THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION AND HOMELAND SECURITY

VOLUME 8 NUMBER 10

April 2010
Emergent Technologies

Editorial Staff

Editors
Devon Hardy
Olivia Pacheco

Staff Writers
Joseph Maltby

JMU Coordinators
Ken Newbold
John Noftsinger

Publisher
Liz Hale-Salice

Contact: CIPP02@gmu.edu
703.993.4840

Click **here** to subscribe. Visit us online for this and other issues at http://cip.gmu.edu

In this month's issue of *The CIP Report*, we feature technologies that are emerging in the fields of infrastructure protection and homeland security.

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION and HOMELAND SECURITY

First, we highlight Virtual USA, an initiative launched by the U.S. Department of Homeland Security's (DHS) Science and Technology Directorate to facilitate information sharing. Then, the Center for Technology Development (CTD) at the Virginia Tech Transportation Institute (VTTI) discusses their development of real-time Data Acquisition Systems (DAS). Next, we include an article about the DHS's Automated Critical Asset Management System (ACAMS), a web-based system used to collect, manage, and prioritize the asset data for many of the Nation's critical infrastructure and key resources (CIKR). We also include an article about the recent Annual Technologies for Critical Incident Preparedness (TCIP) Conference and Exposition held in Philadelphia. An excerpted article from the *Malaria Journal*, which explores the use of mobile phone data to estimate the travel patterns and imported *Plasmodium falciparum* rates among Zanzibar residents, is highlighted. We also present information about vibration energy harvesting, a technology that generates energy from movement.

This month's *Legal Insights* analyzes the safety, privacy, and legislative concerns involved with implementing Advanced Imaging Technology (AIT) scanners at domestic and international airports.

Finally, the Program Manager for Education at the Center for Infrastructure Protection and Homeland Security examines the lessons that can be learned from the recent *Cyber ShockWave* ('CSW') workshop.

We would like to take this opportunity to thank the contributors of this month's issue. We truly appreciate your valuable insight.

We hope you enjoy this issue of *The CIP Report* and find it useful and informative. Thank you for your support and feedback.

Mick Kicklighter

Mick Kicklighter
Director, CIP/HS
George Mason University, School of Law

Virtual USA: A New and Exciting Way of Information Sharing

by Charles L. Werner, EFO/CFO,
Fire Chief, Charlottesville VA Fire Department

Imagine two scenarios:

Scenario 1: A Category Five hurricane strikes a major city in the Southeast United States. The local and State emergency operations centers (EOC's) activates and are immediately in a frenzy of activity; the situation is naturally chaotic as emergency responders are deployed through multiple means, while many are unable to deploy at all given their own personal situations. The field incident commanders struggle to obtain situational awareness and ascertain the impact of the hurricane, such as: the status of the roads; power supplies; location of emergency vehicles; the status of medical supplies and facilities, as well as shelters, etc. To complicate the situation further, the status of numerous special needs populations is unknown. Critical infrastructure such as hospitals, water sources, jails, and sewage systems are damaged or destroyed. Localities are all requesting immediate assistance and clamoring for the same limited resources. The lack of real-time information makes it difficult to efficiently prioritize actions in the EOC as well as the field, only adding to the chaos. In the meantime, offers of assistance are flooding in from around the state and contiguous states as well as from the American Red Cross, and other organizations such as the Federal Emergency Management Agency (FEMA) and the National Guard. While acquiring accurate information and guidance to the citizenry is critical, often times the information is too incomplete or only a "best guess." As the day(s) wear on, things become more problematic as obtaining assistance is often held up or turned away due to the challenges in logistics coordination — often lending to a lack of visibility regarding choice routes that responders should take, or which area or population has the greatest need at the time of emergency or event. It takes a day or more before some semblance of order and control is established. The human cost, in simple misery alone, is very high.

Scenario 2: A Category Five hurricane is set to strike a major city in the Southeast United States. Using their Virtual USA geospatial platform, the city EOC director, working "virtually" with the state EOC and conferring with staff, determines what information to make available to surrounding jurisdictions as well as contiguous states. Using the appropriate protocols, FEMA is also put on alert — as is the National Guard. They determine what planning and operational resources they will need in the EOC and, using multiple means, put them on various stages of alert — providing them the time they need to settle some personal affairs before hunkering down for the long haul. They convene an emergency "virtual" conference with the relevant parties to pre-plan for the likely scenarios based on real-time National Oceanic and Atmospheric Administration (NOAA) weather information and the plume modeling capabilities they have included in their platform. Based on what they are seeing in real-time, they identify the resources they need — both in and out of the state — and make deployment decisions with their counterparts and get things in motion. Resources are prepositioned, evacuation routes planned, shelters and medical facilities identified, and personnel deployed and tracked. Emergency communications and protocols are also put in place and deployed. As the storm hits, the affected localities are able to accurately map damaged areas. Special needs populations are tracked and their statuses are reported. Critical infrastructure facilities are constantly reporting their operating capabilities and the estimated time to return to full functionality. Responders have access to road status and traffic information as they are attempting to reach affected areas. Requests for assistance are mapped and paired with the nearest available resource. The utilities provide a real-time depiction of the power grid, with

(Continued on Page 3)

Virtual USA *(Cont. from 2)*

projected restoration areas and locations of repair crews, which law enforcement can see to facilitate their reentry into affected areas. Some of the plans break down — as they always do, but this is being tracked in real-time and redeployment decisions are made. While there is chaos, it is more ordered and not due to the lack of actionable information

Scenario 1 motivated the creation of DHS's Virtual USA initiative (and is based on an actual event), while Scenario 2 is a reflection of the impact of the "end state" implementation the program can offer.

What is Virtual USA?

Virtual USA is an initiative launched by the Command, Control and Interoperability Division in partnership with the First Responder Technology Program, which are both part of DHS's Science and Technology Directorate. The objective of Virtual USA is to enable seamless information sharing and collaboration across all jurisdictions so that any authorized personnel can obtain real-time, actionable information when they need and in the form they need it. This last point — in the form they need it — is critical to the success of the program. Virtual USA is designed to allow jurisdictions to use whatever system or platform they currently have — they can use whatever technology they want as their base platform. Moreover, it does not require that the jurisdiction procure expensive new software or hire expensive software integrators.

Leveraging Technology

Instead, what Virtual USA does is leverage what is often called Web 2.0 technologies — that is technology that is web enabled, standards based, open architecture, and cheap — although not free — to enable these platforms and systems to "talk" to one another. While Virtual USA does not require that a jurisdiction have a geospatial platform, the program has become a powerful demonstration of the value of geospatial information so that it is more useable. The key here is that information is more valuable in the context of other relevant information. This is difficult when information is only made available in the form of text — the connections are hard to make. Geospatially enabling that information, however, enables the user to "see" the information contextually and in one place, thus making it more immediately actionable. That enables better and speedier analysis to take place to fit the immediate situation. Rafts of analytical tools out there make geospatial platforms even more powerful.

The good news for the emergency preparedness and response community is that the basic tools required to make this happen are readily available and very cost effective. In fact, the impetus for Virtual USA started when DHS saw the potential in two very powerful programs — Virtual Alabama, which uses a Google Earth enterprise platform, and the Virginia Interoperability Picture for Emergency Response (VIPER, see Figure 1 on page 4), which is based on an ESRI (georgraphic informaiton systems software) platform. It was the ability of these systems to significantly improve emergency response capabilities in their respective states as well as their ability to almost seamlessly share information that was the kickoff point for the Virtual USA initiative.

Virtual USA in Action

Virtual USA formally began with the convening of the Regional Operations Platform Pilot (ROPP) in February 2009, which brought together eight states in the southeast United States to demonstrate and ultimately operationalize their ability to share information and collaborate in real-time. In doing so, Virtual USA had two objectives: 1) to help the states improve their own capabilities and 2) to enable regional information sharing and cooperation. Phase 1 of this pilot program led to a November 4th proof of concept in which six of these states along with FEMA's National Response Coordination Center, reacting to a multi-disaster scenario, demonstrated that they could, with few exceptions, share dynamically changing information and collaborate in real-time. The lessons learned from that demonstration has been integrated into Phase II of the ROPP as well as another five states in the Pacific Northwest (PNW) Pilot. In addition, DHS is

(Continued on Page 4)

Virtual USA *(Cont. from 3)*

now developing what they call their Generation II information sharing prototype platform, which is leading to the development of a scalable "opt-in" national information sharing capability that will enable any authorized user to share and obtain relevant actionable information in real-time and in the way they want to see it. This capability will be tested in the summer of 2010.

It is critical to note that Virtual USA is already more than just a proof of concept — it has already shown real results.

1. Where there was previously little collaboration among the states — all the participating states are now working with one another on a regular basis, including sharing information and technical support.

2. When the program began, only two states had information sharing platforms — Virginia and Alabama. This has now expanded to seven of the states in the ROPP. The five states in the PNW Pilot are in the process of establishing platforms as well.

3. The lessons learned and the technical solutions which went into developing these platforms have been shared with over 100 jurisdictions around the country.

4. Georgia used the Virginia platform to manage the floods that took place during February 2010.

5. Mississippi's newly deployed platform was used to find a lost hunter, saving his life.

6. Four days after the ROPP demonstration, Florida used its Virtual USA platform to manage the response to Hurricane Ida.

7. Alabama used its platform to help support Greenburgh, Kansas in the aftermath of a tornado in 2009.

8. The deployment of the platforms has been proved to save time and money. Virginia reports responding over 60% more quickly during recent exercises.

The impressive success of this initiative has already caught the attention of the White House, which is striving to develop programs to enable better access to information and collaboration. Virtual USA has not only been recognized by the White House as a significant Open Government Initiative, it has also been cited by White House officials as a model for government to follow. For example, at the recent ESRI Federal Users conference, Dr. John Holdren, the Assistant to the President for Science and Technology, told the audience in his keynote address that:

Virtual USA is a quite remarkable initiative because it is relying very heavily on resources already in place in the possession of the many collaborators, and simply bringing them together in ways that enable an increased degree of communication and cooperation in responding to various kinds of national emergencies.

Some Key Criteria

For those of us in the State and local emergency response community, Virtual USA is a unique Federal program in several

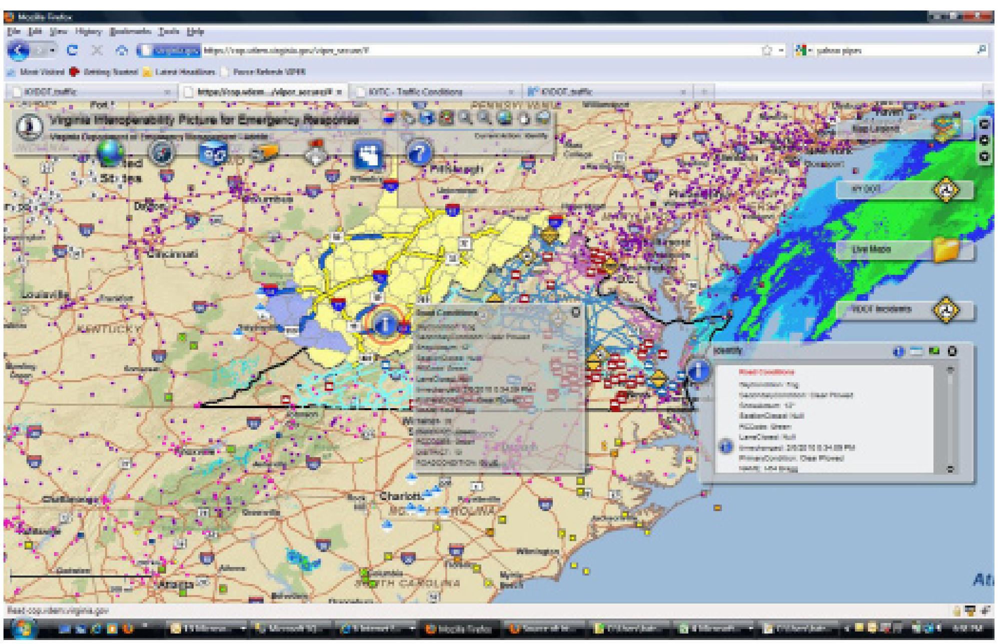

Figure 1: VIPER shows West Virginia road conditions in real-time.
Photo provided with permission by the Virginia Department of Emergency Management, Bobbie Atristain, Chief Technology Officer.

(Continued on Page 23)

The Center for Technology Development (CTD) at the Virginia Tech Transportation Institute (VTTI)

by Sherri P. Box
Public Relations and Marketing Manager, VTTI

The experts who comprise the Center for Technology Development (CTD) at the Virginia Tech Transportation Institute (VTTI) are one of the primary reasons VTTI is recognized as the leader in real-world driving research. This elite team of engineers, technicians, staff, and students has developed real-time Data Acquisition Systems (DAS) capable of collecting and storing large quantities of detailed information (participant driving data) including video, vehicle network information, and information about how the vehicle is being driven (e.g., speed and braking force) as well as the tools needed to analyze this data.

Led by Andy Petersen, the CTD develops, manufactures,

Andy Petersen, Director of the Center for Technology Development

Figure 1: 100-Car DAS

implements, and maintains innovative solutions for transportation research. The CTD is continuously developing advanced systems for data collection with the goal of collecting a wide range of detailed data while remaining unobtrusive to study participant drivers. Virtually all of VTTI's research equipment — real-time data acquisition hardware, software, firmware, machine vision programming, algorithmic programming, control, and automation — is developed in-house by the CTD.

Through its naturalistic research, VTTI has found when drivers are involved in a crash or near-crash, very often they do not remember what they were doing or what happened in the seconds just prior to the incident. They are either traumatized by the event, injured in some way, or it happened so fast they have a hard time recalling exactly what led up to the crash or near-crash. The collection of data of real-world driving situations and driver behavior has provided and will continue to provide new insight into critical incidents. It is now the gold standard for accurately assessing secondary tasks drivers engage in during the seconds just prior to a crash or near-crash. With the use of sophisticated cameras and instrumentation installed very unobtrusively in participants' personal vehicles, VTTI can provide a clear picture of driver behavior and risk perception under real-world driving conditions with real-world consequences. In addition, once the data are collected, they can be re-analyzed and driver behavior can continue to be studied from different perspectives for many years following the initial data collection phase.

Information collected from various on-board systems is processed and stored in the DAS, which is a "black box" unit that was originally installed in the truck of the vehicle under the rear package deck (Figure 1). Also housed within the DAS are sensors such as accelerometers

(Continued on Page 6)

VTTI *(Cont. from 5)*

and gyroscopes. Other technology utilized in the DAS, and developed by the CTD, includes color, infrared, and black-and-white video with MPEG-4 video/audio compression and multi-channel binary data synchronization. A high-precision, differential global positioning system (GPS) with on-site base unit (Smart Road) is also used. The DAS has Doppler-based radar developed by Eaton (VORAD©) TRW. Another feature of the DAS is direct physical (haptic) driver feedback (pedal push-back, and seat vibration) and wireless communication (802.11) between the vehicle and other vehicles or infrastructure. A final feature of the DAS is removable, high capacity, and shock-resistant hard drives for data retrieval.

The first naturalistic driving study ever conducted, the 100-Car Study, utilizing the instrumentation and DAS as described above and developed by the CTD, was completed by VTTI and the results were released in April 2006. In this study, 100 light vehicles in and around the Northern Virginia/ Metropolitan Washington, DC area were instrumented with five unobtrusively placed cameras and an accompanying DAS in each vehicle. The DAS, installed in the trunk of the vehicle, under the rear package shelf, comprised five channels of digital, compressed video, multiple radar sensors, GPS, accelerometers, glare, and radio frequency detectors. The study encompassed 109 primary drivers, 241 total drivers (primary plus secondary) with data collected on the driver with continuous streaming video for 12 to 13 months as they went about their everyday, normal driving behavior, i.e., commuting to work, running to the grocery store, taking children back and forth to their various activities, and running other miscellaneous errands (Figure 2). Drivers' ages ranged from 18 to 73 years old, with 60 percent of the drivers being male and 40 percent, female. The Institute collected over 42,300 hours of driving data with over 2,000,000 miles driven, noted 15 police-reported and 67 non-police reported crashes, 761 near-crashes, and 8,295 incidents with a range of severity of crashes from airbag deployments to minor, low-force, no-property-damage crashes.

Figure 2: Quad Video

Figure 3: Next-GEN DAS

This study was the first time any "real-world" driving data had been collected so one could actually see what secondary tasks drivers are engaging in while behind the wheel of their vehicle.

In 2006, upon completion of the 100-Car Study, the CTD immediately began development of a next-GEN DAS (Figure 3), smaller in size than the 100-Car DAS, and its accompanying software as well as a less expensive version of next-GEN, the mini-DAS, which is slightly larger than the palm of your hand (Figure 4). They have also designed a multi-PC system for the collection of high resolution video as an enhancement to the DAS system used in the 100-Car Study.

Due to this innovative work, VTTI is now poised to conduct the largest naturalistic transportation study ever attempted, with data collection to begin as early as late summer/ early fall 2010. The Transportation Research Board (TRB) of the National Academies is administering the second Strategic Highway Research Program (SHRP 2). According to the SHRP 2 website, the central goal of this

(Continued on Page 18)

Figure 4: Mini DAS in Hands

DHS Web-based System Helps State and Local Government Users Collect and Manage Critical Infrastructure Information

by DHS Office of Infrastructure Protection

State and local jurisdictions use DHS's Automated Critical Asset Management System — more commonly known as ACAMS — to collect, manage, and prioritize the asset data for many of the Nation's critical infrastructure and key resources (CIKR). Available at no cost to users through a Web-based interface, ACAMS provides tools and resources to assess CIKR asset vulnerabilities, develop all-hazards incident response and recovery plans, and build public-private partnerships.

Since no single organization is responsible for securing the assets, systems, and networks that impact nearly every aspect of our daily lives, enhancing the resilience of our Nation's infrastructure depends on cultivating partnerships that promote collaboration and information sharing among all levels of the government and the private sector. Equipped with the data in ACAMS, emergency responders, homeland security officials, and law enforcement personnel are better able to reduce vulnerabilities, enhance security measures, and provide a more robust common operating picture for all participating organizations.

How ACAMS Works

First introduced in 2006, ACAMS provides a platform for approximately 5,000 users in more than 35 U.S. States and localities to engage infrastructure owners in protecting the assets critical to their communities. Using the tools and resources within the system as part of their critical infrastructure protection efforts, ACAMS users can better collect and manage critical asset information for the CIKR in their jurisdiction. This data can be used to create tailored reports, complete Buffer Zone Plans, and develop vulnerability assessments that greatly assist with pre-incident planning and post-incident response.

ACAMS was recently used in planning for the 2009 Academy Awards. Referring to the system's performance, a Los Angeles Police Department officer noted, "[t]he detailed information available in ACAMS on the facility, along with the assessments of the complex, made it possible to show the Incident Commander critical nodes, critical locations, and possible vulnerabilities at the event."

Asset owners and operators work in partnership with State and local homeland security officials to update and edit their facility information in ACAMS. This allows the asset owners to manage their information, while enabling them to support emergency response efforts by ensuring their information is accurate and up-to-date. ACAMS also provides a centralized location for asset owners to house various emergency response plans and security implementation strategies that can provide additional support to response personnel and facility managers.

Sensitive and Proprietary Information Is Protected

Sensitive and proprietary private sector information stored in ACAMS is protected from public disclosure through the DHS Protected Critical Infrastructure Information (PCII) Program. Created in accordance with the Critical Infrastructure Information Act of 2002, the PCII Program provides exemptions from the Freedom of Information Act, similar State and local disclosure laws, and civil litigation.

ACAMS Improves Planning and Response

Working closely with private sector owners to prepare for the 2009 G-20 Summit in Pittsburgh, the Pennsylvania Southwestern Counter Terrorism Task Force and other homeland security officials collected security-related information about the surrounding venues to populate asset data in ACAMS. When

(Continued on Page 8)

ACAMS *(Cont. from 7)*

evaluating asset data in ACAMS, security personnel realized that a planned route to divert protestors would take them near a critical power substation. By being able to see all assets in the surrounding area, they could identify dependencies and potential risks and determine how to address them prior to the summit.

ACAMS was also used as a planning tool to support the XVII and XVIII Super Bowl games, the World Baseball Championships, and the 2008 and, as previously mentioned, the 2009 Academy Awards.

ACAMS users are provided the tools to visually display their infrastructure data in map form through the DHS Integrated Common Analytical Viewer (iCAV). The iCAV integration with ACAMS significantly increases the amount of infrastructure geospatial data available at the State and local level. By layering local asset data from ACAMS with additional DHS and other Federal government data imagery layers through iCAV, a user can visualize the potential impact to infrastructure, as well as the nearest response resources, such as hospitals, police and fire stations, and evacuation routes. The ability to view local asset data from ACAMS in conjunction with iCAV's wide range of analytic functions makes it much easier to see how assets are interconnected and establish a common operating picture.

ACAMS Upgrade and Training

Detailed training on ACAMS and other resources to enhance critical infrastructure protection efforts are available through the CIKR Asset Protection Technical Assistance Program (CAPTAP). This three-day training session provides instruction on ACAMS functionality and also examines the processes and methodologies applied in the development of a comprehensive infrastructure program.

Since ACAMS' inception, DHS has collected feedback from emergency response personnel, infrastructure protection planners, and other homeland security officials, in order to implement system improvements based on its most useful capabilities. An ACAMS working group within the State, local, tribal, and territorial Government Coordinating Council continues to provide guidance to the system's developers to ensure updates are tailored to address the specific needs of State and local jurisdictions. Beginning in April and continuing through July 2010, a new version (ACAMS 3.0) will be introduced to the user community.

ACAMS 3.0 focuses on enhancing the end-user experience and increasing overall operational efficiencies. A more intuitive user interface design and presentation of data elements allows easier navigation, and redesigned database architecture will ensure faster response times.

Other notable changes in ACAMS 3.0 include:

- A flexible security model that enables user permissions and access rights to be determined at the State and local level.

- Enhanced information-sharing capabilities to protect sensitive data from public disclosure, while allowing general information to be shared with a broader audience.

- Additional pre-populated data fields for schools, hospitals, police stations, and fire departments to better establish situational awareness.

- Baseline data requirements to ensure the same level of information is captured about all assets to enable continuity in data collection efforts across the country. ❖

For More Information

ACAMS is one of many tools provided by the DHS Office of Infrastructure Protection to foster public-private partnerships, enhance protective programs, and build national resiliency to withstand natural disasters and terrorist threats. The Office of Infrastructure Protection recently launched a Web page listing its key programs and activities; this page is still being enhanced, so DHS urges readers to visit often: www.dhs.gov/criticalinfrastructure.

To learn more about ACAMS, contact the ACAMS Project Office at ACAMS-info@hq.dhs.gov or visit www.dhs.gov/ACAMS. The second annual CAPTAP

(Continued on Page 19)

11th Annual TCIP Conference Highlights Cutting-Edge Technology and Training Tools for Emergency Response Community

Amidst Philadelphia's bustling traffic, bright city lights, and famous cheesesteaks, approximately 1,000 attendees gathered from February 2-4, 2010 for the 11th Annual Technologies for Critical Incident Preparedness (TCIP) Conference and Expoposition. TCIP, a conference jointly co-sponsored by DHS and the U.S. Departments of Defense (DoD), and Justice (DOJ), brings together homeland security and emergency response stakeholders from across the Nation to share best practices, collaborate, and work toward new initiatives. Attendees at this year's conference included Federal, State, local, and tribal practitioners, academia, and business and industry representatives. With this multi-disciplined and diverse audience and an exhibition hall housing roughly 120 Federal and commercial exhibits, TCIP achieved its mission to foster an opportunity for constructive discussion surrounding the future of emergency preparedness and response.

Themed "Critical Connections: Linking Responders with Technology," this three-day conference highlighted training tools, technology, techniques, and research, development, testing, and evaluation investments that will improve preparedness at the onset of a crisis. The TCIP Conference featured best practices and lessons learned and focused on ways emergency responders can effectively manage life-threatening events including natural disasters and terrorist attacks.

Key leaders, researchers, and practitioners participated in approximately 30 general and breakout sessions. The event showcased in-depth demonstrations, innovative public safety initiatives, demonstrations of the latest cutting-edge technologies, and comprehensive educational training tools.

Additionally, conference speakers — including State and local public safety professionals and Federal experts — shared expert knowledge and experience on topics including voice and data interoperability, Federal resources, infrastructure protection, open source resources for public safety, and mass casualty incidents. Special conference guests included the following keynote speakers: Mr. Scott Deutchman, White House Deputy Chief Technology Officer for Telecommunications; Ms. Mary Lou Leary, Principal Deputy Assistant Attorney General, U.S. Department of Justice; Ms. Theresa Whelan, Deputy Assistant Secretary of Defense, Homeland Defense Domains and Defense Support of Civil Authorities, U.S. Department of Defense; and Dr. David Boyd, Director of the Command, Control and Interoperability Division within the Science & Technology (S&T) Directorate, U.S. Department of Homeland Security.

In addition to highlighting cutting-edge technologies, DHS S&T announced the next phase of Virtual USA, an innovative information sharing initiative that helps Federal, State, local, and tribal emergency responders communicate during emergencies. Five states in the Pacific Northwest — Alaska, Idaho, Montana, Oregon, and Washington — will form the second Virtual USA regional information-sharing pilot. The eight states currently participating in the existing Southeast Regional Operations Platform Pilot — Alabama, Florida, Georgia, Louisiana, Mississippi, Tennessee, Texas, and Virginia — will enter into a second, operational phase.

DHS S&T also announced the development of the First Responder Communities of Practice — an information sharing tool designed to help responders collaborate on best practices to support their respective homeland security missions — and unveiled the newly redesigned Firstresponder.gov. Communities of Practice allows its members —including active and retired first responders, emergency response professionals, and homeland security officials — to engage locally and nationally on critical homeland security programs, projects, and initiatives in a protected environment.

TCIP also provided a forum for

(Continued on Page 23)

The Use of Mobile Phone Data for the Estimation of the Travel Patterns and Imported *Plasmodium falciparum* Rates among Zanzibar Residents

by Andrew J. Tatem, Youliang Qiu, and David L. Smith, University of Florida
Oliver Sabot, The William J. Clinton Foundation
Abdullah S Ali, Zanzibar Ministry of Health and Social Welfare
Bruno Moonen, The William J. Clinton Foundation

This article is excerpted from ***Malaria Journal****. For brevity, the editors of* ***The CIP Report*** *removed all references. To read the complete article, please click here.*

Background

Many countries are committing to nationwide malaria elimination and global eradication is once more back on the international agenda. Historically, the technical feasibility of achieving malaria elimination in a region has been conceptualized as being composed of 'receptivity' and 'vulnerability.' Receptivity represents the strength of transmission in an area, while vulnerability is the risk of malaria importation. While both have been regularly discussed theoretically, neither have been quantified, nor methods for their quantification ever defined.

Quantifying imported malaria risk represents a central component for not only assessing the feasibility of malaria elimination from a region, but for planning the implementation of an elimination campaign. Malaria is constantly being exported and imported around the World, and in areas of high transmission, malaria importation is generally a minor concern. As local transmission is reduced and after malaria has been eliminated from a region, however, importation becomes a primary concern.

Zanzibar, an island group off the coast of Tanzania, is one of the territories in sub-Saharan Africa that has recently expressed its willingness to move from control towards elimination. Since 2003, the introduction of artemisinin-based combination therapy (ACT) and high coverages of long-lasting insecticide treated nets and indoor residual spraying, has reduced malaria prevalence to just 0.8%. These efforts have resulted in the government of Zanzibar considering an elimination campaign and undertaking an elimination feasibility assessment. Nevertheless, proximity and high connectivity to the mainland where transmission levels remain substantially higher in many places implies that imported malaria will be a constant problem.

In general, parasites can be imported into Zanzibar in one of three ways: (i) the migration of an infected mosquito, (ii) infected humans visiting or migrating from the mainland, and (iii) residents visiting the mainland and becoming infected, then returning. While mosquitoes may occasionally arrive through wind-blown or accidental aircraft or ship transport, typically they will only fly short distances. Human carriage of parasites, therefore, represents the principal risk, and is to blame in many past instances elsewhere where malaria has resurged. Quantifying such movements both temporally and spatially, and the resulting imported infection risks, represents an important task if effective, evidence-based planning for elimination is to be undertaken.

Recent approaches to quantifying human mobility patterns point the way to novel insights from new data, especially through the analysis of mobile phone records. Anonimized phone call record data that has both the time each call was made and the location of the nearest mast that each call was routed through can be used to construct trajectories of the movements of individuals over time. Here, the potential of such data for estimating importation risk in the malaria elimination feasibility assessment for the islands of Zanzibar is demonstrated. The low market share on the mainland for the network provider restricts the focus here to those infections brought in by residents returning from mainland travel. However, the approaches put forward are sufficiently generic to be applied to

(Continued on Page 11)

Mobile Data *(Cont. from 10)*

alternative regions, elimination settings, and phone network provider data. Moreover, this exercise aims to present the first exploration of mobile phone based approaches to the quantification of vulnerability to inform malaria elimination decisions and planning.

Discussion

The information derived from the analyses can be used to guide strategic planning for elimination, should the Ministry of Health decide to pursue such a campaign. Typically, three principal means of reducing imported infection risk are considered: (i) Identify infected individuals and treat them promptly, ideally before or upon entry, before they can infect competent local vectors and lead to secondary cases and sustained foci of indigenous transmission; (ii) address the source of infection by directly reducing transmission in all regions that are primary sources of infected travellers; (iii) provide prophylaxis to residents visiting endemic areas. While the second method is being addressed indirectly through the scaling up of control on the mainland, these analyses provide baseline data to inform on the first and third approaches. Screening with rapid diagnostic tests (RDTs) or microscopy at the ports of entry and providing follow-up treatment of infected individuals may play an important role in reducing imported case numbers and outbreaks. Such an approach is being used for all individuals entering the island of Aneityum in Vanuatu, while visitors from Africa were tested at the airports of Oman during its elimination campaign. Moreover, the details of all visitors to Mauritius from endemic regions are recorded and follow-up is undertaken by health surveillance officers. When movement rates are high and resources are limited however, as in the case of Zanzibar, screening all visitors at the ports or providing follow-up may be prohibitively expensive and inefficient due to the large number of low-risk trips undertaken (Figure 1).

Modelling work on achieving and maintaining elimination done for the Zanzibar malaria elimination feasibility assessment suggests that as long as effective coverage with vector control measures is higher than 80%, elimination will be achieved and can be maintained. However, once transmission is reduced to very low levels, scaling down prevention without risking resurgence will only be possible if the importation levels estimated here are lowered considerably [Moonen B, Cohen J, Smith DL, Tatem AJ, Sabot O, Msellem M, Le Menach A, Randell H, Bjorkman A, Ali A: Malaria elimination feasibility assessment in Zanzibar I: Technical feasibility. *Malar Journal* 2009, in preparation]. Prophylaxis for Zanzibari travellers is unlikely to be cost-effective or even practical given the high frequency of travel to mainly low risk regions. Screening on the ferries, especially of high risk groups during high risk periods of the year, might be a simpler and more cost-effective option compared to screening at the port of entry. Passengers are on the slow and fast ferries for six and two hours, respectively; enough time to administer a short questionnaire, a rapid diagnostic test, and treatment if necessary. However, better data is necessary to determine the PfPR in ferry travelers to appreciate the operational consequences of such an approach.

Future work will aim to link the findings here to GIS data on travel networks in the region, and build these into stochastic metapopulation models of transmission, providing flexible tools for elimination planning. Moreover, retrospective analyses of health facility records at Zanzibar malaria early epidemic detection system sites are being undertaken at present, while surveys on the ferries are planned to corroborate and compliment findings here. This work also links into and is complemented by other datasets

(Continued on Page 20)

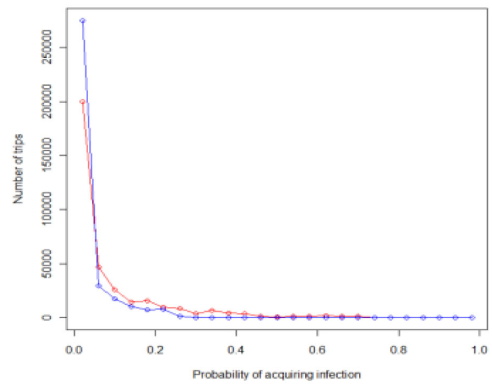

Figure 1: All trips made by Zanzibar residents plotted by probability of infection acquisition, based on region populationweighted mean dEIR (red line) and population weighted principal city mean dEIR (blue line).

Vibration Energy Harvesting

As sensors and computer processors decrease in size, they can be deployed in new places and collect data from a wider range of locations. It becomes possible to gather real-time data from infrastructure about its condition, its environment, and its ongoing health. This new sensor technology requires power to function, either from new battery technologies or from an innovation called vibration energy harvesting. This is a technology that generates energy from movement, (the regular movements of the infrastructure where the sensors are located). One company that provides these devices is Perpetuum. A representative of the company, Mr. Kevin Marzano, Director of Business Development, explains more about vibration energy harvesting.

The technology driving these devices was developed at the University of Southampton, a technology incubator for the United Kingdom. Several patents were granted over the course of research for the technology, which relies upon converting mechanical movement to electrical energy by moving a mass through a series of magnetic coils to generate power.

There are different types of vibration energy devices, which produce different amounts of power. Perpetuum's devices, for example, tend to be larger and generate more power. This makes them more useful in situations where the generator is placed in a high-stress environment and therefore needs to be more rugged. A higher-power output is also more useful when more data needs to be transmitted or when the data needs to be transmitted continuously. A device transmitting smaller packets of data or transmitting intermittently could use a lower-power generator that is smaller, lighter, and can be placed in more locations. Placing generators on machinery provides for the most consistent power generation because the machines move so regularly and the generator can be very specifically calibrated to their cycle of movement. There are also generators designed to pick up a wider range of intermittent vibrations. These sensors are usually deployed on transportation or construction equipment, where a great deal of vibration takes place, but not in regular intervals.

The generators are usually connected to some combination of infrastructure sensors, a wireless radio, and possibly a GPS or a computer processor. These sensor networks typically range in size, from 5 to 100 sensors, and are used in a wide variety of locations to collect a wide variety of information. They can track the location of equipment on remote sites, whether a particular storage or shipping container has been accessed, or the condition of a particular piece of machinery or equipment, facilitating more regular inspections. One use that has been discussed repeatedly is to attach sensors to transportation infrastructure, such as roads and bridges, thus helping to prevent accidents or structural failures. One limitation on current-generation technology is the limits on the range of the miniaturized wireless radios. Their range is generally no more than 100 yards and is often less due to the interference from the high volume of metal at most facilities where they are used. Perpetuum only manufactures the generators themselves and then sells them to a technology integrator, like General Electric, that builds the entire sensor system and maintains it for their customers. Thus, some of these technological problems are outside Perpetuum's area of concern.

The real obstacles hindering widespread use of remote sensing and vibration energy harvesting technologies have generally been technological or cultural. Technological challenges include, requiring that remote sensors generate more power than can be reasonably expected to produce at a low cost. However, these issues are slowly being resolved by newer versions of vibration generators. Cultural issues primarily include convincing infrastructure owners and managers that wireless sensing is part of a broader concept of predictive maintenance and that this newer generation technology is preferable to older technologies, such as batteries. Marzano argues that while vibration generators are more expensive as an initial

(Continued on Page 20)

Legal Insights

Advanced Imaging Technology: Using Emerging Technologies to Secure Airports and Privacy

by Dillon Martinson, JD

The failed attempt of Umar Farouk Abdulmutallab to use a bomb hidden in his underwear to bring down a Detroit-bound airliner on Christmas Day has once again placed airport security in the limelight. In response to this incident, the Transportation Security Administration (TSA) purchased additional Advanced Imaging Technology (AIT) scanners and will deploy them as the primary screening measure at many airports. But this move has been met with controversy.

Securing the flying public involves balancing security, privacy, and the efficient flow of people and goods. This article outlines the safety, privacy, and legislative concerns of AITs and suggests how emerging technologies can ease privacy concerns while at the same time strengthen security.

About Advanced Imaging Technology (AIT)

TSA currently uses two types of AIT scanners, millimeter wave and backscatter (Figures 1 and 2, on page 14). Both technologies can detect the same types of threats, potentially revealing weapons, explosives, drugs, and other contraband whether it is liquid, powder, metallic, or non-metallic. AIT scanners can identify objects, or anomalies on the outside of the physical body but do not reveal items beneath the surface of the skin, such as implants. However, DHS asserts that AIT scanners would have detected the chemical bomb used by the Christmas Day bomber — something a traditional metal detector would not.

Though both types of AIT scanners detect the same types of threats, they do so using different technology. Millimeter wave technology beams the passenger with millimeter wave radio frequency energy from two antennas that spin around the passenger from head to toe at very fast speeds. The energy reflected off of the passenger's body generates a black and white three-dimensional image that resembles a fuzzy photo negative.[1] On the other hand, backscatter technology projects low level X-ray beams over the body to produce a two-dimensional image that resembles a chalk etching.[2]

AITs cost about $170,000 per unit, excluding training, installation, maintenance, and operating staff. Despite these costs, TSA officials believe AITs will offer greater efficiencies because it will allow the TSA to more rigorously screen a greater number of passengers in a shorter amount of time. Officials believe AIT screenings are as effective as a physical pat down but only requires a fraction of the time; a pat down requires two minutes compared to the twenty seconds it takes to produce and interpret an AIT scan.

Figure 1: Millimeter Wave

(Continued on Page 14)

[1] http://wholebodyimagingfacts.com/.

[2] http://www.tsa.gov/approach/tech/imaging_technology.shtm.

Legal Insights *(Cont. from 13)*

Safety Concerns

TSA asserts that both types of AIT technologies are safe for passengers. Backscatter technology was evaluated by the Food and Drug Administration's Center for Devices and Radiological Health, the National Institute for Science and Technology, and the Johns Hopkins University Applied Physics Laboratory. Results from these studies confirm that radiation doses from a backscatter scan are well below those specified by the American National Standards Institute. In fact, the amount of radiation from backscatter screening is equivalent to the radiation exposure a passenger faces from just two minutes of flight on an airplane.[3] Approximately 1,000 backscatter scans in a year would equal the radiation of one standard chest X-ray.[4]

While backscatter technology exposes passengers to ionizing radiation, much like medical X-rays, millimeter wave technology uses radio signals akin to cell phone RF (radio frequency) energy. In comparison to cell phones, the energy projected by millimeter wave technology is 10,000 times less than a cell phone transmission. From the studies conducted, it appears that medical professionals confirm TSA's assertion that both types of AIT technologies are safe for passengers.

Privacy Concerns

In a Privacy Impact Assessment Update, TSA states that the images created by AIT technologies are not equivalent to photography and do not present sufficient details that the image could be used for personal identification.[5] However, both types of AIT technology display anatomically correct images of the screened individual, leading some groups to refer to the process as a "virtual strip search." These groups raise concerns about the government storing images of the public in a massive database or misuse by officials that could lead to publication, either in print or on the web.

TSA is sensitive to these privacy concerns and employs the following safeguards to protect passenger privacy and ensure anonymity:

• The Transportation Security Officer (TSO) who views the AIT-produced image is remotely located in a secure resolution room away from the passenger and officer assisting the passenger at the checkpoint. The TSO viewing the image never sees the passenger, and the officer assisting the passenger at the checkpoint never sees the image.

• Once the remotely located TSO determines there is no threat, the TSO communicates via a wireless headset to the officer assisting the passenger instructing the officer

Figure 2: Backscatter

to allow the passenger to continue through the checkpoint.

• Millimeter wave technology blurs all facial features and backscatter technology has an algorithm applied to the entire image.

• AIT technology cannot store, print, transmit, or save the image. Each image is automatically deleted from the system after it is cleared by the remotely located TSO.

• TSOs evaluating images are not permitted to take cameras, cell phones, or photo-enabled devices into the resolution room.

• AIT screening is optional for all passengers. Passengers may opt for a physical pat-down in lieu of the AIT scanner.[6]

The Electronic Privacy Information

(Continued on Page 15)

[3] See *supra,* note 1.
[4] http://www.dailyfinance.com/story/travel-maze-how-safe-are-whole-body-scanners-at-airports/19330048/.
[5] http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf.
[6] See *supra,* note 2.