



**Dr. Kendra E. Moore**  
**Program Manager**  
**Information Exploitation Office**

## Pirates, Patterns, and Other Passions

Pirates, smugglers, and slave traders—sounds like something from the past. Unfortunately, they are with us today and they are conducting business on the high seas.

Modern day pirates are operating in the Straits of Malacca, the South China Sea, off the coast of Indonesia and West Africa, and in many other places around the world. With smugglers and slave traders, these characters are not the tender hearted pirates of Penzance nor the dashing pirates of the Caribbean.

On October 22, 1999, the *Alondra Rainbow* left the port of Kuala Tanjung, on the east coast Indonesia, bound for Japan with \$10 million worth of aluminum ingots. Less than 3 hours later, while the captain was drafting his departure message to the ship's owners, the *Alondra Rainbow* was hijacked. That message was never sent. A week after the hijacking, when the *Alondra Rainbow* failed to arrive in Japan, its owners reported it missing. By that time, the ship had been repainted and renamed, twice, and was nowhere to be found. The crew was held hostage for a week, then cast adrift in a life

raft until they were rescued 11 days later.

Eventually, nearly a month after it was hijacked, the vessel was spotted and chased down by the Indian Navy while making a run for Pakistani waters. The *Alondra Rainbow* had gone the opposite direction from the search. It had become a ghost ship, fading into the fog of war.

On March 26, 2003, pirates armed with machine guns and machetes, and carrying VHF radios, hijacked the *Dewi Madrim*, a chemical tanker, off the coast of Sumatra. The pirates disabled the ship's communications systems and steered the ship for about an hour, then left taking

the captain and first officer with them. One theory is that these hijackers were terrorists on a training mission, and they never ransomed their hostages because they were looking to gain the expertise necessary to pilot a ship.

What do pirate stories have to do with patterns? Both the *Alondra Rainbow* and *Dewi Madrim* had normal operating patterns that were disrupted by these piracy events.



Pirates hijack vessels, steal cargo, violate embargos, and run blockades. They kidnap and ransom crews or throw them overboard. With smugglers and other ne'er-do-wells, they are a serious and direct threat to maritime commerce. Their activities provide a means of raising funds for criminal and terrorist organizations and can potentially provide a vehicle for terrorist activity.

## Pirates, Patterns, and Other Passions

The *Alondra Rainbow* typically plied the seas from Malaysia to Japan. It didn't usually venture into the Indian Ocean. The captain usually sent a departure message within a few hours of leaving port. On its fateful voyage, it failed to send this message. If someone had known those patterns and realized the *Alondra Rainbow* was not following them, the alert could have been raised sooner, perhaps within a couple hours of being hijacked. Likewise for the *Dewi Madrim*.

Patterns are all around us. They can be explicit (the letter carrier's route) or implicit (you go to the grocery store when you run out of milk). They can be short lived or long lived. They can evolve slowly over time or change suddenly, disappearing only to be replaced by a new pattern. Establishing and following patterns is logical, sensible, and comfortable. Most of you have the same routine every morning and drive the same route to work every day.

Commercial maritime ships follow patterns because it makes sense to do so. They are in the business of making money, and the margins are very slim. Commercial maritime ships follow motion-based patterns. If you think of a single voyage as consisting of a sequence of events (e.g., leaving port, transiting a straight or other choke point, crossing the open ocean, and entering a harbor), you can identify movement and other activity patterns that correlate with these events. If a ship deviates from those patterns, there should be a good business reason for doing so. If there isn't, it is likely the ship is up to no good.

Why does DARPA, indeed, the military, care about pirates? For the same reasons we care about airplanes being hijacked and for the same reasons we care about anything that can disrupt free trade and economic security. A hijacked ship could be sunk to block a choke point or could be used to attack a Naval battle group. Commercial maritime vessels can be used for any number of illicit purposes, including transporting arms, weapons of mass destruction, illegal immigrants, or terrorists.

We should learn the patterns of all the vessels engaged in international maritime commerce. We should learn their normal behavior patterns and use those patterns to detect unusual or anomalous behavior.

What do we know about patterns in the maritime domain? To be honest, not much. We don't know much because, until recently, there was no way to track large numbers of vessels. And, even if we could, we haven't had the technology to learn what is normal for those vessels.

Today, there is a list of 100 to 200 high-interest vessels. They are ships suspected or known to be affiliated with some bad activity, person, or organization, or that carry cargoes that could be dangerous in the hands of the wrong people. In fusion centers around the world, watchstanders and analysts are busy manually tracking and assessing these high-interest vessels. They look for inconsistencies in what those ships say they are doing by comparing it to what they said an hour or a day ago, or by determining if it is feasible for the vessel to arrive at its destination port when it plans. These simple comparisons involve multiple database queries and manual comparison of the returned data. As a result, today's watchstander, who should be closely monitoring more than 100 vessels is lucky to be able to monitor 5.

DARPA is helping to automate this process by providing a set of rapidly configurable and secure software agents to perform data collection and consistency checking, alerting the watchstander to evolving inconsistencies. This effort will result in a factor of 20 performance improvement, allowing a watchstander to monitor over 100 vessels, and focus his or her efforts on analysis, rather than writing SQL queries. The first software drop will occur at the 6<sup>th</sup> Fleet's Theater Maritime Fusion Center in Naples, Italy, later this month. Although this software will provide an order of magnitude improvement and demonstrate the utility of DARPA's agent technologies in an operational setting, it is not enough.

## Pirates, Patterns, and Other Passions

We can and should do more. The International Maritime Organization (IMO) mandates that all ships above a certain size carry an automatic identification system (AIS), which broadcasts information about the vessel. Many ports now require vessels provide advance arrival notice and other information. With the availability of this new data, for the first time it is feasible to develop and maintain long duration tracks on these vessels. Given that we have these tracks, we now have the data we need to learn the normal behavior of these ships.

The Predictive Analysis for Naval Deployment Activities program (PANDA) will provide the logical revolution in predictive analytic support for monitoring maritime surface traffic. PANDA's goal is to develop technology that will learn normal patterns of behavior from all-source track data and leverage those patterns to detect anomalous behavior. PANDA will learn both individual and class vessel models. It will store, update, and manage those models. PANDA will continuously and rapidly learn these models, on as few as a two to six exemplars.

There is a lot of anomalous behavior in the shipping industry, but those anomalies should have some business purpose. For instance, an oil tanker that has gone between two ports for the past 5 years may suddenly go to a new port. Chances are the lease on that tanker has expired, it is now being leased by another company, and it is traveling between the new company's crude oil depot and its refinery. In another case, a vessel may make a trip to a completely new port, merely to take advantage of a significant change in a spot market.

Clearly, we cannot introduce a system that generates hundreds of anomalies. PANDA will incorporate sophisticated anomaly resolution and alert-handling technologies, including the ability to learn and use business rules to update the pattern models. Finally, there will be a mix of data available for analysis. There will be areas of the world where we have very dense data feeds and

areas where the data is sparse. PANDA will incorporate both local learning and global learning and exchange the models and tracks across areas of responsibility and between local and global levels.

To achieve this vision, PANDA will require advanced machine learning technologies; flexible and expandable context modeling and representation techniques; distributed learning, processing, and control technologies; and advanced anomaly handling and alert processing. PANDA will be a distributed system, with nodes at multiple levels, ranging from shipboard nodes to intel processing centers. It will be implemented in a services-oriented architecture, consistent with current acquisition plans. We will conduct annual evaluations and continuous spiral experimentation. We expect to release the PANDA BAA in the coming weeks.

Learning patterns from complex spatiotemporal data requires passion. The multisource track data associated with maritime surface traffic is one set of complex spatiotemporal data. There are other problems and data sets where patterns are important. As our overall detection and tracking capabilities improve and we achieve IXO's goal of persistent surveillance and tracking, we want to exploit that data to learn patterns. We want to exploit that data to learn the enemy's normal operating modes and detect when they change modes. We want to exploit that data to determine when a specific target—be it a traditional military threat, an insurgent, or a suspected terrorist—is being deployed in a new way.

A possibility is to use the data we collect from sensors on our own Forces, on both vehicles and Soldiers, to learn our Forces' normal patterns of movement through different terrains and use the knowledge of those patterns to detect when they run into a problem.

For instance, if we can learn a periodic patrol's normal movement down a road or through a town, we can automatically detect when they encounter

## Pirates, Patterns, and Other Passions

insurgents and scramble backup right away, thereby maximizing the effectiveness of our Forces.

Beyond that, we want to automatically learn and detect models of interactions and workflows about our enemies. We want to exploit multisource data, be it from human intelligence, imagery, or any other source. Ultimately, we want to automatically construct executable and analyzable models of these interactions so we can learn our adversaries' normal behavior and leverage that information to

determine their weaknesses, detect when they change operating patterns, and rapidly learn the new operating pattern. All this requires advances in information extraction, machine learning, modeling languages, the ability to automatically construct and control models, context modeling and understanding, and information presentation. We invite you to bring us your problems that require modeling and pattern analysis, and your ideas for solving these problems.