would be subject to United States jurisdiction"[96] is absurd unless the facts of the case disclose a close link to a customs or immigration violation that has actually occurred. If such a violation is merely threatened, permissible measures may be constrained to visit and inspection.

Finally, in the 200 nm EEZ, coastal States enjoy a limited bundle of sovereign rights and subject matter jurisdiction. They have "sovereign rights for the purpose of exploring and exploiting, conserving and managing the natural resources, whether living or non-living . . . and with regard to other activities for the economic exploitation and exploration of the zone."[97] Under this jurisdiction, the coastal State may also conduct activities pertaining to "artificial islands, installations and structures," marine scientific research and "the protection and preservation of the marine environment."[98] In exercising its sovereign rights the coastal State may "take such measures, including boarding, inspection, arrest and judicial proceedings" as are necessary to enforce its laws with respect to those rights.[99] Curiously, there are no express enforcement provisions in UNCLOS regarding "artificial structures and marine scientific research,"[100] but it is not questioned that, for example, a State's criminal law may in principle extend to vessels that violate laws applicable in a safety zone around an artificial structure.[101] In protecting the marine environment, the coastal State enjoys power to regulate dumping under Article 211(5), to conduct boarding and inspection of vessels causing or threatening "significant pollution of the marine environment" and to arrest and institute proceedings against vessels in pollution incidents that on "clear objective evidence" have caused "major damage or threat of major damage" under Articles 220(5) and 220(6).[102]

---

96. Thomas M. Brown, *For the "Round and Top of Sovereignty": Boarding Foreign Vessels at Sea on Terror-Related Intelligence Tips*, 59 NAVAL LAW REVIEW 63, 77 (2010).
97. UNCLOS, *supra* note 37, art. 56(1)(a).
98. *Id.* art 56(1)(b).
99. *Id.* art. 73(1).
100. Shearer, *supra* note 91, at 335.
101. *See, e.g.*, Arctic Sunrise (Neth. v. Russ.), Case No 2014-02, Award on Jurisdiction (Perm. Ct. Arb. 2014), http://www.pcacases.com/web/view/21.
102. Such jurisdiction being concurrent with that of the flag State. *See also* Shearer, *supra* note 91, at 335.

As regards both the contiguous zone and EEZ, it would be an abuse of right to use such a power of inspection *intentionally* to gain intelligence not related to the subject matters over which rights or jurisdiction have been granted to a coastal State; however, wider use of any information discovered in the course of such a boarding should be permitted for the reasons discussed above in relation to the high seas. Thus, it is hard to see what significant restrictions international law might place upon the use a coastal State could make of law enforcement intelligence gleaned through a lawful VBSS operation in waters under national jurisdiction. One question might be whether VBSS operations can be conducted in international straits subject to the regime of transit passage, under which vessels enjoying such a right "shall not be impeded."[103] There is, however, not space to consider this point further in the present article.[104]

V. PRACTICAL MEASURES

What, practically speaking, follows from this analysis? Some observations are straightforward. If the aim of many maritime security operations is a successful prosecution, then navies and other maritime security agencies must be trained in more than basic boarding and inspection techniques. As Sonnenberg notes: "The ability to conduct inquiries, proper searches, and intelligence collection is just as important [as tactical techniques and procedures], if not more so, because they are the core tasks of a boarding that will determine the outcome."[105] Indeed, one U.S. study has concluded that "the lack of specialized training for VBSS missions is a major deficiency in maritime security operations."[106] The mission needs to determine the capabilities that are required, rather than agency capabilities driving the types of mission that are undertaken. And, as Tomasulo notes, maritime threat response cases may be "planned" or "unplanned."

> Planned responses originate as a result of actionable intelligence. A planned response provides time for the various [stakeholder] U.S. Government agencies . . . to deliberate and select the appropriate mix of resources to achieve the desired outcome in response to a particular threat. The type of

103. UNCLOS, *supra* note 37, art. 38(1).
104. See Shearer, *supra* note 91, at 331–32, for a consideration of this issue.
105. Sonnenberg, *supra* note 1, at 71.
106. *Id.* at 71–72.

> capability employed is based on the level of the threat and the desired outcome.[107]

The threat that will be represented by "an armed terrorist on a vessel that is expected to be non-compliant" may require Navy SEALs.[108] However, if the desired outcome involves "criminal prosecution," then coast guard specialized boarding teams will need to be involved. Some cases may require a mix of capabilities.[109] Thus, it is increasingly important for navies, as well as civilian maritime agencies, to have some appreciation of law enforcement skills, to include minimal use of force in order to reduce disruption to society; the knowledge and ability to conduct effective and legal searches, to piece together case packages and to understand the difference between evidence and intelligence.[110]

The issue becomes only more acute in multinational maritime security operations, such as counter-narcotics and counter-piracy operations, where the prosecuting State may not be the same entity as the boarding State. In the counter-piracy context, it has been noted that "law enforcement agents are generally trained to collect and preserve evidence in accordance with their own criminal procedure requirements. But what is good evidence for a Dutch court may not necessarily be good evidence for a Kenyan court."[111]

Indeed, evidentiary issues can present challenges throughout multilateral operations. For example, the value of otherwise actionable evidence may be lost, not because it is somehow considered tainted, but, due to "the formal requirements of admissibility" in a given legal system.[112] Thus, while Kenya has been willing since 2006 to conduct numerous trials of Somali piracy suspects captured by foreign navies patrolling the Gulf of Aden, its courts faced difficulties in accepting "the admissibility of photographs that were taken by a person not previously authorised by the Attorney-General."[113] In the end, international cooperation required "substantive changes in laws or policy"

---

107. Tomasulo, *supra* note 32, at 34.
108. *Id.*
109. *Id.*
110. Sonnenberg, *supra* note 1, at 124.
111. Rob McLaughlin & Tamsin Phillipa Paige, *The Role Of Information Sharing In Counter-Piracy In The Horn Of Africa Region: A Model For Transnational Criminal Enforcement Operations*, 12 JOURNAL OF INTERNATIONAL LAW AND INTERNATIONAL RELATIONS 82, 92 (2016).
112. *Id.*
113. *Id.*

by a number of States conducting either counter-piracy patrols or trials of captured piracy suspects.[114]

VI. CONCLUSION

This article explored the question of intelligence collection and distribution to support maritime law enforcement operations in the context of modern concerns about maritime security more broadly. This line of inquiry required consideration of intelligence gathering and intelligence sharing/coordinated action in each of two dimensions. Relevant intelligence for law enforcement may consist either of general awareness of the maritime domain or to specific evidence supporting a criminal prosecution. That is, the deployment of finite law enforcement assets requires knowledge of which vessels are engaged in what activities, and where they are located. Regarding the second dimension of law enforcement intelligence gathering, as navies are increasingly involved in maritime security operations that may shade over into law enforcement, greater training and coordination may be required such that naval personnel can act to support law enforcement operations without compromising the collection of admissible evidence.

This issue raises the question of coordinated action and sharing intelligence either between agencies or between governments. Irrespective of which coastal State is being discussed, maritime security operations will require the coordination of a variety of government departments and agencies. Thus, there will be significant questions of horizontal coordination within any government conducting maritime security or law enforcement operations. Additionally, there may be significant questions of coordination between partner States engaged in suppression of such activities as drug smuggling or piracy.

A number of relevant legal questions arising have been considered. The least legally complex question, though perhaps one of the more practically complex, is the interface between partner States in handing over admissible evidence packages from an interdicting or boarding State to prosecuting authorities in a different State. While a certain amount of practical training and coordination may assist in such cases, in some there will simply be no alternative to revisions to domestic legislation if successful prosecutions are to occur. Similar challenges may arise within a coastal State if navies become involved in maritime law enforcement.

---

114. *Id.*

A number of the legal difficulties in achieving maritime domain awareness have also been discussed. While the IMO's LRIT regulation achieves a greater degree of coordinated information sharing among flag States and coastal States that could support the achievement of better MDA, significant gaps in the LRIT regime remain, especially as regards small craft. Such gaps may not be entirely possible to close at the level of national action either. As with any intelligence exercise, while one can seek better information, perfect information is simply not possible.

Finally, some attention has been given to the specific legal question of what can be done with intelligence gathered in the course of a VBSS operation conducted for one purpose, but which results in evidence of an unrelated crime being uncovered. Can such evidence be retained and used for other purposes by the boarding State or shared with other States, including the flag State? I have referred to this as the question of "wider use." Commentators tend to suggest that VBSS may only be conducted for quite limited purposes, and the action taken must not exceed what the original suspicion giving rise to the right of boarding would require. Even if one takes so narrow a view, the conclusion suggested here is that nothing in the law of the sea prohibits wider use being made of evidence uncovered of crimes other than that of which the vessel was originally suspected. Indeed, coming to a contrary conclusion could undermine various duties upon States to cooperate in the suppression of maritime crime. The only relevant limitation would be that deliberately boarding and searching a vessel under color of a suspicion not actually held with the purpose of gathering information about unrelated offenses would likely constitute an abuse of right.