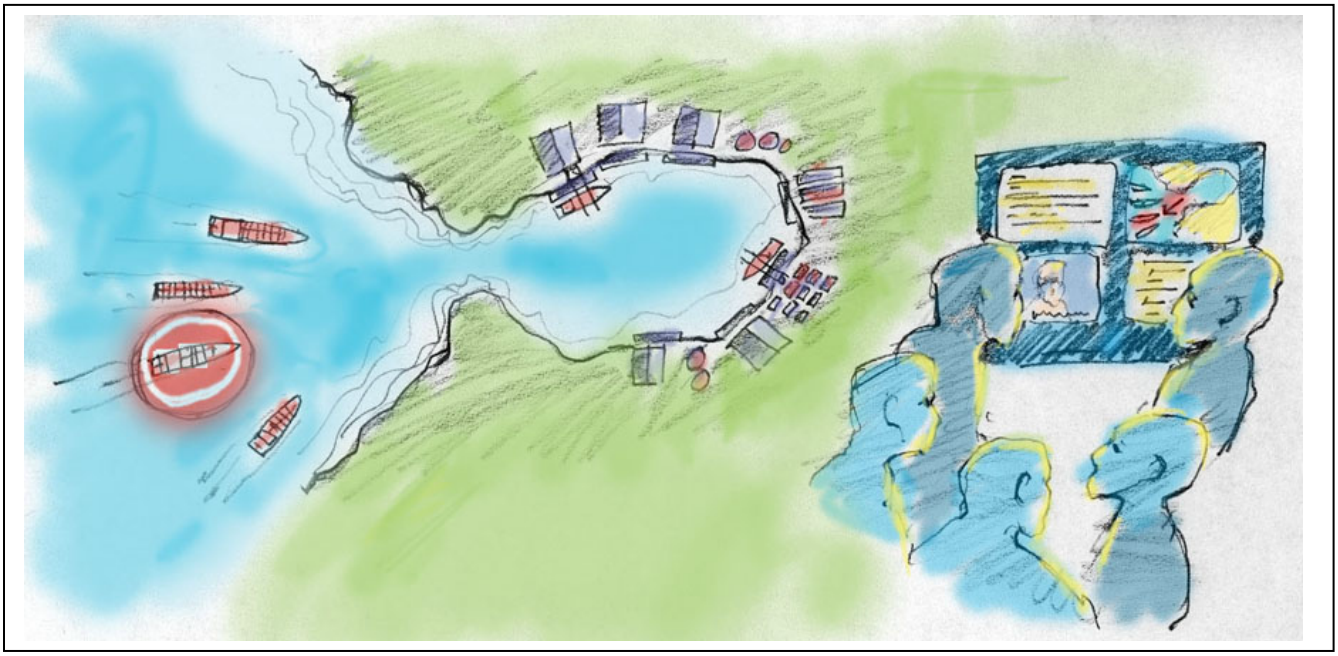
SANDIA REPORT

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.

Sandia National Laboratories

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.doe.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

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 and Judy Moore
Advanced Concepts Group
Sandia National Laboratories[1]
P. O. Box 5800
Albuquerque, NM 87185-0839

Craig Chellis
Pacific Disaster Center[2]
590 Lipoa Parkway, Suite 259
Kihei, Maui, Hawaii 96753

Tak Sugimura
Maui High Performance Computing Center[3]

Abstract

On October 22-24, 2003, about 40 experts involved in various aspects of homeland security from the United States and four other Pacific region countries meet in Kihei, 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 this exercise is 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 demonstrators of advanced technological solutions to these issues. In this approach, the participants were asked to view the problem and their potential solutions from multiple perspectives, and then to identify barriers (especially social and policy barriers) to any proposed technological solution. The final step was to create a roadmap for further action. This roadmap includes plans to: 1) create a conceptual monitoring and tracking system for people and things moving around the region that would be "scale free", and develop a simple concept demonstrator; 2) pursue the development of a system to improve local terrorism context information, perhaps through the creation of an information clearinghouse for Pacific law enforcement; 3) explore the implementation of a Hawaii based pilot system to explore hypothetical terrorist scenarios and the development of fusion and analysis tools to work with this data (Sandia); and 4) share information concerning the numerous activities ongoing at various organizations around the understanding and modeling of terrorist behavior.

[1] jbwhitl@sandia.gov
[2] cchellis@pdc.org
[3] tak.sugimura@mhpcc.hpc.mil

Table of Contents

Purpose

The events of September 11 have dramatically increased the requirements and expectations placed on Homeland security, both for the United States and for its allies. Coastal protection is particularly challenging, with many large metropolitan areas located near the oceans. Islands add additional vulnerabilities, with large exposures, remote locations, and limited population relocation options. In general, island infrastructures are less robust than that on the mainland and create unique vulnerabilities. The Pacific region is one of particular concern, both because of its significance in American history (think of the impact of a second successful attack on Pearl Harbor) and the increasing presence of hostile actors in this area. How will the US and its allies provide protection or respond to an attack on its territories? The successful defense of this area from terrorist attacks will require sensors, information tools, procedures, processes, and, most importantly, collaboration between allies.

To further this effort, the Sandia National Laboratories Advanced Concepts Group, the Maui High Performance Computing Center, and the Pacific Disaster Center co-hosted this workshop, PacFest, which brought together about 40 key players involved in counter-terrorism in the Pacific region to discuss how to jointly develop the technologies that would enable effective defensive and response measures.

The PacFest Process

This "Fest" consisted of two and a half days of intense brainstorming and cataloging of ideas on an off-the-record, non-attribution basis. There was only one formal presentation concerning the status of terrorism in the Pacific region, 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:

I. What is unique about Islands and the Pacific region from the perspective of vulnerabilities, from the perspective of the attacker, from the perspective of the defender, and from the perspective of designing a hardened infrastructure?
II. What role could technology play in the war on terrorism in the Pacific region from the perspective of 1) an individual trying to detect and interdict a terrorist event, 2) a defender, 3) a responder, and 4) a person in charge of recovery?
III. In taking a system view, what is the ideal system that would be required to win the war on terrorism? Here, each group worked to create a solution optimized from the viewpoint of 1) an interdiction team, 2) a defender team, 3) a responder team, and 4) a recovery team.
IV. In session IV, the barriers to achieving this vision were collected from the viewpoint of 1) a private citizen, 2) a business, 3) a government, and 4) a non-government organization.
V. In this session, any technology barriers, required breakthroughs, and existing leverage points were identified.
VI. The final session developed a roadmap of specific actions that would help lead to the implementation of some part of this vision.

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 creating categories and grouping ideas; 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

The workshop, co-hosted by the Maui High Performance Computing Center, the Pacific Disaster Center, and Sandia National Laboratories' Advanced Concepts Group, was held at the facilities of the Maui High Performance Computing Center and the Pacific Disaster Center in Kihei, Hawaii. 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 Maui High Performance Computing Center (MHPCC) is a national supercomputing resource that provides world-class, scalable parallel computing capability to the research, science, and war fighter communities. 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.

PacFest was intended to pull together a small but diverse group of individuals with an interest in dealing with terrorism in the Pacific region. There were participants from four countries besides the United States, namely Australia, Singapore, Fiji, and Palau. The U.S. institutions represented in addition to the three hosts included the Department of Defense, the Department of Homeland Security, the Pacific Command, the Navy, the Army, the East-West Center, the Federal Emergency Management Agency (FEMA), the Hawaii State Civil Defense Agency, the Center of Excellence in Disaster Management and Humanitarian Assistance, the Hawaii State Department of Defense, the Hawaii National Guard, and the Asia-Pacific Center for Security Studies, ACS Defense, Inc., and ThoughtWeb, Inc.

This report is an attempt to summarize the discussions held in large and small group sessions with the intent to capture the key points and opinions of the participants.

Unique Issues of Terrorism for the Region

Most of the unique issues of terrorism in this region identified in the first session revolve around the fact that the region consists of many small islands, separated by vast ocean space, with many governing bodies and with economies dependent primarily on tourism and agriculture.

From the **point of view of the terrorist,** these are remote locations with highly interdependent societies. There will be no easy escape, for example, for victims of a biological attack - quarantine might be the best that can be done, and resupply after attack will be hard. It will be easy to create panic on an island and attacks here could easily cascade to a global impact.

The **vulnerabilities** for the region are great. The geographic issues drive many concerns. The region consists largely of numerous islands with many points for transfer of people and goods. Isolation and remoteness will make logistics difficult for providing backup/recovery.

The economies are highly dependent on only two industries – tourism and agriculture. The region also has "shadow economies" such as drug trafficking with "charities" possibly used as conduits for illegal transfer of money.

There are many strong relationships with western institutions, yielding many symbolic targets against the West. Weak government structures, government corruption and lack of effective laws and enforcement of laws for investigation and pre-emption of terrorist activities and money laundering are concerns. There is limited cooperation between governments, especially related to maritime security, and security at ports of entry is not very strong. Also the region has limited capabilities in technology and highly skilled workers.

Defense of the region will need to be adaptable and flexible with international efforts in some realms. It will need to incorporate individuals as well as government institutions and military. The challenges are the vulnerabilities in shipping, and the lack of a good communications infrastructure for the region given the large area to defend with wide separation among resources for defense. The institutional and governmental challenges are also great – with very different approaches to the allocation of resources relative to other national priorities. The use and sharing of intelligence is globally problematic – across the boundaries of local, state and federal and international agencies – – but amplified in this region with so many nations of varying sizes involved. The rules of engagement are even unclear across this disparate collection of nations.

From the **Responder View,** the issues revolve around the geography challenges and the logistics problems that these impose in addition to the potential for multi-nation coordination in an ad hoc environment. The "tyranny of distance" will create obstacles for effective response from more than one island. This drives the need for stockpiling in preparation for possible events. Evacuation will likely not be an option for small islands so that quarantine is the likely response. With the exception of plans in advance for special international events, there is no planning for coordinated response in the region. Since time is of the essence in effective first response, planning, training and standardization of processes are of prime importance. The lack of this kind of planning and commonality of procedures and processes will make effective response very difficult to attain. The lack of interoperable communications among responders from different nations, technologies, languages and protocols will also limit response. The security of responders on foreign soil will also be an issue should multinational response be required.

Role of Technology in Addressing Terrorism

The second session dealt with the identification of the various roles that technology could play in the war on terrorism.

Enabling interdiction will require the use of "special" intelligence sources including signal intercepts, imaging, and human intelligence gathered by specified agents, as well as "open" sources. The sharing and classification of this data is a continuing issue between government agencies and is even a larger issue across national boundaries. Realizing multi-level security has long been a dream of the information assurance community. In fact, a risk analysis of the impact of NOT sharing data should be included in any study of information security. Reliable machine translation including the unwritten "tone" of a message has not yet been achieved and there are no accelerated language learning tools. Open source data is often difficult to validate and the security of the "feeder documents" necessary to obtain key documents such as passports is often poor. Enhanced sensors and sensor networks and advanced platforms that would allow for airborne, long-term, long distance sensing are needed. Technologies to enable effective global transaction monitoring with the ability to tag items and monitor their movement is essential.

The development of technologies that would help anticipate terrorists' traits and prospective courses of action received much discussion. The use of gaming, modeling, and simulation were identified as techniques for this task. Red teaming to explore hypothetical terrorist scenarios and the development of fusion and analysis tools to work with this data was identified. There is also a need for better ways to share lessons learned and mistakes made. The mobilization of the proper forces for actual interdiction will hinge on the ability to provide rapid transfer of information to the appropriate authorities.

Technology can play a very large role in **hardening the infrastructure critical to the continuing functioning of our societies**. All systems that provide services such as utilities and public safety are of concern. In order to limit cascading failures, understanding the complex dependencies between systems through interdependency and risk/vulnerability modeling is required. Mechanisms to quickly isolate failed components, redundant systems, and systems that can "auto recover" and adapt are also needed. Optimizing the "human in the loop"— using the appropriate human/technology balance – seems the best way to provide the right level of protection since it's not possible to completely prevent all damage. The types of technologies

that need to be considered are communication and surveillance systems (including health surveillance), autonomous remote sensing, cyber security/computer network defense, and better data/information systems and analysis. Systems for tracking movement of people and goods and protecting logistics would also be needed.

The challenges lie in retrofitting existing hardware and software, in modify operating procedures, and in getting better vulnerability assessment. For new construction, we need up-front vulnerability assessment and integration of hardenings feature into the design from the beginning.

Since both the infrastructure of a given society and the "society" itself must survive and contain the effects of an event, there is a need for societal "hardening", reducing the terror of an event when one occurs. Various institutional activities were identified such as risk realization and communication to promote dialogue and debate leading to acceptance of the long-term nature of the problem. The standards, formats, and compatible systems should be developed to support rapid sharing of information and "red teaming" should be used to test effectiveness of various approaches against threat scenarios. Other measures such as psychological hardening, better risk communications methodologies, better communications and training, improved behavior understanding, and enhanced feedback to institutions such as alternatives to 911 calls could be applied to the general population.

Effective response could be enhanced with technology for communications, command and control, situational assessment/awareness aids for first responders, policy and decision support and training. Communication systems need an overall plan with contingencies and with sufficient redundancy and backup. Technology could help with locating and accessing indigenous response capabilities and provide responders with knowledge of communication systems' resources. Technology could help bridge gaps in interoperability, both inter-agency and international, and help with public awareness communication capacity. Providing power (AC/DC/other) is another key issue. Command and Control Systems (national/international) could provide an integrated response capability through the creation of a common operational picture (COP), and effective command, control, and communication (C3). Key features would include state-of-the-art collaboration tools for the formation of virtual teams, effective visualization tools for affected buildings giving structure details, "just-in-time" knowledge transfer from domain experts, as well as effective resource tracking.

Technology could provide better responder protective equipment and monitoring and tracking of response team members, including the ability to assess their physical and mental status and the status of their available resources. Sensors to look through walls, allow remote detection of hazardous materials and assess structural integrity (Smart Buildings) would greatly improve situational assessment and awareness. Other valuable technologies would be tools for containment and decontamination of biological/chemical/nuclear agents. Tools for predictive modeling of plumes and dispersion of agents would be valuable, and would allow rapid damage assessment. Responder performance could be enhanced with technology for web-based guides, training, and certification.

Recovery was defined as the process of "getting back toward 'normal'". This could include criminal investigation and law enforcement, detection and assessment technologies, decontamination of infrastructure / buildings / debris / victims, and protection of the work force.

The first challenge will be to make sure that the recovery event is not worse than the event itself. Communication and effective education are key areas where technology could improve support of recovery from terrorist activities through "distance learning" for Natural Disaster Management Offices (NDMO's), through enhanced sharing of best practices, through effective use of media and communication channels, and through more effective information sharing for planning and decision making. Visualization and Graphic Information systems (GIS), modeling and scenario evaluation (including economic processes) and "information compression" to enable wider dissemination under limited communication bandwidth are key technology drivers. Technology in conjunction with social processes to help determine "how clean is clean enough" will be critical as well as improved models for long-term socio-economic impact assessment. Consideration of both environmental recovery and strategic economic recovery are important. Technologies for rapid deployment of power and water through small, expendable drop-in structures would be useful. Overall, the assessment was that better technologies could make recovery safer, cheaper, and more effective.

Ideal Systems for Combating Terrorism

Having considered the unique challenges for the region and the general role of technology in this problem space, the workshop participants broke into four smaller groups to generate visions of an ideal system for compacting terrorism in the region, optimized for the focus of their particular group assignment. The essence of each ideal system is described below.

Interdiction Team

At the policy level, an increased appreciation and understanding of Asian culture and languages is needed. Ideally, a communication plan aimed at getting our story clearly communicated in the region and helping us to understand the opposing message would be developed. This could also be used to help our society better differentiate real risk from general fear.

A system was envisioned that consisted of:

- a global transaction and travel tracking system, using sensors for tracking chemical, biological, nuclear hazards and explosives,
- a DNA based database for tracking people linked to travel documents, and
- a system that stores red team data and hypothesizes possible futures that can link to these tracking systems,

so that upon sufficient data matching, appropriate international organizations can be notified for a coordinated response.

This system would flag NULL data and discontinuities and manage HUMINT (intelligence gathered by human agents) data efficiently. System abuse would be controlled by two-way transparency. This tool would both push and pull data but would push data when needed based on knowledge of what information the user had. This system would also be used to establish collaboration across countries using multiple languages, creating in essence a virtual global intelligence agency.

The final element of this ideal system would be an automated critical infrastructure protection system to place segments of the infrastructure in protection mode when attack mechanisms are

sensed. This dynamic and evolving system would need to have tools for trend projection and would be tuned to detect deceptions and insider attacks.

Hardening Society and its Infrastructure against Attack

The basic need is the creation of an environment in which terrorism cannot flourish.
The ideal approach to this would be to establish a regional security franchise. If developed properly it would provide a scale-free solution through the use of simple building blocks that are locally customizable within global standards. The features of the basic system would involve border monitoring of people and goods with advanced information assurance techniques for documents and automated review of those documents at borders. This system would use biometrics and smart cards for identification and tracking of people, and tags and seals for containers to identify and track hazardous materials. Documents would be automatically reviewed and verified with advanced integrity and information assurance techniques. Materials and vehicles could be monitored remotely.

A better understanding of the intentions of terrorist actors could be facilitated by developing tools that would model behavior and operations. These would be part of the franchised analysis and warning toolkits. These systems would be locally customized but designed within global specifications to allow efficient sharing of information globally - leading to knowledge and alerts worldwide. A side benefit of this system would be improved communications among these nations as well as improved surveillance for health and local security unrelated to terrorism.

The implementation approach suggested by this group was very important – defining key features with a top down view but with bottom up enhancements. The expandability of this system would be assured through consistent implementation.

Responder View

The ideal system involved 4 aspects – diplomatic, regional systems for intelligence, improved border security at all levels of "borders", and enhanced tools for responders.

An Island States Security Initiative or treaty organization should be created, overseen, and coordinated by INTERPOL and funded through an international appeal. This organization would provide a common operating picture on security and terrorism. It would facilitate the sharing of strategies, security issues (including legal, law enforcement, defense, and public awareness), as well as achievements and successes of regional states in combating the spread of terror. A side benefit will be improvements in the fight against international criminal activities.

An information technology system, operating at the sensitive but unclassified level, should be developed to address terrorism concerns of the members of this initiative. This system could be maintained by INTERPOL or another regional organization. The larger states could share intelligence as required, while other states could provide trainers and assistance in operating local nodes. This system would provide at a minimum, common customs and immigration databases, and maritime shipping and smuggling databases. It could track known sea and air routes for rogue ships and planes using satellites and other imaging technologies. The system could provide profiles of likely threat groups and individuals and trends in terrorist activities.

A virtual wall for border security could be developed, applicable to land, sea and air "borders". It would be used for people or cargo, using standoff layered multiple sensors (visual, thermal, CBRNE)

embedded in facilities and routine structures. This wall would be interconnected with other systems and agencies. The use of "fingerprints" of people and materials, natural or induced (electronic, chemical) as part of badging or containers and in conjunction with information security (making these difficult to alter yet easily authenticated) would be essential elements of the Virtual Wall system.

Finally, the protective gear for first responders should be much more adaptable than it is today. This gear should use materials which can change their protective properties once the nature of the hazardous environment is described or sensed.

Recovery Vision

The ideal system would be a multi-national, inter-agency, synchronized system to defeat terrorism and designed with multi-cultural/multi-national/multi-domain requirements to deter, respond and recover from terrorist acts. This system would involve people and machines, in a scalable system that is reliable, redundant, and deployable, with mobile, cheap and interoperable sub-elements. The data for this system should come from multiple sources, tagged for appropriate release and use. It would use standardized protocols and standardized forms, especially for field-collected data. The presentation for this information must include geospatial and temporal aspects to provide a regional situation awareness and "common operating picture".

Modeling, analysis, and simulation of terrorist networks and critical infrastructure networks would be an essential element of this system. It would allow for scenario evaluation and course of action decisions as well as post-action assessment and training. Sensors that are quick and easy to deploy, built to interoperability standards would support decision makers in Emergency Operation Centers.

International (multi- and bi-lateral) cooperation for response and recovery would result in standards for tools and operations and training for counter terrorism and WMD response and recovery teams. It would also facilitate shared use of facilities and equipment in crisis response.

The Combined Ideal System

The common themes of the four subgroup recommendations were coalesced into the following two system concepts for combating terrorism in the region.

A system for monitoring and tracking of information, vessels, goods and people that would be

- Regionally deployed
- Locally customized
- Globally interoperable
- Scale-free
- Layered

with automated alerts and forwarding of information and with flows to interdiction and response agencies.

A system to provide better understand the enabling environment for terrorism in the region to:

- understand the status of terrorism, extremism, political violence
- develop technologies to help focus regional knowledge and expertise on counter terrorism
- develop tools or applications to lower information sharing barriers (e.g. language)

leading to better strategic decisions and public support, resources, and institutions.

Challenges and Opportunities

The challenges to achieving the "ideal" solution were divided into five sections, four focusing on the "social" barriers as viewed by an individual citizen, as viewed by a business, as viewed by a government, and from the view of a non-government organization (NGO), and a final section on technology barriers and leverage points.

From the **citizen** perspective, the first barrier will be the fear that the money to pay for these technologies will come from the diversion of funds from other needed programs such as education and health. The second set of barriers will stem from concern around privacy and civil liberties. Questions such as:

- Can I, as a citizen, trust the government (or, if I'm not a US citizen, trust a US developed solution) to use the system for its intended purpose and only its intended purpose?
- Will the system try to change or not respect our culture?
- Will it destroy out Island traditions of tolerance?
- Will the system somehow facilitate corruption in government?

The final barrier identified will be the tendency for the average citizen to deny the danger or to believe that this system would really make them safer.

For those involved in **commerce**, the major concern was the cost of doing business.

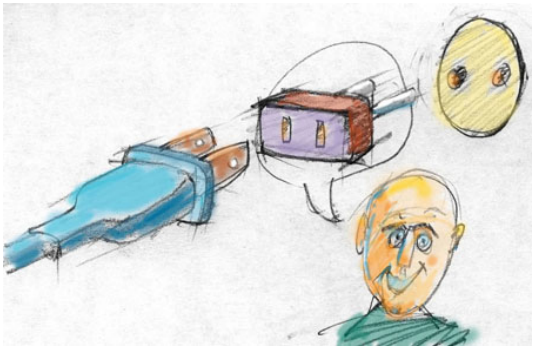
- Would this system slow down commerce, increase taxes, or have increase compliance costs?
- Would it decrease my access to (cheap) labor?

This system could require business strategy changes that could increase start-up business costs, especially in developing countries, or reduce the benefits of globalization. There could also be concern about data security for these systems. In particular, business would want assurances that competitors will not get access to proprietary data or gain a competitive edge through data access. They would also be concerned that government will use this data for audits or compliance checks in addition to detecting terrorism.

From a **government** perspective, issues will again arise around money; specifically how the money for these systems will be raised. There will be the tendency to have these funds distributed through "pork barrel" politics. The debate will rage about whether or not we really have a "threat" worth spending resources. There will be political issues around fear of electorate alienation because of citizen concerns about these systems. Also, improved international and agency relationships will have to be developed respecting sovereignty of nations and working through current bureaucratic cultures and the historical international environment of mistrust. Finally, the whole subject of information sharing with its associated legal/policy issues, agency/organizational cultures, and information security and controls present huge barriers to major changes. In most cases, small Island nations feel that information sharing is not an equitable, two-way street with the United States.

The major concern for **non-government organizations** will be that governments will be focusing money on the wrong place. They will also be concerned that these systems would affect their institutional and cultural operational styles. NGO's are typically very suspicious of governments, especially the military, and would fear that they would be adversely affected by association with governments in these systems. In general, NGO's fear systems that might compromise their independence, effectiveness, or security in any way.

Technology barriers and required technology breakthroughs largely fell into information and computing or sensing and tagging areas with a few outliers.



In information/computing, barriers were identified as available *bandwidth* (especially for smaller islands) and *storage* with more than peta-byte systems required. *Information assurance* was felt to not be up to the challenge, with authentication, confidentiality, and the availability of information an issue. The question of the possible need for multilevel security systems to NSA standards was raised, especially in the context of a multinational effort (which may require more even more levels), as was the extreme difficulty of achieving any NSA system approval. The need for better *language tools* for translation, natural language processing and better technologies for teaching languages was identified. The challenge of effectively *extracting knowledge from information* will require extensive research in data mining, context extraction, and pattern recognition. In general, the whole problem of managing and analyzing large volumes of data is not yet solved. Other problems included the lack of a *common operating environment* and of common standards/protocols. The high cost of software development must be considered as a possible barrier. The barriers involved in the development of *mathematical models* that adequately depict terrorism network and resources are enormous, with large multi-disciplinary efforts needed to develop the *social cultural modeling* (with possible predictive capability) that is desired. Finally, there will be a need for improved technologies to *detect, intercept, and exploit communications*.

For sensing/tagging, the lack of non-destructive*, standoff detection* technologies for explosives and BCNRE was identified as a barrier. Inexpensive technologies for *biometric detection* such as DNA to identify people and for clandestinely *marking or tagging* mobile targets are needed. The development of *tamper proof containers* for shipping and reliable, inexpensive technology to detect, track, and classify small boats from a distance would also be of high value. *Effective robotics* have not been adequately developed to place sensors into areas difficult or dangerous for human access. Finally, *nano technologies* with improved engineering to rapidly and cheaply manufacture large numbers of small things must be developed.

There are many **leverage points** where existing programs and capabilities could be used to rapidly prototype some of these concepts. The ability to build standard web based interfaces provides a valuable starting point for any multi-national systems. We can build on the informal, unofficial multilateral development of standard process (MPAT) and collaborative sites for Civilian-Military Operations (APAN's CMOC). There are also existing videoconferencing facilities and more ability to videoconference using standard IP Internet protocols. The ASCI program continues to fund new parallel systems with enormous computing capability. Existing marine surveillance customs and immigration systems, the Navy's perimeter defense systems, which are under development, many existing information sources (open sources) and emerging counter terrorism centers can be utilized. Sandia is working with the intelligence community on expanded red teaming concepts and on the development of a "hypothesizer" engine to manage and reconstruct the hypothetical space within which a terrorist act could occur. In the area of terrorism organization modeling, there are significant activities underway at PACOM (JIACG, J08 led initiative), Sandia, DTRA, MCCDC (Project Albert), among others.

Several generic leveraging concepts were also identified. For example, industry is leading the charge for security in some areas and might be very interested in cargo tracking systems, which could increase performance, reduce inventory losses, and have other commercial benefits. It was noted that by putting counter terrorism into a broader context of improving quality of life might allow the leveraging of other funding. Finally the types of multi-national efforts suggested in this workshop can create opportunities for positive collaboration between US and other governments.

Recommendations for Action

The participants agreed that following actions should be taken as a result of PacFest:

The concept for a monitoring and tracking system described in the system solutions should be piloted. The approach suggested was multi-phased:

1. A white paper describing the features and approaches for development will be written. *This will start with a requirements description from Michael Rosenthal of Palau.* This will be forwarded to the participants and additions and refinements will be made.
2. This white paper will be presented at an appropriate international forum for refinement, interest and buy-in. *John Reitz will investigate the Western Pacific Naval Symposium or the North Pacific Coast Guard.*
3. Sandia and the Pacific Disaster Center will look for a way to investigate the technical architectures for a "scale free" approach.
4. Identify funding agent(s) for the development of a concept demonstrator.
5. Develop a simple concept demonstration and use a specific country or situation for initial testing and refinement.
6. Migrate the demonstration to selected pilot sites – Albuquerque? Palau? Perth?

In order to make progress on the recommendations for better understanding of the enabling environment for terrorism in the Asia-Pacific region:

- *Paul Smith-will draft a concept paper on improving local terrorism context information and the clearinghouse approach.*
- Judy Moore-will send a Sandia white paper on "Know-Net" to the PacFest group.

Improved technologies for language translation are needed to facilitate collaborations within the region. John Reitz will draft specifications on machine translations. (Refer to work at Johns Hopkins University Center for Language and Speech Processing).

Chris Murray will initiate a brief concept paper about a system to determine what an individual using a system knows, and probes to make the individual aware of what they need to learn, then pushes the right information to them.

During the workshop, several related efforts were discussed and ideas for leveraging these were developed:

- Create a pilot project around red teaming for Hawaii to feed the hypothesizer being explored by Sandia. *John Whitley and Mike McCurdy will explore this*.
- Information needs to flow about modeling of terrorist behaviors by DTRA, PACOM, Sandia, and the U.S. Marines.

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. Special thanks to Cheryl Lawrence, Susan Clements and Debra Blaeholder in this regard. We are also grateful to Peter Colvin, Chris Chiesa and Jim Gosler for their help in facilitating breakout sessions. 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. The Maui High Performance Computing Center (MHPCC) is a national supercomputing resource and a Center of the Air Force Research Laboratory (AFRL) Directed Energy (DE) Directorate, managed by the University of Hawaii.

Appendices

List of Participants

Name	Organization
Al Adams	Consultant
Prudence Buckton	Defence Imagery and Geospatial Organization (DIGO), Ministery of Defence, Australia
Josko Catipovic	Naval Undersea Warfare Center
Craig Chellis	Pacific Disaster Center (PDC)
Chris Chiesa	Pacific Disaster Center (PDC)
Allen Clark	East-West Center (EWC)
Peter Colvin	Pacific Disaster Center (PDC)
Woody Goins	FEMA (DHS) Pacific Area Office
Jim Gosler	Sandia National Laboratories, Advanced Concepts Group
Vic Gustafson	Hawaii State Civil Defense Agency
David Hamon	Defense Threat Reduction Agency
Joe Harris	Sandia National Laboratories, Advanced Concepts Group
Ed Hoffer	Center of Excellence in Disaster Management and Humanitarian Assistance
Chia Chung Hong	Ministry of Defence, Singapore
Gan Ling Horng	Ministry of Defence, Singapore
Ray Isawa	Pacific Disaster Center (PDC)
Gary Ishikawa	Hawaii State Department of Defense
John Lacio	HI Army National Guard, 93rd Civil Support Team
Stephen Jayjock	Maui High Performance Computing Center (MHPCC)
Michael McCurdy	US Pacific Command - J0811
George McNamara	Naval Undersea Warfare Center
Merle Miyasato	Foreign Military Studies Office, Ft. Leavenworth, Kansas
Judy Moore	Sandia National Laboratories, Advanced Concepts Group

Chris Murray	ThoughtWeb, Australia
Earnest Paylor	Department of Defense
Luisa Ratudina	Ministry of Home Affairs and Immigration, Fiji
John Reitz	USPACOM Asia Pacific Area Network (APAN)
Michael Rosenthal	Ministry of Justice, Palau
Dave Seaver	U.S. Pacific Command, J34, Force Protection & Critical Infrastructure Protection
Paul Smith	Asia-Pacific Center for Security Studies (APCSS)
Todd Spires	ACS Defense, Inc.
Tak Sugimura	Maui High Performance Computing Center (MHPCC)
Ed Teixeira	Hawaii State Civil Defense Agency
Stanley Toy	HI Army National Guard, 93rd Civil Support Team
Steve Watkins	U.S. Pacific Command, Joint Interagency Coordination Group for Combating Terrorism (JIACG/CT)
John Whitley	Sandia National Laboratories, Advanced Concepts Group
Jennie Williamson	U.S. Army, Pacific
Gerold Yonas	Sandia National Laboratories, Advanced Concepts Group

Agenda

Tuesday, October 21

1800 – 2000 Evening Dinner Social & Jumpstart for Discussions

Tables discuss the "What are the unique terrorism vulnerabilities for this region?" and "What are the operational disadvantages and advantages for terrorist activity?"

Wednesday, October 22

0800 - 0830 *Check-in, Continental Breakfast*

0830 - 0900 *Welcome, PAC Fest Purpose and Administrative Details*

0900 - 1000 *Terrorism in the Asia-Pacific Region - Backdrop and Context for the Brainstorming Sessions*

Break

1015 - 1030 *Overview of the Agenda and Discussion of Brainstorming Rules*

Session I - Unique Terrorism Issues for the Pacific Region

1030 – 1100 *Written Brainstorm*

Collecting ideas for these subtopics:

- What are the unique terrorism vulnerabilities for this region?
- What are the operational disadvantages and advantages for terrorist activity?
- What are the unique disadvantages and advantages from the defender perspective?
- What are the unique issues in response & consequence management?

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 - The Role of Technology in Fighting Terrorism in the Pacific Region

1330 – 1400 *Written Brainstorm*

Collecting ideas for these subtopics:

- Enabling early interdiction of terrorist plots
- Hardening society and infrastructures
- Enabling effective response to terrorist acts.
- Reducing time and cost of recovery

1400 – 1530 *Sub-Group Sessions*

Organize, refine, add, synthesize and create a report for the plenary session

Break

1545 - 1700 *Plenary Session*

Reports from each group and coalesce to create a unified view

Thursday, October 23

0800 - 0830 *Check-in, Continental Breakfast*

Session III - The System View to Winning the Game

0830 - 1030 *Sub-Group Sessions*

Four groups – each work to develop a vision of the ideal system – but **optimized** from an assigned perspective:

- understanding what is unfolding,
- hardening society and its infrastructures against attack,
- enabling quick and effective response to attack, and
- reducing the cost and time for recovery from an attack.

Break
1045 – 1230 *Plenary Session*
Reports from each group and coalesce to create a unified view
1230 – 1400 *Lunch -Free time*
Session IV - The Social Barriers to This Vision
1400 – 1430 *Written Brainstorm*
Collecting ideas on the barriers to our ideal system from the following perspectives:

- Citizen (Culture & Family)
- Commerce (Economics)
- Government (Politics)
- Non-government agencies

1430 – 1530 *Plenary Session*
Large group discussion to refine and create a unified view
Break
Session V - Technology Challenges, Breakthroughs, and Leverage Points
1545 – 1615 *Written Brainstorm*
Collecting ideas on:

- Technology barriers
- Required technology breakthroughs and synergies
- Current activities to leverage

1615-1700 *Plenary Session - Large group discussion of these technology issues*

Friday, October 24

0800 – 0830 *Check-in, Continental Breakfast*
Closeout Session – Path to the Ideal System
0800-0915 *Written Brainstorm of Roadmap*
Bringing all of the ideas together to develop the plan forward
0915-1100 *Group discussion, summary, and action items*

Suggested Readings

1. "Making the Nation Safer: The Role of Science and Technology in Countering Terrorism", Committee on Science and Technology for Countering Terrorism, National Research Council of the National Academies, http://www.nap.edu/html/stct/index.html, 2002
2. Whelden, Craig, "Hawaii's Homeland Security", Military Review, May-June, 2002, p2-7
3. Asia Pacific Area Network Website!.. *fostering security cooperation in the Asia-Pacific* http://www.apan-info.net/default.asp
4. "Primer**:** Maritime Security in Asia: Threats and Initiatives", Virtual Information Center, October, 2003, http://www.apan-info.net/specialfeatures/partners/VIC%20Maritime%20Security%20Primer.doc
5. "America Strikes Back – The War on Terrorism – Special Press Summary", Virtual Information Center, October 9, 2003, http://www.apan-info.net/terrorism/terrorism_press_summary_detail.asp?id=286
6. "Terrorism: Concepts, Causes, And Conflict Resolution", Advanced Systems and Concepts Office, Defense Threat Reduction Agency, and Working Group on War, Violence and Terrorism Institute for Conflict Analysis and Resolution, George Mason University, http://www.dtra.mil/about/organization/terrorism.doc
7. Whitley, John B., Yonas, Gerold, "The War On Terrorism and What We Can Learn From Our War With Fire", Sandia National Laboratories, Albuquerque, NM, SAND2002-2404, July 2002.

Distribution

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

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