NMIO Technical Bulletin

National Maritime Intelligence-Integration Office

JULY 2014 - VOL 7

Director NMIO View:

Rear Admiral Elizabeth L. Train, USN

As the Director of the National Maritime Intelligence-Integration Office (NMIO), I am pleased to present Volume 7 of NMIO's Technical Bulletin. As reflected in Presidential Policy Directive 18, "Maritime Security," NMIO is designated by the Director of National Intelligence as a U.S. Intelligence Community Service of Common Concern, providing and facilitating maritime intelligence integration and Maritime Domain Awareness (MDA) information sharing for operational use by various Federal maritime stakeholder departments and agencies. NMIO continues to be the unifying maritime voice for the U.S. Intelligence Community.

Volume 7 of the NMIO Technical Bulletin is the product of a study team at the Naval Postgraduate School, Monterey, California. The team identified and assessed emerging technologies that may impact maritime domain security with a focus on advances in technology that inspire and foster innovations that may prove useful in either attacking or defending targets in the maritime domain.

I would like to personally thank the authors who have invested their valuable time to contribute to this edition of the Technical Bulletin, sharing their insightful knowledge and perceptions of the impact of emerging technologies on the maritime domain. As we work together to promote global maritime security, I encourage others to become more involved in this community publication by submitting articles to help us broaden the topics and regions covered in this product.

I am equally grateful to our readers. Your insights, commitment, and feedback continue to positively affect the safety of the international maritime domain. It is my hope that through increased awareness and collaboration our mutual efforts will strengthen the governance of the global maritime commons. NMIO is focused on identifying concerns and issues that resonate among government, academic, industry, and foreign partners, and remains dedicated to collaborating with global stakeholders to identify the most efficient and cost effective solutions to our mutual maritime challenges.

The Technical Bulletin is one of our key vehicles to promote enhanced MDA and information sharing. We appreciate and invite your continued input, interaction, and contributions to this and other efforts that promote this shared mission. We hope you enjoy this publication, and I look forward to working with you to advance maritime security and build shared domain awareness.

NMIO Technical Bulletin **Volume 7, July 2014**
Editor In Chief: Dr. Paul Shapiro, Chief Science and Technology Advisor, NMIO
Phone: 301-669-2269 or 301-669-3400
Email: pshapiro@nmic.navy.mil
Chief, Strategic Engagement, NMIO: Mr. Brian F. Eggleston
Phone: 301-669-3830
Email: beggleston@nmic.navy.mil
Production: ONI Media Services
Address: 4251 Suitland Road
Washington DC 20395

Correspondence : Dr. Paul Shapiro
Contributions welcome: We welcome contributions from all Global Maritime Community of Interest stakeholders, both domestic and international. In submitting your article, please highlight who you are, what you are doing, why you are doing it, and the potential impacts of your work. Please limit your article to approximately one to two pages including graphics.
Cover image: Deployment of a communication platform as part of a major oceanographic field experiment. U.S. Navy Photo by Javier Chagoya

Table of Contents

Introduction

The National Strategy for Maritime Security provides that the safety, security, economy, and environment of the United States is a vital concern. Therefore, a study team at the Naval Postgraduate School, Monterey, California, at the request of the National Maritime Intelligence Integration Office (NMIO), identified and assessed emerging technologies that may impact maritime domain security. The “technical scan” focused on advances in technology that inspire and foster innovations that in some cases may present a potential threat and in other cases prove useful to defend targets from various or specific threats in the maritime domain. The destruction or degradation of high value targets causes high loss of life and severe economic consequences. Ultimately, the goal is to identify the likelihood and consequences of an attack in the maritime domain.

Five assessments from the study have been included in this technical bulletin spanning a broad range of topics. Each assessment provides the implications of a technology, details of the technical characteristics, early indicators, drivers and inhibitors for adoption, parallels and precedents, and the sources of reference materials.

This study was conducted by the Naval Postgraduate School under the auspices of the Chief Science and Technology Advisor, National Maritime Intelligence Office (NMIO). Points of view or opinions stated in this study do not necessarily represent the official position of the NMIO, the United States Navy, or the U.S. Government.

Choke Point Risk Assessment

Gary Langford, Department of Systems Engineering, Naval Postgraduate School

Implications

Shipping through the Panama Canal, the Suez Canal, the Straits of Gibraltar, the Straits of Hormuz, and the Straits of Malacca account for up to 80 percent of the shipping trade annually. Asymmetric and nation-states can threaten commercial and strategic goods transiting through these "choke points" with both conventional weapons and improvised means of disruptions. Assessing the risks associated with these transits is problematic – generally relying on formulations that apply to only simple situations or are extrapolations from unrelated kinds of activities. Many proposed schemas for determining risks have been proposed, and all purport to identify risks and offer correlative factors that imply mitigation strategies. However, no validated means of assessing risks yet exists because no theory of risk has been posed; no framework for analysis has been vetted with sufficiency to provide an analytical or predictive formulation that adequately characterizes risk. Many characterizations of risk analysis rely on statistical-based methods and preference their methods with discussions about averages and distributions. A working definition for risk is something that is perceived to be significant, but may not be understood or accommodated in current thinking.

Details

The qualitative assessment of risk is a learned response from correlating prior experiences of risk and reward (Wunderlich, K., Symmonds, M., Bossaerts, P., and Dolan, R.J. 2011). Risk assessment is personal, but sometimes reflected in group dynamics and decision making. Risk management includes the concepts of combining multiple instances of activities of different assets to reduce the total risk in a portfolio of assets. For maritime shipping, a portfolio of ships or the type of cargo in transit is exposed to a variety of situations that are instrumental in creating cause for thinking in terms of different risks. While the specifics of a particular ship or cargo container may be difficult to particularize, an aggregation of seemingly similar situations may be expected to have similar behaviors and outcomes. The statistical validation of that statement is found in historical data, i.e., a basis for prior experience. Quantifying that experience forms a likelihood of historically significant events recurring based on similar assumptions and circumstances. Presumably the greater care taken in developing the database of prior events helps to correlate the events with proximate and conditional correlative actions (Langford 2012). Correlation does not imply causality. Causality is often thwarted by the complex nature of the actions and the determination that the action is related to a specific situation. More generally, the "complexity" that results from a set of actions is often characterized by the total number of objects and processes that are involved in some manner with the actions. The greater number of objects and processes, the more complex the correlative relations (Homer 2001; Li 1997).

The quantitative assessment of risk is problematic, with perhaps the exception being the most simple of events, e.g., fair coin toss. Applying the logic (Lowrance 1976) that is typical of simple risk analysis, Lewis (2006) defines risk as a function of three variables: threat, vulnerability, and damage. Vulnerability and damage can be thought of from an experiential perspective, i.e., as the historical correlative factors that characterize risk and reward. From an analytical view, threat seems to be bothersome, especially considering asymmetric conflicts and assessments.

Replacing damage with value, Langford and Horng (2007) capture risk through threat, vulnerability, and value. An element e of a system is associated with a risk, R_e, defined by

$$R_e = X_e U_e V_e = X_e(1 - a_e)V_e \qquad (1)$$

where threat, X_e, is a set of harmful events that could impact the element; vulnerability, U_e, is the probability that element e is degraded or fails in some specific way, if attacked; value, V_e, results from a successful attack on element e; and susceptibility, a_e, is the likelihood that an asset will survive an attack, V_e is given by (1). It may be loss of productivity, casualties, loss of capital equipment, loss of time, or loss of dollars. Susceptibility is the complement of vulnerability.

Since an element in a system (or network) may be connected to more than one element, the number of Value Transfer Functions (VTFs), exchange of value between elements, associated with the element is the degree of the element. Subscribing to Mannai and Lewis (2007), we obtain the system risk, R, as

$$R = \sum_{i=1}^{n+m} X_i(1-a_i)g_i V_i \qquad (2)$$

in which n denotes the number of elements, m the number of links or VTFs, and g_i denotes the degree of the i^{th} element.

As a result of the VTF between two elements, e_1 and e_2, at the moment of their interaction, we have

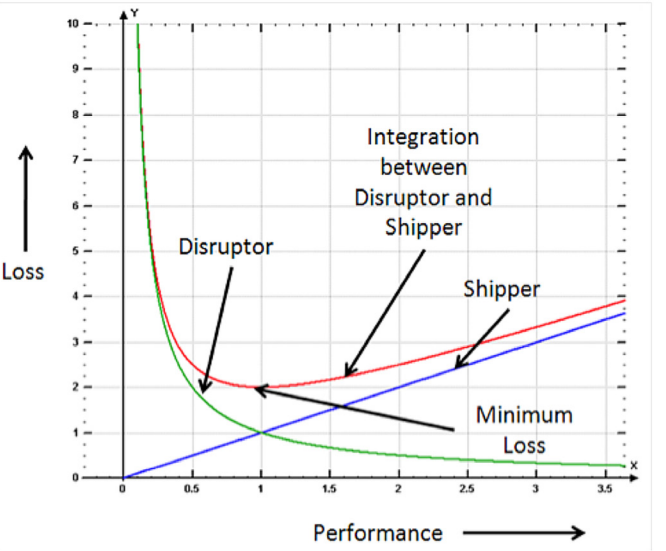
$$\frac{V_{e_1}}{R_{e_1}} = \frac{V_{e_2}}{R_{e_2}} \quad (3)$$

It is the expression in (3) that forms the basis for risk management.

Dealing with the concept of "threat" is a non-statistical foray into motivations, intent, knowledge, skills, and abilities of those who want to impose their will for their purpose. Qualifying the "threat" is more than historical precedence, more than statistical frequency, and more than the considerations of subject matter experts. All these factors are important, but by themselves do not stand up to the rigors of good intelligence. Having actionable intelligence permits a better quantification of risk. Without actionable intelligence, risk must be predicated on "gut feeling" with its related problems. Inevitably, a more quantitative assessment of risk is necessary.

Without providing explicit examples, risk can be thought of as a type of integration between an adversary and a target ship. Applying a model of integration that relies on a mereology of objects and processes to illustrate the whole (i.e., the result of integration) from the parts (e.g., disruptor, ship), three questions can be addressed. First, why does integration occur, i.e., why and where is there damage (or disruption)? Second, why and when does disruption not occur? And third, in orchestrating a solution (solving the problem), is there a solution that satisfies all stakeholders (including the disruptors)? While these three questions are merely posed to help shape thinking, their answers are also fundamental to analyzing risk, and in particular, "threat". The impetus is to address value and risk within an ontological framework.

Generally, risk is a structural property of the interactions between objects, whereas specifically, risk is inherent in the interactions involving enterprise, business, and process. Risk is akin to interaction with an exchange of Energy, Matter, Material wealth, or Information (EMMI). An instructive way to consider risk (as an integration) is to capture the losses that each stakeholder experiences when the event of "disruption" occurs. The individualized loss for each stakeholder is their damage, the interaction is their threat, and the circumstance is their vulnerability. Were the interaction between disruptor and ship to occur, the risk is area under the loss function from the perspective of a given stakeholder. The intersection of loss functions for the stakeholders involved in the interaction indicates the minimum loss that is achievable given there is an integration (i.e., a disruption). There can be interactions without integration. A typical loss function is shown in the figure below. The combined loss function for the stakeholders (disruptor and shipper) are shown with a minimum loss at Performance = 1; the disruptor shows an increased losses if he fails to achieve a certain level of performance and an effective economy of scale that derives from a disruption; and a shipper reflects greater costs as he steps up additional security measures.



Loss functions for components or wholes can be built to help quantify risks. Interpreting the curves can be done analytically or notional, depending on the focus of determining the amount of money that is cost effective for a given level of security or whether the trends in spending or more important. The means to quantify risk are outlined in the source (Langford 2012).

Early Indicators

The formal development of loss functions coupled with scenario planning. Scenario planning differs from contingency planning, sensitivity analysis, and simulations. Scenario planning explores the joint impact of various uncertainties, especially useful when determining risks. Scenarios provide credible context in which to explore various options of policy, operations, or strategies. There are four distinct types of scenarios: demonstration, driving force, system-change, and slice-of-time. An early indicator of analyzing risk is scenario planning.

Drivers & Inhibitors

Drivers: Planning needs and schedule.

Inhibitors: None.

Parallels & Precedents

Used widely in operational planning, insurance assessments, and in comprehensive risk analysis.

Sources

1. Homer, S. and Selman, Alan L. 2001. Computability and Complexity Theory, Springer-Verlag.
2. Langford, G., and Lim, H.L. 2007. “Predicting and Assessing Disruptive Technologies Using Event Space Modeling,” Proceedings of Asia-Pacific Systems Engineering Conference, 23-24 Singapore, March.
3. Langford, G. 2012. Engineering Systems Integration: Theory, Metrics, and Methods, CRC Press, Boca Raton.
4. Lewis, T. 2006. Critical Infrastructure Protection in Homeland Security, John Wiley & Sons, New Jersey.
5. Li, M. and Vitanyi, P. 1997. An Introduction to Kolmogorov Complexity and Its Applications, Springer Verlag.
6. Lowrance, W. W. 1976. Of Acceptable Risk. William Kaufman, Inc.
7. Mannai, A.W. and Lewis, T. 2007, “Minimizing Network Risk with Application to Critical Infrastructure Protection,” Journal of Information Warfare, 6(2): 52-68.
8. Wunderlich, K., Symmonds, M., Bossaerts, P., and Dolan, R.J. 2011. “Hedging Your Bets by Learning Reward Correlations in the Human Brain,” Neuron, 71, 22 September, pp. 1141 – 1152.

Electro-Optical Sensors for Ship Defense

John Osmundson, PhD, Department of Information Sciences, Naval Postgraduate School

Implications

The increasing incidence of piracy and asymmetric attacks on ships in waters remote from coastal areas has prompted the need for enhanced onboard protection measures for both civil ships and warships. A key element to effectively countering an attack is its early detection: enabling the ship's crew sufficient opportunity to prepare for and prevent invaders from intruding the close-in range or, worse boarding the ship. The possibility of permanent and continuous surveillance of a ship's surroundings would also reduce the need for crew personnel to be assigned to this task.

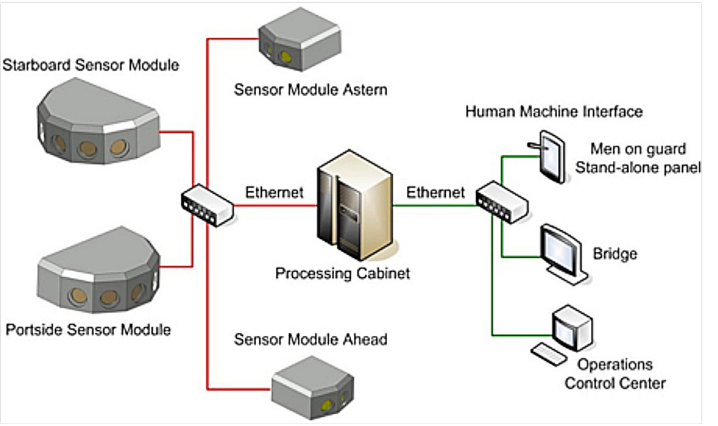


Figure 1. System architecture for automatic surveillance of a ship's surroundings using sensors [1].

Details

Ship reaction and defense against potential pirate and terrorist attacks requires early sensing of the emerging situation. Close-in range electro-optical surveillance systems capable of day and night imaging can provide the sensing support necessary to enhance the ship's situational awareness and therefore the ship's security. A surveillance system consisting of a staring wide area sensor package equipped with uncooled infrared (IR) sensors provides continuous high quality imagery of the platform's surroundings. The image data is evaluated, both manually by a human observer and automatically using signal processing algorithms suited for the detection of potential pirate and terrorist attacks in maritime environments. This sensor system can be augmented by an electro-optical sensor system that has higher resolution and can track multiple targets.

Using video imagery of the surroundings, a single crew member can essentially monitor the whole ship and raise the alarm to initiate counteractive measures. This system can even detect approaching objects possessing a low radar cross-section. The real-time video imagery allows the human operator to classify the type of threat.

Modules containing uncooled IR microbolometer sensors are arranged on the ship to continuously cover its surrounding. Using this configuration, the number of 'dead zones' caused by shadowing are minimized, and observation is possible from the ship's hull. Image data is transferred to a computer for real-time processing. Live video imagery and alarm data can be fed to several clients simultaneously. All of the system components can be connected on a common network (Figure 1).

Automatic processing for the purpose of object detection imposes specific demands on the image quality, such as stable performance with high detection rates and low false-alarm probability. Sensors operating in the long-wavelength IR spectral band have night-vision capabilities and are independent of external illumination. In addition, they avoid sensor saturation. Long-wave IR sensors experience low impact from sun glint and external illumination. Thus, objects with low thermal contrast respective to their natural background (i.e., little temperature difference) can be resolved in the long-wave IR spectral range. Sensors with different spectral responses partially enhance the detection rate under specific daily environmental conditions.

Video graphics array-format microbolometer detectors possessing 50mK noise equivalent temperature difference (i.e., low camera noise) and exhibiting few pixel defects capable of operating in large detector formats and with high thermal resolution are used. The temporal response of microbolometer detectors is fully compatible with the scene dynamics for maritime applications. The detectors are equipped with fast IR optics that meet the demands of illuminating the full detector area and provide high image quality over a wide range of temperatures. Cryogenic cooling of detectors is not required, which extends detector lifetime and reduces the need for maintenance.

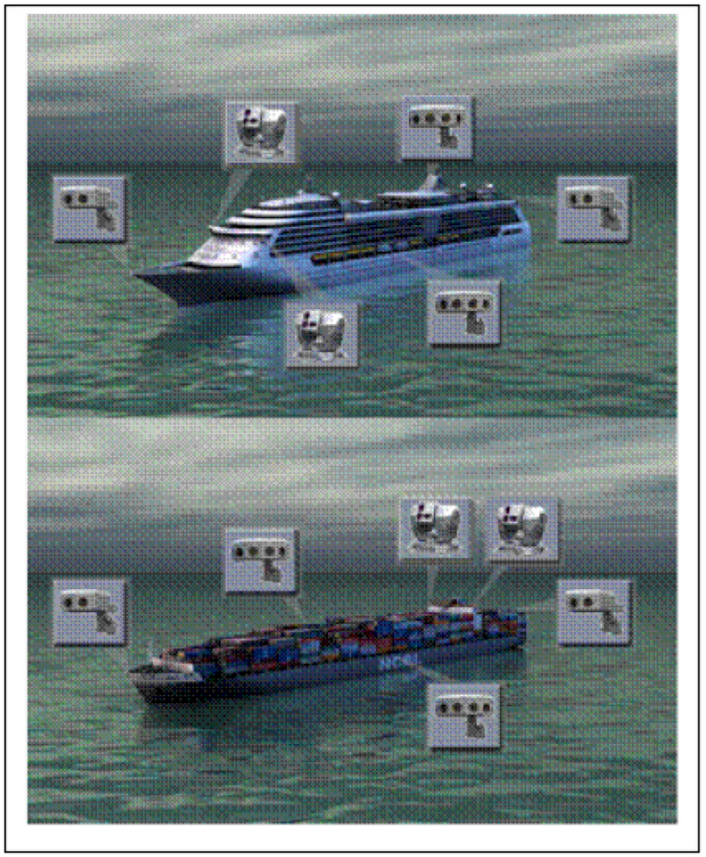


Figure 2. Notional Arrangement of Surveillance System on a Cruise Liner and a Container Ship [2]

The staring arrangement of sensors used to cover the surroundings of the vessel is based on commercially available low cost microbolometer IR detectors. This is in contrast to surveillance systems that use a continuous scanning approach or a step-stare approach, both of which require accurate relative alignment of moving electro-optical components, increasing system cost and increasing maintainability requirements.

Early Indicators

Improvements in large IR detector formats.

Better IR detector thermal sensitivity

Drivers & Inhibitors

Drivers: Need for advanced warning of potential attacks on ships.

Inhibitors: Cost of systems, crew training.

Parallels & Precedents

Surveillance sensing and monitoring systems at commercial centers.

Automotive applications such as night vision and adverse weather driver assistance systems.

Sources

1. Künzner, Nicolai, Jörg Kushauer and Stefan Katzenbeißer, “An electro-optical sensor system that includes automatic image processing enables detection of threats to naval platforms”, 9 April 2012, SPIE Newsroom. DOI: 10.1117/2.1201204.004166
2. Künzner, N., J. Kushauer, S. Katzenbeißer, K. Wingender, Modern electro-optical imaging system for maritime surveillance applications, Waterside Security Conf. (WSS) , p. 1-4, 2010. doi:10.1109/WSSC.2010.5730255
3. Künzner, N., J. Kushauer, S. Katzenbeißer, “SIMONE—Ship infrared monitoring, observation and navigation equipment”, Strategie und Technik, p. 52-55, 2008.
4. Stockfisch, D., Stockfisch, “Fregatte Klasse 125”, Strategie und Technik, pp. 54-59, September 2008

Metamaterial Imaging System for Maritime Security Application

Tom Huynh, PhD, Center for Decision, Risk, Controls & SIGINT, Naval Postgraduate School

Implications

Detection of maritime threats requires remotely collecting (i.e., capturing and transmitting) images of large oceanic areas of interest. Metamaterial-based sensors or imaging systems may provide a revolutionary means to collect exceedingly large amounts of these images without requiring excessively large communications bandwidth for transmission of the images. This article discusses the potential use of metamaterial-based imaging systems in reducing image transmission loads and, hence, communications bandwidth. This technology applies to both counter-smuggling operations and global supply chain security.

Details

The maritime community faces many challenges in realizing its goals for achieving maritime security. One of these challenges is communication bandwidth overload caused by transmission of an enormous amount of images of a scene (e.g., a large area of an ocean traversed by vessels) captured by current digital cameras or imaging systems. This challenge could be overcome if a full image of the scene could be obtained with far fewer pixels, resulting in a significantly reduced demand for communication bandwidth. A full image with far fewer pixels could be achieved with an imaging system that compresses the image as it is being collected before it reaches the sensor. Such an imaging system may be possible with recent advances in metamaterials.

Metamaterials are electromagnetic materials, which consist of periodically arranged artificial structures with a pitch smaller than the wavelength of excitation [10, 11]. Theoretically proposed by Pendry et al. [1], and experimentally demonstrated by Smith et al. [2], metamaterials have attracted intensive research interest from microwave engineers and physicists in recent years. These materials can control and manipulate electromagnetic waves and exhibit some exotic electromagnetic properties that strongly depend on the geometry of metamaterial molecules rather than on their composition [3]. Some of these properties are backward propagation, reverse Doppler effect, reverse Vavilov-Cerenkov effect [4], negative refraction [2, 4, 5], diffraction-limit breaking imaging [6, 7], and cloaking [8, 9].

Tackling the communication bandwidth overload challenge is encouraged by a recent development of a thin metamaterial compressive imaging system [12]. This new system enables a collection of 400 pixels of data with only 10 measurements (a 40:1 compression ratio). Its metamaterial aperture is 40 cm long and has no moving parts or lenses. It consists of two copper plates separated by a piece of plastic. One of the plates is etched with repeating boxy structures of about 2 mm long that permit passage of different microwave frequencies (Figure 1). These various microwave frequencies used to scan a scene will provide the information necessary to reproduce it [13, 14].

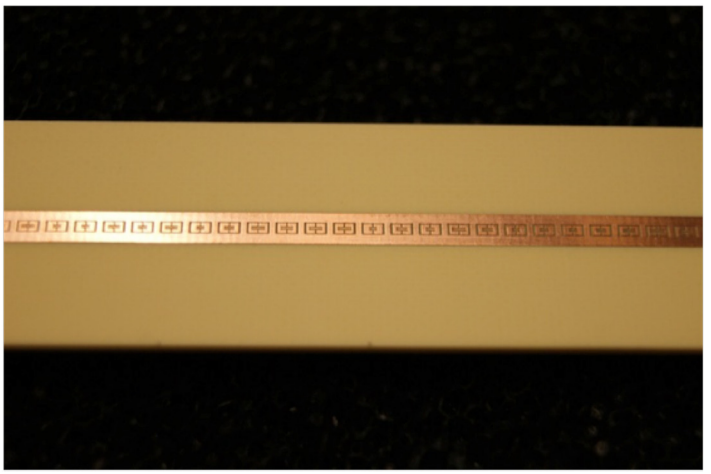


Figure 1. One-dimensional metamaterial aperture [12]

This kind of imaging system could provide the capability needed for harbor protection. For example, this capability could aid Singapore in its harbor protection effort by solving its problem of reducing transmission overload, caused by transmission of extremely large amounts of images of scenes of regions of its ocean and Straits that are densely populated by ships.

Harbor protection for other countries would also benefit from this capability. The realization of this capability for harbor protection or maritime security applications in general necessitates a successful

transition of this imaging system technology from its laboratory state to a commercial state. The transition is clearly not simple, as this technology needs further verification and validation so as to ensure in particular lossless compression of images is achievable and meaningful. Furthermore, cost analysis must be done to ascertain its advantages.

Early Indicators

A new microwave compressive imaging system developed at Duke University is reported in source [12]. In this system, microwaves traverse the metamaterial and interfere with each other to produce a wave pattern that propagates from the metamaterial aperture to an object and, upon reflection from its surface, returns to a detector near the original metamaterial aperture. The object is then identified by combining the intensity of the scattered waves with the wave pattern exiting the aperture.

Drivers & Inhibitors

Drivers: A driver related to maritime security enhancement is a need for reducing transmission loads of scenes images containing potential threats among non-hostile objects.

Inhibitors: Potential inhibitors pertain to engineering and physics and to the pace of technology development.

Parallels & Precedents

A precedent is the demonstration of the feasibility of this metamaterial-based sensor technology [12].

Sources

1. Robbins, D. J., Pendry, J. B., Holden, A. J., and Stewart, W. J., "Magnetism from conductors and enhanced nonlinear phenomena," IEEE Trans. Microwave Theory Tech., 47(11):2075, 1999
2. Smith, D. R. , Padilla, W. J. , Vier, D. C. , Nemat-Nasser, S. C., and Schultz, S., "Composite Medium with Simultaneously Negative Permeability and Permittivity," Phys. Rev. Lett., 84:4184, 2000.
3. Pendry, J. B., "Metamaterials in the sunshine," Nat. Mater, 5, 599–600, 2006.
4. Veselago, V. G., "The electrodynamics of substance with simultaneously negative values of ε and μ," Sov. Phys. Usp., 10, 509–514, 1968.
5. Robbins, D. J., Pendry, J. B., Holden, A. J., and Stewart, W. J., "Magnetism from conductors and enhanced nonlinear phenomena," IEEE Trans. Microwave Theory Tech., 47(11):2075, 1999.
6. Pendry, J. B., "Negative refraction makes a perfect lens," Phys. Rev. Lett., 85, 3966–3969, 2000.
7. Smolyaninov, I. I., Hung, Y.J., Davis, C.C., "Magnifying superlens in the visible frequency range," Science 315, 1699–1701, 2007.
8. Pendry, J. B.; Schurig, D.; Smith, D. R., "Controlling electromagnetic fields," Science, 312, 1780–1782, 2006.
9. Cai, W., Chettiar, U. K., Kildishev, A. V., and Shalaev, V. M., "Optical cloaking with metamaterials," Nat. Photonics, 1, 224–227, 2007.
10. Plum, E., "Chirality and Metamaterials," PhD Thesis, University of Southampton, Faculty of Engineering, Science and Mathematics, Optoelectronics Research Centre, February 2010.
11. Chen, T., Li, S., and Sun, H., "Metamaterials Application in Sensing," Sensors, 12, 2742-2765, 2012.Hunt, J., Driscoll, T., Mrozack, A., Lipworth, G., Reynolds, M., Brady, D., and Smith, D.R., "Metamaterial Apertures for Computational Imaging," Science, 18 January 2013, Vol. 339, no. 6117, pp. 310-313.
12. Hunt, J., Driscoll, T., Mrozack, A., Lipworth, G., Reynolds, M., Brady, D., and Smith, D.R., "Metamaterial Apertures for Computational Imaging," Science, 18 January 2013, Vol. 339, no. 6117, pp. 310-313.
13. Drake, N., "New Metamaterial Camera Has Super-Fast Microwave Vision," Jan.17, 2013. (http://www.wired.com/wiredscience/2013/01/)
14.Fellet, M., "Metamaterials perform image compression before light reaches the sensor," Jan. 17, 2013. (http://arstechnica.com/science/2013/01/)

Models for Analysis of Competing Hypotheses for Assessing Maritime Threats

Tom Huynh, PhD, Center for Decision, Risk, Controls & SIGINT, Naval Postgraduate School

Implications

Collected and analyzed intelligence needs to be integrated to enable formulation of actionable intelligence and assessment of global maritime threats to U.S. and allied interests [4]. Improvement in analysis of collected intelligence or evidence is needed to satisfy this need and requires advanced methods of analyzing multiple alternative hypotheses with multiple items of evidence. This technology scan discusses the potential use of Bayesian approaches to assessing the relevance and the value of evidence in the determination of the likelihood of competing hypotheses.

Details

Achieving maritime security is faced with many challenges. One of these challenges is analysis of collected evidence so as to enable formulation of actionable intelligence and the assessment of global maritime threats to U.S. and allied interests [4]. To meet this challenge, advanced methods of intelligence analysis must be carried out and developed.

The fundamental elements of intelligence analysis are evidence, hypotheses, and analysis. Intelligence analysis aims at arriving at the most plausible hypothesis from among several alternative hypotheses that best fits the evidence being analyzed. A methodological challenge is to create a framework for reasoning about alternative hypotheses (i.e., "judging the relevance and the value of evidence to determine the likelihood of competing hypotheses" [8]) or the analysis of multiple hypotheses with multiple items of evidence to support intelligence analysis "that can be used under a wider variety of circumstances and which can handle both empirical data and formally-expressed beliefs as evidence for or against each hypothesis" [8]. One of the approaches is the so-called Analysis of Competing Hypotheses (ACH).

ACH Methodology

Developed in the mid- to late-1970s by Richard Heuer, a former CIA Directorate of Intelligence methodology specialist, ACH [2] is a method for systematically comparing the likelihoods of competing hypotheses based on the available evidence. The ACH method, consisting of eight steps [2] provides "a basic framework for identification of assumptions, arguments, and hypotheses; consideration of all evidence and hypotheses – including its value relative to the hypotheses; a method of disconfirmation for identifying the most likely hypotheses; an approach to reporting the results of the analysis; and an approach to detecting future changes in the outcomes" [8]. Essentially, in the ACH approach, the analyst is required to simultaneously evaluate all reasonable hypotheses and reach conclusions about their relative likelihood based on the evidence provided [8].

The steps taken in ACH can be simply described as follows [10].

1. Identify the possible hypotheses. List significant evidence and arguments for and against each hypothesis.
2. Build an ACH matrix with hypotheses in the top row and pieces of evidence in the first column. Analyze the diagnostic value of each piece of evidence for each hypothesis. Refine the matrix and repeat this step when necessary.
3. Draw tentative conclusions about the relative likelihood of each hypothesis by trying to disprove the hypotheses instead of proving them. Analyze the sensitivity of each conclusion to a few critical items of evidence.
4. Report final conclusions by discussing the relative likelihood of all hypotheses rather than the most likely one and identifying milestones for future observations that may indicate events of unexpected behaviors.

The first ever approach to ACH was manual. It was then automated by Palo Alto Research Center (PARC) for the Intelligence Community; this automation resulted in a software tool based on ACH, called ACH0 [7]. Recent years have seen Bayesian and other advanced forms of ACH for updating beliefs in hypotheses as evidence is obtained, such as Bayesian updating model for intelligence analysis [5], Bayesian approach for fusion of intelligence information [6], a multinomial-Dirichlet model for ACH [11], and ACH using a normative Bayesian probabilistic framework [10].

Bayesian Approaches to ACH

Bayesian inference is a statistical procedure for quantifying uncertainty. From a mathematical perspective, Bayesian inference is clearly an

optimal method for calculating probabilities based on a series of subjective probability judgments by intelligence analysts or other experts. In order to relate an item of evidence to a hypothesis, Bayesian ACH usually requires the analyst to make at least two (and usually four) separate judgments [3]:

- What is the probability I would see this evidence if this hypothesis is true?
- What is the probability I would see this evidence if this hypothesis is not true?
- What is the probability that this hypothesis is true if I see this evidence?
- What is the probability that this hypothesis is not true if I see this evidence?

An ACH matrix can be represented by a Bayesian network, enabling Bayes reasoning about competing alternative hypotheses [10]. A Bayesian network, which encodes probabilistic relationships among variables of interest, has both a causal semantics and a probabilistic semantics, and is an ideal representation for combining data with prior knowledge or subjective beliefs or analysts' judgments.

ACH Using a Normative Bayesian Probalistic Framework

ACH using a normative Bayesian probabilistic framework combines the strengths of ACH and Bayesian networks for interpretation of situations and evaluation of hypotheses. Bayesian networks generalize ACH matrices (or tables). The added generality might be important to the analyst for hypothesis management. As emphasized by Valtorta et al. [10], the following fictitious example was devised to illustrate their techniques.

An analyst, who is experienced with terrorist activities related to the oil infrastructure of Iraq and Iran, needs to determine whether terrorists will try to create conflict in Iran by attacking the oil infrastructure in the Abadan region by analyzing the following competing hypotheses:

H1: Terrorists will bomb the oil refineries in Abadan.
H2: Terrorists will bomb the oil pipelines in Abadan.
H3: Terrorists will bomb the oil wells in Abadan.
H4: Terrorists will bomb the oil facilities in Shiraz.
H5: Terrorists will not launch an attack.

The evidence presented to him includes:

E1: A phone wiretap on a suspected terrorist cell in Beirut records a discussion about crippling the Iranian economy by destroying oil production facilities within the Abadan region.
E2: The oil refinery in Abadan can produce 0.37 million barrels per day. Oil is transported through pipeline.
E3: The oil refinery in Shiraz can produce 0.04 million barrels per day.
E4: There is an oil pipeline with from Abadan to Basra, which crosses the border. The capacity of this pipeline is over 0.2 million barrels per day.
E5: Historical analysis allows us to conclude that the affected oil industry will cripple the Iranian economy, which will lead to the conflict with its neighbors.
E6: The area near a border is easier for terrorist to infiltrate.
E7: Terrorists prefer a target that is near a road.

The hypotheses and items of evidence lead to the following ACH matrix, in which '+/-' means there is/ is not a connection between a piece of evidence and a hypothesis.

Table 1: An ACH Matrix [10]

	H1	H2	H3	H4	H5
E1	+	+	+	-	-
E2	+	+	+	-	-
E3	-	-	-	+	-
E4	+	+	-	-	-
E5	+	+	+	+	-
E6	-	+	-	-	-
E7	-	-	-	-	-

Figure 1 shows the bipartite graph, corresponding to the ACH matrix in this example. It is a special case of a Bayesian network corresponding to the ACH matrix [10].

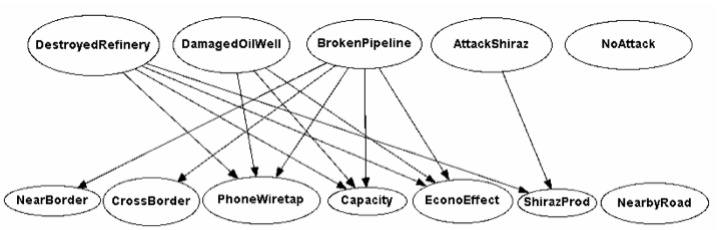


Figure 1. Bayesian network corresponding to the ACH matrix in Table 1 [10].

The nodes in a Bayesian network (BN) represent the possible hypotheses. The nodes representing the disproved hypotheses are linked to evidence nodes, whereas the nodes representing the unproven hypotheses are not. The disproved and unproven hypotheses are with the near-to-zero probability values in BNs. Unproven hypotheses are kept until they are disproved by incoming items of evidence. The prior knowledge includes explicit evidence (in the messages) and the analysts' assumptions or arguments and is stored in BN fragments. Diagnosticity of evidence (items

most helpful in judging the relative likelihood of the hypotheses) is captured by the conditional probability tables residing in the BN fragments. The relative likelihood of hypotheses is assessed by the computed probability values of each hypothesis, after matching the messages with the BN fragments and composing the BN fragments into a situation-specific scenario. (The probability representation of the likelihood is finer than the notation of minus/plus or the numerical scale in ACH.) The sensitivity of the hypothesis to the provided evidence can also be analyzed. Furthermore, in [10], the tacit knowledge is captured in the form of additional BN fragments and which additional pieces of evidence should be collected to increase the confidence in the conclusions reached.

Multinomial-Dirichlet Model for ACH

In this multinomial-Dirichlet probabilistic framework for ACH, which is a Bayesian extension of ACH, a combination of a Dirichlet prior distribution on the hypothesis probabilities and multinomial data (or evidence) results in a Dirichlet posterior distribution on the hypothesis probabilities. The true hypothesis is a single draw from a multinomial distribution, and evaluation of the evidence then provides the information about the parameter of this multinomial distribution, which gives the probabilities of the hypotheses [11].

The algorithm proposed in source [11] for implementing the multinomial-Dirichlet probabilistic framework for ACH consists of (1) constructing the framework for the ACH matrix, (2) assigning evidence weights, (3) relating evidence to hypotheses, and (4) computing the posterior. The posterior distribution is used for all inference.

The Dirichlet posterior distribution on the hypotheses allows easy computation and use for conducting inference. If pieces of evidence are against one or more hypotheses, irrelevant to all hypotheses, and subject to deception, then posterior distributions are not Dirichlet, and inference becomes more difficult as a result of this loss of conjugacy. In this case, several extensions of this model are available for handling these special types of evidence. Furthermore, Monte Carlo methods can be used to make inference computationally feasible, and samples from the posterior can be obtained fairly quickly [11].

When an evidence item is entered as either for, against, or irrelevant to a hypothesis (it is as though the evidence associated with it is missing), the posterior distribution on the hypothesis probabilities is no longer in closed form. In order to express the posterior, the evidence is partitioned by type into three sets: set A contains evidence items with only numerical values; set B contains evidence items that are irrelevant to hypotheses; and set C contains evidence items that are just for and against hypotheses and pertaining to irrelevant hypotheses. The posterior distribution, $\pi(p|E)$, is then given by [11]:

$$\pi(p|E)\alpha\prod_{i\in A}\prod_{j=I}^{N} p_j^{x_{ij}} \prod_{i\in B}\prod_{j=R_i}^{N}\frac{p_j^{x_{ij}}}{\sum_{k\in R_i} p_k}\prod_{i\in C}\Big(\sum_{i\in F_i} p_j\Big)^{\omega_i}$$

where $\boldsymbol{p}$ is the probabilities of the hypotheses; $\boldsymbol{E}$ the items of evidence, N the number of hypotheses; P_j the probability of the j^{th} hypothesis, ω_i the weight of the i^{th} evidence item indicating its strength or relative importance such that $\sum_{i=1}^{M}\omega_i = n_{ess}$, M being the number of evidence items and n_{ess} being the equivalent prior sample size of the evidence; x_{ij} the relative likelihood of the i^{th} evidence item conditioned on the j^{th} hypothesis; F_j is the complement of the set of hypotheses the i^{th} evidence item is against; and R_i the set of hypotheses to which the i^{th} evidence item is relevant.

This model offers an advantage over simpler approaches such as the approach in source [6] in its ability to weight evidence items by importance or diagnosticity.

This model can also incorporate evidence with the potential for deception, but the posterior distribution may not be obtained in closed form and Monte Carlo methods will be required to make inference possible [10]. In source [8], ACH is modified to account for cognitive factors that contribute to poor deception detection; the resulting model is called ACH-CD (counter-detection). An explicit counter-deception business process based on ACH-CD and aided by Bayesian belief networks is used to identify distinguishing evidence that a deceiver must hide and a counter-deceiver must uncover, isolate local deception in intelligence reporting and sensing from global deception, and identify circumstances when it might be fruitful to entertain additional hypotheses. It is shown in source [9] that analysis of evidence available to the Japanese Navy prior to the Battle of Midway using ACH or ACH-CD, methods to isolate local and global deceptions, and Bayesian belief networks might have detected the American deception that allowed U.S. Pacific Fleet carriers to surprise, ambush, and sink four Japanese carriers threatening Midway Island.

Tackling the challenge of improvement in analysis of collected intelligence or evidence to analyze multiple alternative hypotheses with multiple items of evidence is encouraged the Bayesian approaches to assessing the relevance and the value of evidence in the determination of the likelihood of competing hypotheses. Accuracy in the intelligence analysis resulting from these approaches would enable formulation of actionable intelligence and assessment of global maritime terrorist threats to U.S. and allies' interests.

Early Indicators

Only open-source examples demonstrate the applicability of the Bayesian approaches to ACH in non-intelligence domain [10, 11]. Unknown details of how historic deceptions have succeeded, such as the Battle of Midway, have been successfully determined with ACH-CD [9].

Drivers & Inhibitors

Drivers: A driver related to maritime security enhancement is a need for intelligence analysis that requires approaches other than the nontraditional approaches to ACH.

Inhibitors: First, the Bayesian approaches to ACH require the analyst to be well versed in Bayesian analysis or the assistance of a Bayesian methodologist to guide the mainstream analyst through the process [3]. Second, the assignment of weights to hypotheses in the multinomial-Dirichlet model can seem overly subjective as can the assignment of an equivalent sample size-ness. The sensitivity of conclusions to choices of weights must be examined, though care should be taken that weights are not manipulated to obtain a preconceived conclusion [11]. Finally, unless distribution conjugacy is possible, often considerable analytical and computational difficulty inherent in Bayesian methods must be overcome in order to derive solutions and compute numerical answers [1].

Parallels & Precedents

No parallels and precedents in intelligence domain are known as all open-source examples to demonstrate the applicability of the Bayesian approaches to ACH pertain to non-intelligence domain.

Sources

1. Ferson, S., "Bayesian methods in risk assessment," 2003, http://www.ramas.com/bayes.pdf
2. Heuer, R. J., "Psychology of Intelligence Analysis," Washington, D.C.: Central Intelligence Agency Center for the Study of Intelligence, 1999. [Online]. Available: http://www.cia.gov/csi/books/19104.
3. Heuer, R. J., Jr., "How Does Analysis of Competing Hypotheses (ACH) Improve Intelligence Analysis?" Version 1.2, October 16, 2005, established by Pherson Associates.
4. Hoppa, R. V., RDML (Select) USN, "NMIO Briefing," National Maritime Intelligence-Integration Office, 15 Feb 2012.
5. McLaughlin, J., "A Bayesian updating model for intelligence analysis: A case study of Iraq's nuclear weapons program," 2005.
6. Pate-Cornell, M. E., "Fusion of intelligence information: A Bayesian approach," Risk Analysis 22 (2002), no. 3,445-454.
7. Pirolli, P. and Good, L., "Evaluation of a Computer Support Tool for Analysis of Competing Hypotheses." Palo Alto, CA: Palo Alto Research Center, 2004 (UIR Technical Report)
8. Pope, S. and Jøsang, A. "Analysis of Competing Hypotheses using Subjective Logic," 10th International Command and Control Research and Technology Symposium: The Future of C2 Decision-making and Cognitive Analysis, paper126.pdf
9. Stech, F.J. and Elsässer, C., "Midway Revisited: Detecting Deception by Analysis of Competing Hypothesis," 72nd MORS Symposium, Naval Postgraduate School, Monterey California, 22-24 June 2004.
10. Valtorta, M., Dang, J., Goradia, H., Huang, J., and Huhns, M., "Extending Heuer's Analysis of Competing Hypotheses Method to Support Complex Decision Analysis,"IA-05.pdf
11. Wilson, J. L. and Duncan, K. E., "A Multinomial-Dirichlet Model for Analysis of Competing Hypotheses," AP0912 09 AP0912.pdf

Big Data Analytics in Maritime Security Applications

Tom Huynh, PhD, Center for Decision, Risk, Controls & SIGINT, Naval Postgraduate School

Implications

Voluminous amounts of collected data or evidence need to be processed in order to enable formulation of actionable intelligence and assessment of global maritime threats to U.S. and allied interests. Satisfaction of this need requires technologies that enable effective and timely handling of such huge amounts of collected data. Such technologies are known as "big data" technologies, which are the focus of this technology scan.

Details

In maritime security missions, as in security missions in general, it is crucial to get the right information to the right people at the right time to accelerate actionable decisions in mission-critical environments [13]. Related to this right-information-to-the-right-people-at-the-right-time challenge is the problem of processing "big data" − that is, to rapidly and efficiently analyze extremely large sets of data amassed from data or intelligence collections. To solve this difficult problem, advanced methods and "big data" tools to handle mountains of collected of data pertaining to maritime security are needed.

"Big data" refers to extremely large amounts of data, both structured and unstructured, from disparate sources such as communications records, email, words, images and video, documents, machine-generated data, and streams of sensor data. The size of these data amounts can be on the order of petabytes and larger. As of 2012, the size of data sets on the order of exabytes (2.5×1016) of magnitude can feasibly be processed in a reasonable amount of time [5][22], and 2.5 quintillion (2.5×1018) bytes of data are created every day [17]. According to a Cisco estimate, global mobile data traffic flow over the Internet in 2015 will reach 6.30 exabytes a month [3]. In the intelligence domain, the United States National Security Agency's Utah Data Center is currently being built and, when finished, will be able to handle yottabytes (1024 or one septillion (1,000,000,000,000,000,000,000,000) bytes), which is 1000 zettabytes, of information collected by the NSA [1].

There are five dimensions to the definition of big data: volume, variety, velocity, variability, and complexity. The first three are espoused by International Data Corporation (IDC) [18] and the latter two by SAS [21]. "Volume" refers to the amount of data. "Variety" is reflected by all types of data formats. "Velocity" is the rate of producing and processing data to meet demand [6]. "Variability" refers to data flows highly inconsistent with periodic peaks. "Complexity" results from multiple sources of huge volumes of data. Ultimately, regardless of the factors involved, the term "big data" is relative; it applies (per Gartner's assessment) whenever an organization's requirement to handle, store, and analyze data exceeds its current capacity [21].

Just as in any other domain, maritime big data comes from fast ingesting and archiving. Ingesting is the necessary starting point, followed by searching, indexing, and archiving for future use. Maritime data currently comes from coastal methods of surveillance, such as coastal radars, sonars, airborne or ship-based sensors, Automatic Identification Signal (AIS) (for merchant and fishing vessels), VTS (for port and coastal control), LRIT (long-range identification and tracking for merchant ships over long distances), and VMS (for fishing vessels on a global level). Maritime data would be expected to be significantly augmented as a result from persistent global monitoring of the oceans and the world's shipping lanes, assuming the existence of sensor networks with appropriate architectures. The sensors could include earth observation satellites, such as electro-optical systems and Synthetic Aperture Radar (SAR) satellites. SAR satellite data can include the size and kind of ship, the ship's heading, and its speed. Big data would then consist of data from future SAR satellites and current commercial SAR satellites such as TerraSAR-X, RADARSAT and COSMO-SkyMed, data from existing shore-based and airborne monitoring systems, and AIS information. AIS information can also come from AIS receivers installed onboard SAR satellites, such as the Spanish PAZ satellite to be launched in 2014 and the German TerraSAR-X Next Generation (TerraSAR-X2) to be orbited in 2016. The amount of data would increase further with a constellation of these satellites with improved revisit times and intra-day revisit times, such as the envisaged WorldSAR Alliance of TerraSAR-X2 satellites as well as TerraSAR-X, PAZ, RADARSAT and Sentinel [9].

Data volume grows continually, as it comes from not just sensors, messages, and ship manifestos, but also, for intelligence analysis purposes,

from databases that contain information and data pertaining to HUMINT, SIGINT, MASINT, OSINT, as well as social and behavioral science matters (including anthropology, economics, geography, history, international relations, law enforcement, political science, regional studies, social psychology, sociology, and theology). Strategies for processing big data – that is, acquiring, storing, and analyzing the data – are thus needed. Each step in the big data process is vital. The focus of this article is big data analytics.

Big data analytics is the process of examining big data to identify hidden patterns, unknown correlations, and other useful information. Whereas software tools such as predictive analytics and data mining can be used for data processing, traditional data warehouses cannot support it. Emerging big data technologies associated with big data analytics, such as NoSQL databases, Hadoop, and MapReduce, have been used to overcome the failure of traditional data warehouses to support big data processing. These techniques form the core of an open-source software framework that supports the processing of large data sets across clustered systems [15].

Derived from Google's MapReduce and Google File System papers, Apache Hadoop enables applications to work with thousands of computation-independent computers and petabytes of data. The Apache Hadoop "platform" is now commonly considered to consist of the Hadoop kernel, MapReduce, and Hadoop Distributed File System (HDFS), as well as a number of related projects – including Apache Hive, Apache HBase, and others [12].

A 100 percent open source capability written in the Java programming language, Apache Hadoop is the de facto standard for storing, processing, and analyzing huge amounts of data across servers − from hundreds of gigabytes of data (the low end of Hadoop-scale) to terabytes or petabytes of data; it can scale to hundreds or thousands of computers and to efficiently distribute large amounts of work across a set of machines. Hadoop thus implements strategy of moving computation to the data, instead the data to the computation [11, 16].

Computation on large volumes of data in a distributed setting has been performed before. What makes Hadoop unique are its simplified programming model, allowing quick writing and testing of distributed systems, and its efficient, automatic distribution of data and work across machines, utilizing the underlying parallelism of the CPU cores. Grid scheduling of computers can be performed by existing systems such as Condor, but, with Condor, automatic distribution of data requires the management of a separate storage area network (SAN) in addition to the computing cluster. Collaboration among multiple computing nodes must also be managed using a communication system such as MPI. It is challenging to work with the Condor programming model, and it can result in subtle errors [11].

Programs run by Hadoop must be written to conform to a particular programming model, called MapReduce. MapReduce programs enable computation of large volumes of data in a parallel fashion that requires a division of the workload across a large number of machines. To process large volumes of information, MapReduce programs use two different list processing functions − map and reduce − to transform lists of input data elements into lists of output data elements. The mapping function (Mapper) transforms a list of input data elements to a list of output data elements. The reducing function (Reducer) iterates over the input values to produce an aggregate value as output. Reducer is often used to turn a large volume of data into a smaller summary of itself. In MapReduce, every value is associated with a key. The mapping and reducing functions receive input as (key, value) pairs and produce output also as (key, value) pairs. Another component of a Hadoop MapReduce program, called the Driver, initializes the job, instructs the Hadoop platform to execute one's code on a set of input files, and controls the placement of output files. In short, MapReduce allows a high degree of parallelism to be achieved by applications. MapReduce also provides a high degree of fault tolerance for applications running on it by limiting the communication which can occur between nodes, and requiring applications to be written in a "dataflow-centric" manner [11].

Finally, the first-ever enterprise class NoSQL solution for harnessing vast volumes of real-time unstructured and semi-structured big data is provided by Cisco and Oracle − NoSQL software from Oracle and innovative hardware from Cisco Unified Computing System.

Early Indicators

The current use of Hadoop for handling big data encourages its adoption for intelligence analysis in general and maritime security missions in particular. Hadoop has been used for online travel, mobile data, e-commerce, energy discovery (detection of undersea oil reserves), infrastructure management, satellite image processing (to detect patterns of geographic change), fraud detection (related to financial services organizations and intelligence), IT security, and health care [8].

A wide variety of organizations use Hadoop for both research and production. Morgan Stanley puts vast amounts of web and database logs into Hadoop and

processes them using some time-based correlation algorithms to identify triggers of market events. JPMorgan Chase (JPMC), a financial services company with over 150 PB of online data, 30,000 databases, and 3.5 billion user-account logins, turns to Hadoop to carry out the task of reducing fraud, managing IT risk, and mining data for customer insights. eBay, an online auction house, which deals with 10 Terabytes or more of incoming data per day, turns to Hadoop and a 500-node Hadoop cluster using Sun servers running Linux. Orbitz, an online travel site, uses a combination of Hadoop and Hive [14] to process weblogs to derive useful metrics related to hotel bookings and user ratings. Sears, faced with the task of evaluating marketing campaign results and setting pricing, employs a 300-node Hadoop cluster that stores and processes some two Petabytes of data [4].

Drivers & Inhibitors

> **Drivers:** A driver related to maritime security enhancement is a need to store and process big data associated with maritime security activities.
>
> **Inhibitors:** Inhibitors to an organization's effort on big data analytics include "a lack of internal analytics skills and the high cost of hiring experienced analytics professionals, plus challenges in integrating Hadoop systems and data warehouses, although vendors are starting to offer software connectors between those technologies" [20].

Furthermore, existing architectures lag behind new technologies and, if unmodified or properly designed, may not render possible or effective the use of big data technologies.

Some cautions, rather than inhibitors, need be mentioned when dealing with big data for intelligence analysis in general and maritime security in particular. The peril of "false discoveries" may loom in the processing of huge data sets and fine-grained measurement, as a meaningful needle is sought in massive haystacks of data [19]. Also, if not handled properly, big data might lead to a pernicious use of data, in that it supplies more raw material for statistical shenanigans and biased fact-finding excursions [19].

Parellels & Precedents

No parallels and precedents of big data analytics in the intelligence domain or maritime security domain are known. Only open-source examples to demonstrate the use of big data technologies are available and discussed in the section on early indicators.

Sources

1. Bamford, J. "The NSA Is Building the Country's Biggest Spy Center (Watch What You Say)". Wired Magazine. Retrieved 2013-03-18.
2. Harris, D. "10 ways companies are using Hadoop (for more than ads)," Jun. 5, 2012. http://gigaom.com/2012/06/05/10-ways-companies-are-using-hadoop-to-do-more-than-serve-ads/
3. 4syth.com Emerging big data thought leaders, "For Big Data Analytics/There's No Such Thing as Too Big," The Compelling Economics and Technology of Big Data Computing March 2012.
4. Fortune 500 companies using Hadoop, November 8, 2012. http://ravistechblog.wordpress.com/2012/11/08/fortune-500-companies-using-hadoop/
5. Francis, M. (2012-04-02). "Future telescope array drives development of exabyte processing". Retrieved 2012-10-24.
6. Garner, http://www.gartner.com/newsroom/id/173191
7. Groundbreaking Ceremony Held for $1.2 Billion Utah Data Center". National Security Agency Central Security Service. Retrieved 2013-03-18.
8. Harris, D., "10 ways companies are using Hadoop (for more than ads)," Jun. 5, 2012. http://gigaom.com/2012/06/05/10-ways-companies-are-using-hadoop-to-do-more-than-serve-ads/
9. Herrmann, J. F., "Open Ocean Surveillance: A combination of new technologies in Earth observation and telecommunication offers near-real-time maritime monitoring." http://www.astrium-geo.com/files/pmedia/edited/r15873_9_openoceansurviellance_gif_10-8_final.pdf
10. Hoppa, R. V., RDML (Select) USN, "NMIO Briefing," National Maritime Intelligence-Integration Office, 15 Feb 2012.
11. http://developer.yahoo.com/hadoop/tutorial/module1.html#challenges
12. http://en.wikipedia.org/wiki/Apache_Hadoop
13. http://gov.aol.com/2012/08/30/are-we-missing-the-big-picture-with-big-data/#?icid=apb1#page1
14. http://hive.apache.org/
15. http://searchbusinessanalytics.techtarget.com/definition/big-data-analytics
16. http://www.cloudera.com/content/cloudera/en/why-cloudera/hadoop-and-big-data.html
17. IBM, "What is big data? — Bringing big data to the enterprise". 01.ibm.com. Retrieved 2013-03-05.
18. IDC. "Big Data Analytics: Future Architectures, Skills and Roadmaps for the CIO," September 2011.
19. Lohr, S., "The Age of Big Data," http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0
20. Margaret Rouse, January 2012: http://searchbusinessanalytics.techtarget.com/definition/big-data-analytics
21. SAS, http://www.sas.com/big-data/
22. Watters, A. (2010). "The Age of Exabytes: Tools and Approaches for Managing Big Data" (Website/Slideshare). Hewlett-Packard Development Company. Retrieved 2012-10-24.

AUTHORS

The mission of the Naval Postgraduate School is to provide relevant and unique advanced education and research programs to increase the combat effectiveness of commissioned officers of the Naval Service to enhance the security of the United States. In support of the foregoing, and to sustain academic excellence, foster and encourage a program of relevant and meritorious research which both supports the needs of Navy and Department of Defense while building the intellectual capital of Naval Postgraduate School faculty.

Authors from the Naval Postgraduate School, Monterey, CA are Dr. Thomas Huynh, Center for Decision, Risk, Controls & SIGINT; Dr. Gary Langford, Department of Systems Engineering; and Dr. John Osmundson, Department of Information Sciences.

In this issue: