Intelligence and Avoidance of Capture by Pirates off the Coast of Somalia

Nis Leerskov Mathiesen

Introduction

Every day, merchant vessels are able to avoid pirate threats due to a mesh of intelligence support. But civil-state intelligence cooperation needs to evolve if avoidance is to play a larger role compared to deterring or defending against an attack on a merchant vessel.

Since the beginning of 2011, privately contracted armed security personnel (or PCASP) have become the counter-piracy measure of choice for many shipping companies. Although they come with a substantial cost, the use of PCASP has demonstrated their value in deterring and defending against pirates. As a popular saying goes 'No ship with armed guards has been taken by pirates.' Whether this claim will endure or not, defence against pirates is nonetheless most effectively done in a layered fashion. Considering avoidance, detection and deterrence of pirates is part of all structured risk assessment-based planning.

In a layered and defensive mode of thinking avoidance of pirate attack is one of the first steps to take. The most extreme measure of this is to reroute ships, where possible, from Europe south of Africa to Asia to avoid the Arabian Sea. On a smaller scale, however, it is also done on an everyday basis, as vessels steer clear of known pirate hotspots. The key to effective avoidance is intelligence. There is already an impressive multitude of agencies and companies that work in supplying intelligence on Somali pirates. But despite – or perhaps due to – this multitude there are several issues standing in the way of using the full potential of intelligence for active risk avoidance. It will be pointed out below what shortcomings the current system has and possible ways to improve the situation.

On the face of it, the counter-piracy operation off Somalia is one of the most advanced cooperative military undertakings across traditional coalition lines and national interests. At the

US-led Shared Awareness and Deconfliction (SHADE) meetings the EU, Russia, China, Japan and several smaller countries plus private industry associations as well as UN organizations orchestrate an overlapping or shared effort to protect a common interest. This has received praise and admiration from many commentators - and rightly so. But looking at the intelligence side of things, the more competitive and suspicious undercurrent of national interest is dominant. This is not surprising as intelligence systems and sharing has always been one of the most closely guarded systems in a military organization.

Types of Intelligence

The intelligence that is interesting for merchant shipping is mainly to be found on the tactical and the operational level. Tactical intelligence pertains to pirate attack groups: Where are they, how many are they, how do they operate? Tactical intelligence mainly stems from surveillance, reconnaissance and encounters with pirates at sea. This means that both navies and merchant vessels are gathering information for their tactical intelligence.

Operational intelligence can be viewed as the information about region-wide developments that might have an influence on the tactical side of things: Which pirate groups are active, who are the leaders and investors, how do they organise and operate this pirate season? This type of intelligence is not directly applicable on the bridge of a merchant vessel or in the shipping company, but is still shaping the operating environment. Operational intelligence can be obtained through traditional intelligence means such as human sources, image intelligence and signals intercepts but also in a good old fashion by talking to people and reading open sources. This means that government intelligence agencies as well as private intelligence companies, journalists, ordinary citizens, Internet users and NGOs gather information that can be processed into operational intelligence.

Strategic intelligence about the Somali situation – such as the political wrangling or the general forecast of the country's direction – is influencing the operational level and strategic intelligence shares some traits with the above but will not be treated here.

Current Situation

For a long time the United Kingdom Maritime Trade Operations (UKMTO) has been the mainstay of aggregating, analysing and disseminating tactical intelligence for the purpose of avoidance. This was initially done on a limited budget by a small but dedicated staff in a small apartment in Dubai. More recently, UKMTO has been up-scaled, but considering their centrality in the intelligence cooperation, the operation is still doing a large amount of work with a very limited staff. UKMTO is the main contact point for mariners under attack and does get some of the most high-grade information, including pictures and descriptions, directly from merchant vessels. They are also a central node in the MERCURY chat system. UKMTO disseminates intelligence for avoidance directly to ships in the area and a broad selection of partners, but does not aim to keep public record of incidents. Since piracy became an issue with international attention, NATO and EU have started operating military operations in the area. Both organizations have also set up civil-military liaison bodies that supplement and overlap some of UKMTO's services.

UKMTO, however, will not receive nor disseminate all intelligence. There is a tendency that intelligence collected by military aircraft, ships and other means is kept within a national or coalition system, like NATO's CENTRIX. Some of this is shared on a need-to-know basis with UKMTO, but some is also released more unilaterally.A good example is processed analysis and forecasts on NATO Shipping Centre's homepage or from the US Office of Naval Intelligence. A good deal of this intelligence is, however, kept out of public sight. This is in keeping with the systems that collect and disseminate, which are designed for wartime naval battles.

There are some important non-governmental providers of tactical intelligence as well. The International Maritime Bureau (IMB) has a global role as a piracy reporting centre. They sit more removed from the military sources but will get certain types of reports from merchant vessels that have not previously been sent to UKMTO. More importantly, IMB acts as librarian of incidents, producing a public overview of all incidents that have been reported to them. Between UKMTO and IMB, most of the incidents that are reported by vessels or companies off

Somalia will be gathered up. Beyond these, however, there are still a number of incidents that go unreported. Some shipping companies are not interested in getting their name associated with a case. This also seems to be the case with some armed security providers, who are sometimes put in charge of reporting incidents for vessels. Word or reports of these and other unreported incidents, however, might filter out through small regional media outlets, word of mouth – or they will simply never get beyond the vessel involved.

Main Problems

To sum up the situation off the Horn of Africa, there is a lot of information and intelligence about pirates that can be used for avoidance. But in the current environment, problems arise in the assessment, analysis and dissemination of intelligence.

Assessing incoming reports is an important part of the counter-piracy cycle. As useful as it is for a Master to know that a ship 100 nautical miles up ahead has just been attacked, it is disruptive to have harmless sightings of fishermen or smugglers reported in multitude. Piracy in itself is a small-scale, criminal event and thus it can be difficult to point it out short of when a ship is boarded. The vetting of incidents is the most effective the closer to the collecting source it is. The intelligence nodes in the military systems should, however, be the backstop. This is not always the case, unfortunately, as most military personnel rotate in and out of jobs. So even vital command posts like that of UKMTO are rarely granted for more than six months. This also means that the "corporate knowledge" is worn thinner than necessary. Given that most navies active in the area have now been there for a long time, the problem lessens somewhat, but military systems should consider changing placement policies.

Analysing the piracy threat for avoidance purposes is one of the tasks that require experience and "staying power". To this comes gathering and analysing operational intelligence to understand the trends. It is striking that none of the organizations dealing with tactical intelligence has a significant capacity to gather, analyse and present operational-level intelligence in the context of avoidance. The reason for this is again a historical one, as most of the capacities needed for understanding a criminal organization on shore traditionally rest with a country's security or

criminal intelligence agency, not with navies. Operational intelligence is analysed by international and national agencies today, but there is an obvious gap when Masters and companies have to relate this to the day-to-day tactical intelligence. Fusing the sources consistently on a day-to-day basis would be helpful to spread a fuller understanding of the problem.

Lastly, dissemination of collected data and finished intelligence products is likely the largest problem. This is to some extent a technical issue as has been pointed out by many observers, including NATO's own Joint Analysis and Lessons Learned Centre. But the real stumbling block is a conceptual one. As mentioned above, military intelligence systems are designed for wartime use and emphasise compartmentalization, classification and operational security – all of this for good reasons. But in the Somali piracy context, these parameters become destructive when it comes to tactical intelligence for avoidance purposes. As an example, there are several instances where a picture or a location of a known pirate group could not be shared immediately to a nearby naval ship because the vessel was from another country or coalition. The problem of sharing is aggravated when intelligence needs to cross the governmental-commercial divide. Although most intelligence organizations and navies in the area have established close contacts to industry bodies, individual shipping companies and private intelligence companies by now, there is still a culture of classification that keeps much vital and non-compromising intelligence out of the hands of those who have the most immediate need. Obviously, intelligence should not fall in the wrong hands, but weighing the benefits against the disadvantages on the short and long term, intelligence should be shared more readily. In the current situation, shipping companies and private intelligence companies have become producers as well as consumers of intelligence, so for intelligence agencies and navies a more open culture of sharing would likely benefit these organizations themselves.

Conclusion

Avoidance of known pirate attack groups is the best method for merchant shipping when trying to mitigate the risk of piracy. The current environment for actionable tactical intelligence is in

itself promising, with a historical high degree of cooperation across traditional state divides as well as between governments and commercial actors. But the system is less than perfect. Owing to traditions and structures designed for a wartime setting, intelligence agencies and navies tend to keep information and intelligence that could otherwise be put to good use, in their closed systems. Given that Somali piracy is not a threat to national security as such for most countries, a conscious revision of intelligence procedures would be a worthwhile endeavour that could even benefit the individual country in the end.

*This article was commissioned by the Institute for Near East and Gulf Military Analysis (INEGMA) on behalf of the second United Arab Emirates Counter Piracy Conference, '**A Regional Response to Maritime Piracy: Enhancing Public-Private Partnerships and Strengthening Global Engagement'**, organized by the UAE Ministry of Foreign Affairs in partnership with global ports operator DP World, held in Dubai in June 2012. The opinions expressed in this paper are the views of the author only, and do not reflect the opinions or positions of the conference organizers. Content may have been edited for formatting purposes.*

For more information, see the conference website at www.counterpiracy.ae.