SANDIA REPORT

SAND2005-2294
Unlimited Release
Printed June 2005

PACFEST 2004: Enabling Technologies for Maritime Security in the Pacific Region

Report of the Workshop
November 18-19, 2004, Kihei, Hawaii

John B. Whitley, Judy H. Moore, and Craig Chellis

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation,
A Lockheed Martin Company, for the United States Department of Energy's
National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by Sandia Corporation.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865)576-8401
Facsimile: (865)576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd
Springfield, VA 22161

Telephone: (800)553-6847
Facsimile: (703)605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2005-2294
Unlimited Release
Printed June 2005

PACFEST 2004: Enabling Technologies for Maritime Security in the Pacific Region

Report of the Workshop
November 18-19, 2004
Kihei, Hawaii

John Whitley[1] and Judy Moore[2]
Sandia National Laboratories
P.O. Box 5800
Albuquerque, New Mexico 87185-0839

Craig Chellis, Pacific Disaster Center[3]
590 Lipoa Pkwy, Suite #259
Kihei, Hawaii 96753

Abstract

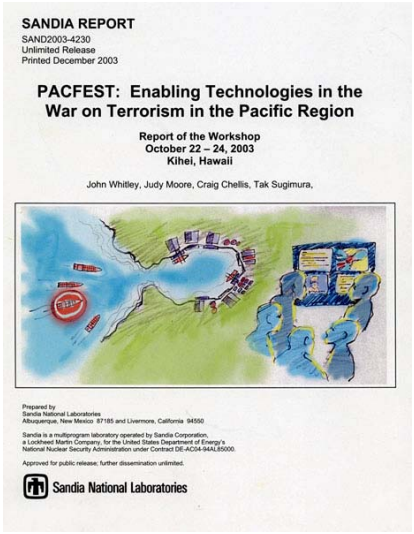
In October of 2003 experts involved in various aspects of homeland security from the Pacific region met to engage in a free-wheeling discussion and brainstorming (a "fest") on the role that technology could play in winning the war on terrorism in the Pacific region. The result was a concise and relatively thorough definition of the terrorism problem in the Pacific region, emphasizing the issues unique to Island nations in the Pacific setting, along with an action plan for developing working demonstrations of advanced technological solutions to these issues. Since PacFest 2003, the maritime dimensions of the international security environment have garnered increased attention and interest. To this end, PacFest 2004 sought to identify gaps and enabling technologies for maritime domain awareness and responsive decision-making in the Asia-Pacific region. The PacFest 2004 participants concluded that the technologies and basic information building blocks exist to create a system that would enable the Pacific region government and private organizations to effectively collaborate and share their capabilities and information concerning maritime security. The proposed solution summarized in this report integrates national environments in real time, thereby enabling effective prevention and first response to natural and terrorist induced disasters through better use of national and regional investments in people, infrastructure, systems, processes and standards.

[1] jbwhitl@sandia.gov
[2] jhmoore@sandia.gov
[3] cchellis@pdc.org

Intentionally Left Blank

Table of Contents

Purpose


SANDIA REPORT
SAND2003-4230
Unlimited Release
Printed December 2003

PACFEST: Enabling Technologies in the War on Terrorism in the Pacific Region

Report of the Workshop
October 22 – 24, 2003
Kihei, Hawaii

John Whitley, Judy Moore, Craig Chellis, Tak Sugimura,

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.

Approved for public release; further dissemination unlimited.

Sandia National Laboratories

In October of 2003 experts involved in various aspects of homeland security from the United States and four other Pacific region countries met in Hawaii to engage in a free-wheeling discussion and brainstorm (a “fest”) of the role that technology could play in winning the war on terrorism in the Pacific region. The result of that exercise was a concise and relatively thorough definition of the terrorism problem in the Pacific region, emphasizing the issues unique to Island nations in the Pacific setting, along with an action plan for developing working demonstrations of advanced technological solutions to these issues (see reference 1).

Since the PacFest 2003 workshop the maritime dimensions of the international security environment have garnered increased attention and interest. To this end, PacFest 2004 sought to identify gaps and enabling technologies for maritime domain awareness and responsive decision-making in the Asia-Pacific region. The “Fest” consisted of two days of intense brainstorming and cataloging of ideas that:

- Brought together a small, international group committed to the vision of regional maritime security through multi-national, multi-agency cooperation
- Provided a collaboration and knowledge sharing environment that stimulated innovation
- Built a proposal for an Advanced Concept Technology Demonstration (ACTD) wherein each coalition country takes on a share of the developmental responsibilities and challenges
- Created a unified approach suggesting follow-on workshops and consultations throughout the region

The workshop occurred immediately following the Asia Pacific Homeland Security Summit and Exposition held in Honolulu, Hawaii, during 14-17 November. The venue for PacFest 2004 was the Maui High Performance Computing Center (MHPCC) in Kihei, Hawaii (on Maui) and was co-hosted by the Sandia National Laboratories Advanced Concepts Group and the Pacific Disaster Center/East-West Center. The Sandia Advanced Concepts Group (ACG) has been chartered to develop solutions to future national security problems that don't yet exist but are on the horizon. Since September 11, 2001, the ACG has focused its efforts toward the "War on Terrorism.” The Pacific Disaster Center (PDC) is a non-government organization (NGO) that provides applied research and analysis support for the development of more effective policies, institutions, programs, and information products for the disaster management and humanitarian assistance communities of the Asia Pacific region and beyond. The common interest of these institutions in the identification and implementation of technology solutions to national security was the genesis of this workshop. About 20 key players involved in counter-terrorism in the Pacific region met to discuss how to jointly develop the technologies that would enable effective defensive and response measures.

The PacFest Process

This “Fest” consisted of two days of intense brainstorming and cataloging of ideas on an off-the-record, non-attribution basis. There were two formal presentations concerning the *Challenge of Maritime Security* and *Maritime Defense in Depth*, with the remainder of the time spent sharing expertise through the small group brainstorm sessions. The brainstorming sessions sequenced through the following six

topical sessions: Requirements and Desired Functionality, Requirements for Information Sources and Processing, Challenges and Opportunities, Creating and Implementing the Ideal System, Prototyping, and Moving Ahead – the Roadmap. (See Agenda in the Appendices).

The process used was a combination of written brainstorming and small group sessions followed by large group discussions. The written brainstorms were carried out on large pieces of poster paper placed on the wall with the session subtopic identified at each station. Participants were given about 30-45 minutes to move about the room and enter their ideas and react to the ideas of others. At the end of this time, a facilitator took the poster papers capturing the ideas of the larger group and worked with the subgroup to: organize by grouping ideas and creating categories; refine by editing, condensing, and clarifying; add new ideas, expand, and enumerate; synthesize by combining diverse concepts into a coherent whole; and finally create an outline report for the plenary session. Each group then selected a person to present the plenary report.

Participation

PacFest 2004 was attended by a small but diverse group of some 20 individuals with an interest in helping Pacific region governments and private organizations effectively collaborate and share their capabilities and information concerning maritime security. The participating organizations were the Ministry of Defence, Australia, the U.S. Department of Defense, the Office of the Secretary of Defense, U.S. Pacific Command, U.S. Northern Command, U.S Coast Guard, U.S. Naval Undersea Warfare Center, U.S. Department of Homeland Security, the East-West Center, ThoughtWeb, Australia, Sun Microsystems, Inc., the Pacific Disaster Center, and Sandia National Laboratories.

This report summarizes the key points and opinions of the participants in the large and small group discussions.

Requirements and Desired Functionality

The first session dealt with identifying the requirements and desired functionality of a system for maritime domain awareness and responsive decision-making. This question was analyzed from four different perspectives; an individual responsible for Port security, an individual involved in maritime commerce, a general view of other maritime users such as fishermen or recreational users, and finally from the viewpoint of an informant to a terrorist cell who wants to pass useful information to a terrorist to further the accomplishment of a terrorist act.

Port security

Several different types of users were identified in this category. These included:

- the captain of the port (US Coast Guard or equivalent),
- commercial port managers (who direct the flow of commerce),
- various government and military port managers (who focus on legal compliance),
- a port facility manager (who may operate the infrastructure), and
- local law enforcement (who would provide local response forces).

All of these users would require access to threat information such as knowledge of emerging methods of attack, threats and events at other local or international ports, and information on who may be conducting surveillance of the port. Access to all threat data such as terrorist organizations, manpower, capabilities (weapons, communications), intentions, history, methods of operations, etc., would be of great value. Information on the port security force(s) such as contact information and authorities/jurisdiction of security forces inside and outside of the port

perimeter would be required, as would the command and control processes of all security response forces. Information and best practices on port physical security measures in areas of port surveillance, cargo tracking, and integrated sensors should be available, as would methods to maintain port access (physical/personnel security). The system should display port management information to allow the user to make an informed trade-off between security and port efficiency (risk management/economic impact). The system should help coordinate customs activities with cargo movement (status capability), display stand-off ship identification and confirmation, along with cargo, crew manifests(s), recent port-of-call history, owner, flag state, and provide overall situational awareness of inbound ships. It should alert the user of dangerous cargo arriving or suspected dangerous individuals.

Commerce/Shipping

The users in this category include both the ship master and the cargo owner. Their major concerns center around efficiency and safety (reduced insurance). For the ship master, key questions that the system should help answer include:

- What are the available port facilities and the expected schedule (including delays)?
- What are the local government regulations and compliance requirements?
- What is the current state of threats in the area?
- How can I support threat mitigation?
- What recourses are available to reduce the threat to my ship?
- How can I call for help?
- How can I assure that my crew is not a threat?
- How can I assure that my cargo is what it is stated to be?
- How can I assure that my ship is seaworthy, safe, and the crew drilled?
- What is the weather in my area/path?
- What is the current status of navigation aids?
- Who has collision avoidance systems – automated ID systems (AIS)?
- How can I perform an efficient load/unload?
- Are there best practices – operations that I should implement?
- Where can I find local knowledge of practices, merchants … (maritime exchange)?
- What is the security level of the destination port?
- How do I contribute to situation awareness – types of threats, how to train crew, who do I tell (systematized)?

For the cargo owner, key questions for the system include:

- How can I contribute to port security?
- Where is my cargo -now (geographically; on ship)?
- What risk factors apply to my cargo?
- What are the insurance and other impacts if I pull into a non-certified port?
- Is theft a concern?
- Is passenger safety/security a concern?
- Can I get passengers checked against watch lists?
- What are current best practices for security procedures and equipment?
- What is my relationship to the other modal/domains (i.e., land transport/air – train and trucks)?

Other maritime users

The category of other Maritime users included local commercial fishermen, ferries, tugs, and various recreational users. Their primary concern would seem to be the impact of the system on their freedoms and civil rights. Would a system requiring monitoring of small boats be an invasion of owner/crew privacy? In general, these users want as little impact as possible from governments on their business in both cost and loss of privacy. However, the system could help supply valuable safety information. For example, the system could indicate exclusion and closed zones, areas that need environmental protection, areas of danger, sensitive operations, weather, navigation aids. Is freedom of movement constrained? The system could involve these users in surveillance: How can I help? – Could I be another set of eyes? – What should I look for? – How do I report it?

What information would be useful to plan an attack?

This terrorist perspective considered the information that would be useful both for planning attacks and for helping facilitate the actual attack. To this end, access to vulnerability and risk assessments would be of high value both in selecting the target and identifying perceived vulnerabilities to exploit. Other valuable information on all local targets would include:

- Details on the port and its operations, especially security measures.
- Descriptive information that might help identify fault lines between agencies/domains that could be exploited to the terrorist advantage.
- Details of port and ship operations, port processes, time-tables, identification of cargo, crew, and ships entering the port.
- Lists of companies that do business in the port that could be used to provide cover for an operation.
- Information on the technologies used for surveillance, access control for port activities and warehouses, operations could help identify weaknesses and provide operational plans.
- Maintenance routines and expected security measures for both ships and the port.
- Details of port and ship processes/organization/technologies.
- General information on the regulations and security culture could help identify vulnerabilities.
- Regional patrol schedules, response capabilities, and the security forces appreciation of the terrorist capabilities and resources would give an advantage to the attacker.
- Information about other illegal activities in region would help the attacker look for leveraging opportunities, as would information on hazardous materials in the port that might be leveraged during an attack.

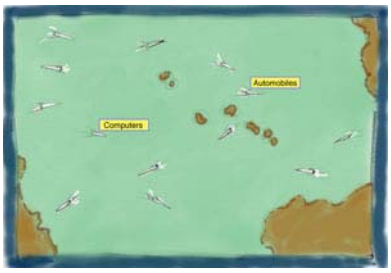
Requirements for Information Sources and Processing

There are currently a number of maritime information systems, either in operation or planned, that could supply data for the Pacific region. The possible sources for this kind of data were brainstormed around the following perspectives:

- Location and what's on each ship,
- Response capabilities (for both terrorism and disasters),
- Threat understanding, detection, and prioritization, and
- Best practices for defense.

Locations and contents of ships

A great deal of location/cargo information is already available for vessels greater than 300 tons. Much of it is proprietary (may be available for a fee) and some of it is in controlled DoD databases which may limit its usefulness. But there also is a significant amount of location/cargo data available from Lloyd's of London. Currently much of the data is only reported when vessels "push" the data to the existing tracking systems. This overall system of "indirect" tracking systems only works with cooperative vessels.



A better solution would be to interrogate vessels directly and thus provide more reliable data. One use of such a system would be to mark "good" vessels and cargo. This would allow defenders to focus efforts on the "unknown" vessels. There are currently no anomaly reports available in existing reporting systems. For licensed international importers and exporters, there are standard manifest (and hazardous material) information requirements and information exchange requirements that could be accessed. One could also tie manifest/crew lists to AIS/GMDSS (Automated ID System/Global Maritime Distress and Safety System) reporting/maritime IFF (Identify Friend or Foe) and require all ships to report via GMDSS or Maritime IFF (this could then be checked with Satellite based AIS).

For vessels less than 300 tons, there is much less data collection in place. There is a voluntary reporting system for pleasure boats, and with the Vehicle Identification Number (VIN), name, and port of call one could access owner and detailed ship information. There was some discussion of a future global navigation system that would track smaller vessels, but the PacFest 2004 participants were uncertain of its status. There also exists a DoD database (watch list) of suspicious vessels that could be accessed. One novel idea would be to track fuel purchases as an indirect indicator of small vessel activity.

Response capabilities (terrorism and disasters)

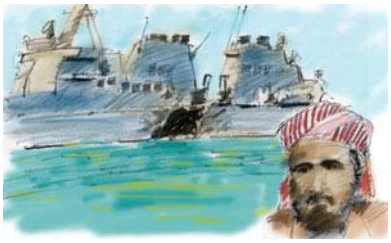
Numerous types of information feeds and resource management tools are already in place in various emergency management systems that could be used for data. These usually include communications among various participants, their agencies, and an agreed language. Information is also usually available on the status of the "scene," including infrastructure, casualties, atmosphere contamination, response units, shelter locations, and hospital availability (beds, supplies, expertise). Information on critical infrastructure is sometimes available including the important sites and status of capability. For many International/Regional/National/State/City units, there exist response plans (National Incident Management System (NIMS), National Response Plan(NRP)), communication and control plans, public information/media plans, locations and responsibilities of all incident control centers, and maps of jurisdictions. In a terror event, desired data would include:

- Type of weapon (nuclear/chemical/biological)
- What hazard is in environment? (radiation, heat/fire, chemical or biological agent)
- Atmospheric data – wind at surface and at high altitude, humidity, precipitation
- Plume data – downrange impacts
- Shelter locations
- Local/State/Federal response capabilities and whom to contact
- Remote sensors on scene transmitting via data link to command center
    - Infrared (heat/fire)
    - Air sampling

- Hospitals/medical supplies; hospital bed status and availability
- Evacuation options, if any
- Shelter in place options
- Real-time status of roads to scene
- Aircraft availability and capability
- Public communication information
    - Prepared packets
    - Trusted sources
    - Government communication channels

Threat understanding, detection, and prioritization

The participants identified numerous information feeds that could supply data on the terrorist threat. Both open and restricted (law enforcement sensitive) information is available from various law enforcement data sources. The system should be able to enable collaboration between countries on topics such as risk mitigation and information sharing built upon Interpol.
It might be possible be gain access to some level of national intelligence data. The International Chamber of Commerce (ICC) provides piracy data through the International Maritime Bureau (IMB). Lloyds of London also provides maritime incident reports, as do other international finance and commerce sites. It also is important to understand what terrorists are using the maritime environment for, such as logistics, concealment, and delivery.



A challenge will be facilitating communications with other system users (language translation). News feeds provide a wealth on information on incidents and developments. Processing and accessing the information will require some type of access control system, perhaps a multilevel security system (MLS). Cross data base/data mining and anomaly detection will be key features to allow for a smart push-pull system tailored to user needs and access privileges. A system that could access modeling codes to show predicted impacts of the users actions would be very useful, as would counter-terrorism databases that map terrorist connections. The system should interface with decision aid/support systems (not predictive). Finally, access to organizations that study terrorism (Government, NGOs, Universities, Private) would be vital. This access should include the ability to "task" the organization with questions that would receive answers in a timely manner. The system should access reports from groups monitoring terror group communications web sites and should use the best information/cultural resources – local nationals from same cultures as terrorists, for understanding of threat, getting intelligence on local activities, and showing linkages for informant recruitment to allow penetration of terrorist networks.

Best practices for defense

One of the major features of the envisioned system would be to provide a powerful source of best practices information for maritime security. There are numerous guidelines and processes available in the area of risk management, especially from professional societies. Lloyds and Petrospot (UK) provide technology assessment services and information. Red teaming is a developing field that could help improve defensive capabilities. There are several sites developing vulnerability analyses with various types of computer codes available.
Information about technologies for interoperative communications and near-real-time decision support is becoming available and could be part of the information system. Effects modeling by universities and the military could be accessed. The system should take advantage of research

that has been conducted on “human-in-the-loop” systems when considering automated advice and guidance on decision options. The USS Cole provided many lessons learned. As countries develop doctrines to be applied on an international basis they should be shared along with rules of engagement. All partners should also share options for a good offense in the maritime environment are developed.

Challenges and Opportunities

The purpose of this PacFest session was to collect ideas on what would constitute the major challenges to implementing the basic features of the envisioned system(s) and what existing programs should be leveraged. Thoughts were collected around the areas of:

- Encouraging collaboration,
- Policies necessary for sharing, and
- Existing technologies and initiatives.

Encouraging collaboration

The major challenges in encouraging collaboration identified by the group were differing cultures, languages, and obtaining adequate and stable funding. As with any multi-national effort, there will be fear of one country dominating the requirements and of conflicting national goals and interests. There is also often reluctance to adopt a formal sharing policy.

The participants felt that many positive developments today indicate that this effort could succeed. The existence of international meetings such as Asia-Pacific Homeland Security Summit, the USG's Senior Steering Group for Marine Domain Awareness and its outreach working group, USPACOM's Multinational Planning Augmentation Teams (MPAT), other programs that involve the exchange of personnel (at least personal meetings) and the exchange of technology, and the successful programs such as World Intellectual Property Organization and the Law of the Sea all provide examples of international collaboration.

The group felt that there must be a mindset change from “what’s mine is mine, what’s yours is negotiable,” to “we are all in this together, we all have a common interest, and it’s a global community/economy.” The system must be able to demonstrate benefits (especially economic – if I give information, what do I get?) and demonstrate that it can meet a great need that the players are allowed to self discover. These efforts start with small steps and build trust and confidence among the players.

The U.S. Joint Interagency Task Force model for interagency cooperation could provide a possible framework. Any successful program will be a long process of dialogue, training, and exercises, designed both to show partners the benefits and to develop skills. Collaboration needs to be integrated with operational systems that generate direct benefits to the participants, creating sustainability and motivation to contribute. There will be a need for multi-national leadership with a governing body for the knowledge sharing/collaboration environment. Some felt that there is a need for UN leadership, but others disagreed. There is always policy inertia that must be identified and overcome. In the U.S., the Coast Guard will have to provide much of the resources, but it would be best that the U.S. not lead the international effort as in the Regional Maritime Security Initiative (RMSI).

Policy for sharing

There are many areas that will require policy development for the required level of information sharing to be successful. These include trade (industrial) secrets, Department of Defense security classification, public policy on the disclosure of “sensitive” information such as

environmental impacts, fishing activity, and threat type and status. There is also the question of where and how the UN would fit into this system. The major obstacles include conflicting cultural values and norms, language, individual national or organizational goals, the basic competing interests between nations, issues of the classification of intelligence information, funding, and the existence of "Rice Bowls" where this new effort may threaten the existence of an established activity. Agreeing on the policies to allow for joint funding for joint efforts will also be required.

There are many existing opportunities that could be referenced by this initiative. All countries have a common interest in making money and defeating terrorists. The set of existing international expos/workshops/conferences could be used to further this exchange, as could ongoing efforts to manage the globalized economy with its associated trade rules (WTO).

Also, the Senior Steering Group for MDA is working on common standards for MDA development. Perhaps a good first step would be to share the metadata of this effort. This would benefit everyone, aid understanding, improve the consistency and usability of data, and help create the environment to negotiate exchanges of data. This might make strategic use of the maritime security crisis to push the regional cooperation envelope.

Existing technologies and initiatives

The consensus of the group was that most of the basic technologies for this type of application already exist. What is needed is an application that can fuse the existing data. There are ample opportunities to make this happen through government/private industry collaboration. Competition could be used to encourage work toward a common goal where everyone, both governments and business, can benefit. It is a problem that no one knows exactly what they want, but that there are always lots of companies that think they know what you want. What is needed is cooperation between companies, a workable solution to the information classification problem, and supportive import/export policies. Another problem is the existence of legacy systems that may be too expensive to replace (i.e. Global Command and Control Systems (GCCS)) and the fear of giving away or losing proprietary technology. The system will need strong metadata management.

The following is a list of available technologies (or initiatives) that the participants felt could contribute to this effort:

- Science, Engineering and Technology Unit, National Security Division, Dept of the Prime Minister and Cabinet, Australia
- Automated ID System (cooperative emitters, can be turned off)
- JHOC/SCC (Joint Harbor Operations Center, Sector Coordinating Council)
- DHS Motivation & Intent Initiative
- UN doing Marine Electronic Highway (MEH) – mostly about safety
- RECAAP – Japanese led system for anti-piracy
- IDSS (integrated decision support system) – PDC system
- Extraction Transformation and Load tools (ETL)
- Knowledge storage systems community products
- Decision support
- Enterprise architecture
- Biometrics/security authentication
- RFID (radiofrequency identification)
- Pattern analysis

- National MDA effort
    - National Security Presidential Directive (?)
    - COP working group
    - Technology group
    - Intelligence working group
    - Outreach working group
    - Strategy & policy working group
    - Budget working group
    - Legal working group
- Operational Enduring Friendship (OEF)
- RMSI (Regional Maritime Security Initiative)
- PSI (Proliferation Security Initiative)
- ISPS (International Ship and Port Facility Security)
- CSI (Container Security Initiative)
- SUA (suppression of unlawful acts) - UN
- UN CLOS (UN council laws of sea)
- IMO (International Maritime Organization)
- ASEAN (Association of Southeast Asian Nations)
- ARF (ASEAN Regional Forum)
- APEC (Asian pacific economic cooperation)
- FPDA (Five power defense arrangements)
- North Pacific Heads of Coast Guard agencies
- ABCA (Australia Britain, Canada, America)
- NAASC/WASC (North America air security council/wide area surveillance council)
- US Army Pacific's (USARPAC) Chemical/Biological/Radiological/Nuclear/Explosive (CBRNE) multi-agency training calendar

Creating and Implementing the Ideal System

The participants were divided into two groups for this exercise and asked to consider the features of an ideal system that was *optimized* specifically to facilitate either the transmission of the best tactical information for interdiction <u>*or*</u> one optimized to manage information from diverse sources and for diverse users.

Best tactical Information for Interdiction

The primary users to consider for such an optimized system would be a multi-national blend of civilian law enforcement, military, and private businesses or persons. The system would need a powerful multi-level security policy with either a real time access system or perhaps two systems -- one a web based lowest common denominator and the second a classified system. The system could help fight piracy, but would not deal with root causes. Its real focus would be on counter-terrorism. It would implement regional doctrine development and perhaps follow the MPAT model, where the Multinational Planning Augmentation Team is a "cadre of military planners from nations with Asia-Pacific interests capable of rapidly augmenting a multinational force (MNF) headquarters (HQ) established to plan and execute coalition operations in response to military operations other than war (MOOTW)/small scale contingencies Model." The MPAT model was used successfully in the multi-national response to the recent Indian Ocean Tsunami disaster. Another working example is the ASEAN Regional Forum (ARF), which tries to enhance stability and find advantageous multilateral solutions. China has welcomed ARF collaboration and has a proposal for defense dialogue.

The group generated three terrorism scenarios to "storyboard" how the PacFest system could facilitate counter-terrorism activities. In scenario 1, the first event flagged by the system was a non-specific intelligence report of terrorists and pirates operating in a region. The system response would be to generate a non-specific notice to relevant users in the region. The next event in the sequence was the detection of a large commercial ship being approached by fast vessels in open water. The system sensor network observed and reported that this ship was being approached. The system then generated an alert to the appropriate command center and supplied the following information:

- Name, cargo, location, flag, contact
- Security plan for ship
- Local response options

The command center then warned the ship's captain and alerted the appropriate law enforcement/military and consequence management units. If a terrorist incident then occurred, the system would transition to a consequence management mode to help facilitate the response.

In scenario 2, the triggering event was a report of a known bomb maker traveling to a specific area. The system responded to this report by flagging the event and generating an alert to the appropriate users, providing them with a suggested distribution list (such as local leaders) of those that could be involved in finding the individual. It also provided specifics on techniques used by this person and his organization, and generated an All-Points-Bulletin (APB) in multiple languages.

In scenario 3, the triggering event was a report received from an unknown person seeing a personal submersible being tested. In this case, the system made associations with other possible relevant data, provided information to an expert group to make a technical assessment, and generated an appropriate threat alert based on the analysis.

Ideal System for Diverse Sources

The objective of a design idealized around the concept of maximum usefulness for diverse sources and users is to create a common operating picture that provides effective understanding of the stakeholders' area(s) of interest as defined by an agreed rule-set. The system must be an internet-based system organized to access the relevant categories of information. Major features would be:

- Capable of data mining in multiple sites and the ability to come back with specific information (processes)
- Stakeholders could access system independently, with ID controls for categories of information; capacity also for users to contribute data (with appropriate controls) which then becomes available to other users
- Could be tailored for varied users
- Could handle compartmentalized (classified or proprietary) information
- Could handle (translate) multiple languages
- Includes a public outreach system to encourage public participation and input
- Revenue based on fees from users (e.g., governments, corporations, etc. – scaled fee schedule)
- Participants solicited incrementally, via other participants (e.g., Indonesia by Singapore); use of targets (events) of opportunity, confidence-building processes
- Host and startup to be provided by U.S. (and consortium of "willing" partners)

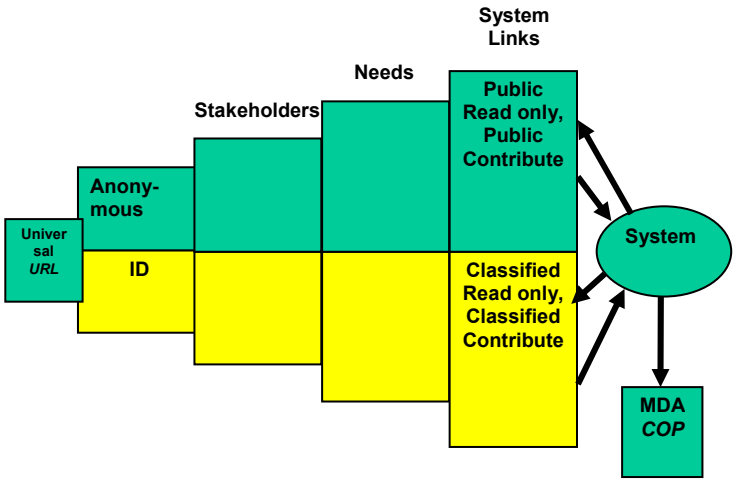


Figure 1. System concept diagram showing the two paths through the system, one as an anonymous user, the other as a registered user with classified access.

Prototyping

During this session, the group reviewed several operating (or proposed) systems that could form the basis for realizing the ideal system. First, the USPACOM's Asia Pacific Area Network (APAN) and Virtual Information Center (VIC) provide an unclassified, open source clearinghouse of public data, obtaining feeds from multiple sources. This system has a staff of analysts that create reports and "primers" on relevant subjects and are supported by a military contract. They have about three people involved in network and membership management, and maintain a first level of access control. This contrasts to the seventeen levels of access they maintain for a CBRNE site.

The Pacific Disaster Center (PDC) has state-of-the-art capabilities for Geographic Information Systems (GIS) analysis and for real-time displays of events that could be integrated into the system's display. ThoughtWeb, Inc. provides a development framework that focuses on personalized, prioritized, pro-active push of information to the decision maker. The USG's Maritime Domain Awareness program (MDA) is collecting real-time monitoring data, and the Maritime Tracking System Concept is being proposed to gather real-time information on ship locations. The PacFest group's conclusion was that the kind of capabilities that we need do exist -- the technologies are there. If we could marry these together, we could have a viable system without a large development program.

Moving Ahead – the Roadmap

The group was asked to help develop a roadmap on how to proceed with the idea. The first suggestion was to not look to the military to lead the process; a focus on law enforcement and paramilitary initiatives will be a better vehicle for bringing the region together. It was felt that it was imperative to find means to present the demonstration prototype to multiple forums, e.g., CSCAP (Council for Security Cooperation in the Asia Pacific), the Counter Terrorism Task Force at APEC, or its associated program STAR (Secure Trade in Asia-Pacific Region). It would also be very powerful to get a sponsor from ASEAN (e.g. Malaysia) for a concept demonstrator to the ARF. It might even be possible to build on the developing disaster

management system in Malaysia – a Regional → Country → City model. Potential target audiences for the proposal included:

- ARF CBM conference – March 05
- Knowledge Fusion – Malaysia, Singapore, Australia, Indonesia, U.S. - Maritime in Senior Officials' Meeting (SOM) – meeting about the 3rd week in January 05
- Government + private sector + IMO (International Maritime Organization, UN body)
- RECAAP may also be a good place to present

A set of suggested actions were developed:

- Two-page write-up on concept demonstrator by early 2005.
  - Murray, Reitz, Chellis, Whitley
- Brockett and Thomas to brief USPACOM S&T Advisor
- Thomas to brief IMO contact, IALA (International Lighthouse Association)
- Brockett to also brief IMO contact
- Support ARF conference with our ideas
- Support technology Working Group (WG) with data
- Support strategy and policy WG with ideas/avenues of approach
- Develop limited objective experiments with our partners to develop/exercise cooperation with them and demonstrate to others (countries and organizations) the benefits of cooperation.
- Coordinate with/support CMA (Cooperative Maritime Awareness) ACTD (PACOM initiative, USPACOM S&T Advisor)
- Determine effective access methods (relationships, trust) to operational data, e.g. shipping companies, ports, etc.
- Build a concept demonstration integrating multiple existing products
- Demo disk for briefing/marketing of concept
- Investigate the ASOC and associated effort (PPMI?)
  - JHOC San Diego – Rob Keller – ASOC
  - SSC SD Dr. Paulette Murphy – PPM

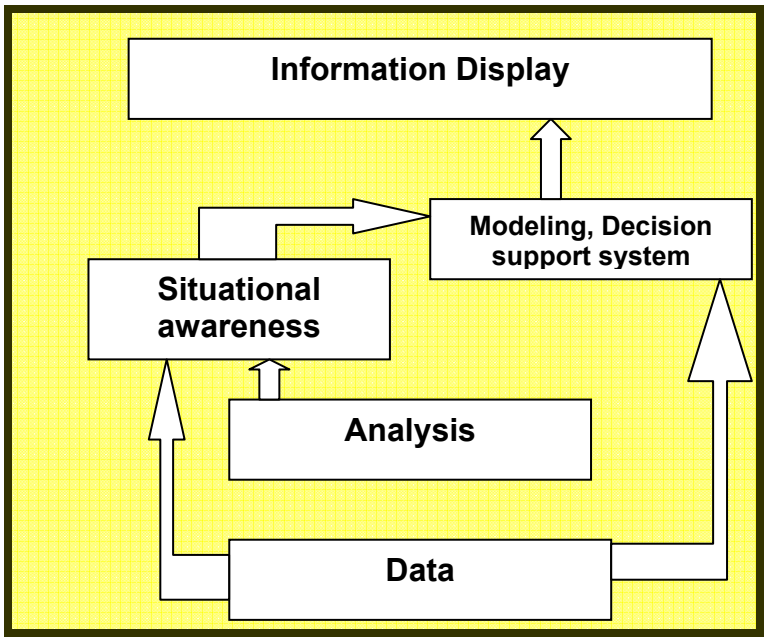


Figure 2. General system framework.

Summary

The PacFest 2004 participants concluded that the technologies and basic information building blocks exist to create a system that would enable the Pacific region governments and private organizations to effectively collaborate and share their capabilities and information concerning maritime security. The system would be focused on protecting our ports, commerce, and citizens and our different interests, values, professions, disciplines, and beliefs. The objectives would be a multi-national, smart collaborative network enabling people with diverse interests and knowledge to quickly learn from one another and to detect and take effective action in response to disparate events and observations; in short, a system that would:

- Be a 'go-to' place for people interested in counter-terrorism information and issues
- Give decision makers a personalized, prioritized, proactive push of information
- Be used by a broad range of public and private security-related institutions
- Leverage existing efforts in collecting and analyzing open source information
- Provide a common operating picture that promotes effective understanding of the stakeholders' area(s) of interest as defined by agreed rules

The system would be Internet based and organized to access relevant categories of information. It would be simple and scalable to account for user limitations in knowledge, bandwidth, and training. It would be capable of data mining in multiple sites and returning specific information (processes). It would be independently accessible by users, with ID controls for categories of information; users would be able to contribute data, with appropriate controls, which then becomes available to other users. It would also be able to appropriately handle open, classified or proprietary information, would include features to encourage public participation and input, and would deliver added value from underlying applications and databases.

The suggested approach is to pursue an Advanced Concept Technology Demonstrator (or similar proposal) focused on addressing these requirements. Such an approach would implement a security solution reference architecture that enables open integration with value-adding components from diverse technology leaders. A pre-integrated suite of tools and contextual models would provide easy user access through a common entry point, joint databases and intelligent, real-time analysis of content. The scope of the system would include:

- Collaboration and knowledge sharing
- Vulnerability assessment tools/processes
- Response capability assessment
- Threat detection and prioritisation
- Disaster awareness and response
- Issue identification and management

It is important to recognize that the system would NOT be a maritime shipping command and control system. It could, however, draw upon summary information from many of the existing and planned systems of this type. Neither would it be an incident command system for real-time first-responder, law enforcement, or military operations. Again, summary reports from such systems might be displayed, however.

To avoid information overload to the user, the system would be based on a personalized Web portal with multi-level security. The information presented to the user would be based on an "importance profile" and "personal key words" and would change daily. It would have shared/common data standard (information) products and processes and a common situational awareness picture. *Integration of all these elements would be key.* It should support solutions at many levels, from local to enterprise level -- for projects, teams, and agencies -- to national, regional and international programs and the broader Maritime security community.

Main potential contributors to the Prototype could include:

- ThoughtWeb, Inc.:
  - Integrating platform
  - Processing of information sources and personalization
  - Information push where required
- Asia-Pacific Area Network/Virtual Information Center
  - Open source information and analysis
  - Subject matter primers
- Pacific Disaster Center
  - Integration of geospatial awareness and collaboration tools
  - Hosting of server
- MDC/CMA
  - Real-time maritime awareness information

In summary, the proposed solution would integrate national environments in real time which would enable effective prevention and first response to natural- and terrorist-induced disasters through better use of national and regional investments in people, infrastructure, systems, processes and standards.

Acknowledgments

We would like to thank the Maui High Performance Computing Center and the Pacific Disaster Center for the use of their facilities for this workshop and for their logistic support of the event. Ken Miller, a contractor to Sandia National Laboratories, created all the artwork. The design of the workshop sessions was the work of Judy Moore and John Whitley. Sandia is a multi-program laboratory operated by Sandia Corporation, a Lockheed Martin Company for the United States Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000. The Pacific Disaster Center (PDC) is a public/private partnership sponsored by the Department of Defense through Cooperative Agreement #DASW01-02-2-0001 with the East-West Center, which designates it as Managing Partner of the PDC.

Appendices

List of Participants

Name	Organization
Dick Baker	East-West Center
CAPT. Steven Brockett	U.S. Pacific Command, Joint Interagency Coordination Group for Combating Terrorism (JIACG/CT)
Josko Catipovic	Naval Undersea Warfare Center
Craig Chellis	Pacific Disaster Center (PDC)
Allen Clark	Pacific Disaster Center (EWC)
LCDR. Greg Coupe	USNORTHCOM, Interagency Coordination for Law Enforcement and Security
Jack Foidl	Department of Defense, Office of the Assistant Secretary for Network Information and Integration
Joe Harris	Sandia National Laboratories, Advanced Concepts Group
Gary Jones	Sandia National Laboratories (Singapore Programs)
Mick Martin	Industry Director, Sun Microsystems, Inc., Australia
Tom Martin	Department of Homeland Security, Science and Technology Directorate
Judy Moore	Sandia National Laboratories, Advanced Concepts Group
Chris Murray	ThoughtWeb, Inc., Australia
Earnest Paylor	Department of Defense, Office of the Assistant Secretary for Network Information and Integration
John Reitz	USPACOM Asia Pacific Area Network (APAN)
Guy Thomas	Science & Technology Advisor, Maritime Domain Awareness, U. S. Coast Guard
CAPT. Artie Walsh	Chief, Office of Integration and Coordination, U.S. Coast Guard
Peter West	Director of Domestic Security Department Defence Special Interest Maritime Security, Australia
Allan White	ThoughtWeb, Inc., Australia
John Whitley	Sandia National Laboratories, Advanced Concepts Group

Agenda

Wednesday, November 17

1800 – 1930 Evening Social & Jumpstart for Discussions (Wailea Marriott)

White board question: What are your greatest concerns about threats to maritime activities in the Pacific region?

Thursday, November 18

0800 - 0830 Check-in, Continental Breakfast
0830 - 0900 Welcome, PacFest 2004 Purpose and Administrative Details
0900 - 1000 Background Presentations:

- *The Challenge of Maritime Security - USPACOM*
- *Maritime Defense in Depth - OSD/HD*

Break

1015 – 1030 Overview of the Agenda and Discussion of Brainstorming Rules

Developing a system for maritime domain awareness and responsive decision-making

Session I - Requirements and Desired Functionality
1030 – 1100 Written Brainstorm
Collecting ideas for these subtopics:

- Port security
- Commerce/Shipping
- Other maritime users
- What information would be useful to plan an attack?

1100- 1200 Sub-Group Sessions
Organize, refine, add, synthesize and create a report for the plenary session
1200 - 1330 Plenary Session & Working Lunch -
Reports from each group and coalesce to create a unified view

Session II - Requirements for Information Sources and Processing
1330 – 1400 Written Brainstorm
Collecting ideas for these subtopics:

- Location and what's on each ship
- Response capabilities (terrorism and disasters)
- Threat understanding, detection, and prioritization
- Best practices for defense

1400 – 1500 Sub-Group Sessions
Organize, refine, add, synthesize and create a report for the plenary session
Break

1515 - 1615 Plenary Session
Reports from each group and coalesce to create a unified view

Session III - Challenges and Opportunities
1615-1700 Written Brainstorm

- Encouraging collaboration
- Policy for sharing
- Existing technologies and initiatives

Friday, November 19

0800 - 0830 *Check-in, Continental Breakfast*

Session IV - Creating and Implementing the Ideal System

0830 - 930 *Sub-Group Sessions*
Four groups – each work to develop a vision of what they would want and how to contribute:

930 – 1030 *Plenary Session*
Reports from each group and coalesce to create a unified plan

Break

Session V - Prototyping

1045 -1130 *Walk through a demo*

1130 -1215 *Break into groups to discuss the demo and collect feedback.*

1215- 1315 *Working Lunch - Demonstration of Asia-Pacific Area Network (APAN) Maritime Security portal.*

Session VI - Moving Ahead – the Roadmap
Bringing all of the ideas together to develop the plan forward

1315-1345 *Written Brainstorm– connect info sources to analysis to user interface*

- *Connect User to Processing to Info sources*

1345-1445 *Plenary Session*
Large group discussion to refine and create a unified view

Break

Closeout Session - Path to the Ideal System

1500-1600 *Group discussion, summary, and action items*

Suggested Readings

1. John Whitley, Judy Moore, Craig Chellis, Tak Sugimura, “PACFEST: Enabling Technologies in the War on Terrorism in the Pacific Region,” SAND2003-4230, December 2003

Evening discussion question

During the social event prior to the start of the meeting, the participants were asked to respond to the following question: “What are your greatest concerns about threats to maritime activities in the Pacific region?” The following responses were collected.

- Use of maritime transport assets-ships, containers, crews, passengers-to introduce WMD into the U.S. and allied countries--the maritime WMD delivery system.
- Piracy and use of ships as a weapon in a crowded port.
- Getting an international protocol that requires non-solar ships and boats to have automatic identification systems installed and operating.
- That we will overreact and bankrupt our economies.
- Terrorists close Long Beach and at least one other west coast port (all 4?)
    - Mines?
    - Sarin?
    - Anthrax?
- Merging IMO's future global navigation system with Mandatory Ship Reporting systems and passenger and crew identification systems.
- Creating a protocol for mandating biometric identification of both maritime workers and passengers that can be crosschecked with terrorist databases.
- That the government will create another bureaucracy to "deal" with the "problem."
- A small vessel and a rudimentary device that is generally not tracked until it is in port. Once in the harbor, it explodes its device.
- In many Pacific countries the release of a disease could cripple the agricultural industry.
- The lack of inspection of sea-born connexes (between 1-5%) is of serious concern.
- If nuclear waste was brought in a lead-lined container and exploded it would destroy a city's life and livelihood, i.e. Sydney Harbor.
- Compromising security at container terminals such as PSA (Singapore), our shipping to the west coast of the U.S. and other ports.
- Denial of passage in the Malacca Straits.

Distribution:

25 Pacific Disaster Center
Attn: Craig Chellis
590 Lipoa Parkway, Suite 259
Kihei, Maui, Hawaii 96753

1	MS0839	Gerold Yonas, 16000
10	MS0839	Judy Moore, 16000
10	MS0839	John Whitley, 16000
1	MS1201	Jim Gosler, 5004
1	MS0961	Joe Harris, 14020
1	MS9018	Central Technical File, 8945-1
2	MS0899	Technical Library, 9616