

## Information Sharing for Homeland security: challenges and solutions

**Mr. Sheng Xiong**, APHSS Fellow

Temple University

**Mr. Ted Sheppard**, Mentor

Program & Business Development Officer, Pacific Disaster Center

**Mr. Ted Ralston-III**, Mentor,

Executive Specialist, Boeing Company

As a Fellow, I attended the Asia-Pacific Homeland Security Summit in 2008 (APHSS). Mr. Ted Sheppard, the Program & Business Development Officer of Pacific Disaster Center (PDC), was assigned as my mentor. My paper assignment is about the panel: *Science and Technology Solutions to Homeland Security Challenges – Risk and Vulnerability Assessments & Solutions*.

I attended all the panels presented by PDC. In these panels, speakers from ESI, PDC, ESRI and UHM talked about the information sharing technology and their applications to every stage of the disaster management (preparedness, response, recovery and mitigation). I was very impressed with the power of those GIS software. On the other hand, many attendees raised their concerns for various aspects of these software including collecting data, information exchange, risk assessment, vulnerability of cyber security and so on. For example, the following questions were asked: “under extremely conditions like 2005 hurricane Katrina when many areas lost power, how could people gain the access to the internet?”; “What if the main server of GIS loses power? ”. “How do we deal with the cyber security if the terrorists try to hack our system?” “How do we know the severity of the destruction just by what we saw?” Dr. Rohan Gunaratna, the Head of the International Centre for Political Violence & Terrorism Research, emphasized a typical example - in the recent terrorists attack in Pakistan, security guards saw a “car accident” instead of ‘suicide bomb’. Speakers discussed many solutions to these problems. For example, Mr. Dolejs, Vice President of the International Emergency Services Integrators (ESI), addressed the first problem: “we have two backup generators for the main server

and we test them every month.” Mr. Johnson, Public Safety and Homeland Security Director, ESRI, said a beforehand vulnerability assessment is the key to the second issue. The advanced assessment will avoid us to be cheated by what we see on the surface.

Although experts have done a great job in finding solutions to some concerns about difficulties and challenges, some concerns still remain challenging. One of these challenges is the improvement of effectiveness of information sharing.

The need for information sharing has been recognized by the national security community long ago. But only in the past few years has this requirement received appropriate priority. Today this effort still remains a work in progress, because maintaining a comprehensive yet cohesive information network that enhances inter- and intra- Department information sharing is complicated by geographical, infrastructural, and technical challenges.

The following are some examples that speakers discussed in their presentation with respect to the vulnerability in today’s information sharing system. Many communities do not have an accurate or complete set of policies for large-scale or protracted events. Information sharing and inter-agency coordination is clearly needed to facilitate a successful large-scale emergency incident response or recovery effort. Although emergency service disciplines typically respond well within their own areas of expertise, communication patterns with other responders that would insure the rapid exchange of valuable information may not have been established. In many cases, one service discipline does not have the immediate knowledge of the assets deployed by another discipline, or the location of these resources and personnel.

A fast exchange of useful information via networks will significantly enhance the effect of military and security operations. One of the great challenges is the rapid collection, processing, and

dissemination of information. However, information security remains one of the biggest hurdles for effective information exchange. The first hurdle of network centric information sharing is the information sharing itself. This includes setting up the whole network infrastructure and to ensure the interoperability of applications and data. After that, the second hurdle is to share information securely within the own organization or across different organizations. In the past, there was little information exchange beyond the boundaries of the own organization. Today, many different operations have to cooperate and directly share information, such as defense operations, as well as homeland security and disaster response missions. This ranges from a local volunteer fire brigade over policy makers and large humanitarian organizations to the armed services of different countries. With respect to security, these organizations have very different capabilities, policies and doctrines. The ability to meet all their security requirements is a key challenge to information sharing.

So what would help improve the effectiveness of the information sharing system?

The commercial sector must address the entirety of information sharing issues with the national security community. Industry must work on creating global scale in technologies such as identity protection and verification, role-based access and object-level security. Most of these technologies and capabilities exist today, but not at the scale we need. Migration strategies are needed to transit identity verification and attribute correlation to widely available on-network services.

Industry must help solve the problem of scalability and inter-enterprise transparency. We must be able to federate identity and individual attributes across enterprises so that data owners can make informed decisions on access. Link these initiatives with the knowledge management efforts underway in the intelligence community and the Defense Department, and we could achieve an ease of delivery

that is lacking today. Major contributions are needed from industry on migration strategies from the current network and systems architectures to the more integrated service-oriented architectures that are emerging. Current security solutions cannot be removed until robust object protection schemes are in place. Simple network and system access mechanisms we use today cannot be replaced with more object-focused access controls until identity verification and attribute correlation can be provided as a multi-enterprise service. Access to data will not be transparent across enterprises until there is uniformity of metadata and seamless network interfaces.

The entire national security community must work together to articulate to industry the gaps in process, governance and technology, and to specify the priorities in filling these gaps. There is great work being done in agencies throughout government to address information sharing. Most of that work is internal to the enterprise. More cross-enterprise work is now needed. In fact, ESI, PDC and ESRI already realized it and are going to establish partnerships after the summit.

We know that industry does address information sharing needs. What is needed now is a much stronger approach to meeting the challenges of information sharing. They should not be individual challenges, but should be addressed collectively.

As Mr. Dolejs mentioned in APHSS, homeland security involves integrating people and business processes across multiple agencies, departments, and organizations in the U.S. government, along with other public and private sector organizations both within the U.S. and across the globe. We need not only a robust system that is scalable, secure, and flexible, but more importantly we must establish a common integrated technology platform that possesses a true open architecture capable of supporting the data integration of all federal, state, and local government entities in one, central,

common operating environment. To conclude it is essential for us to make every effort to improve and coordinate homeland security information sharing.