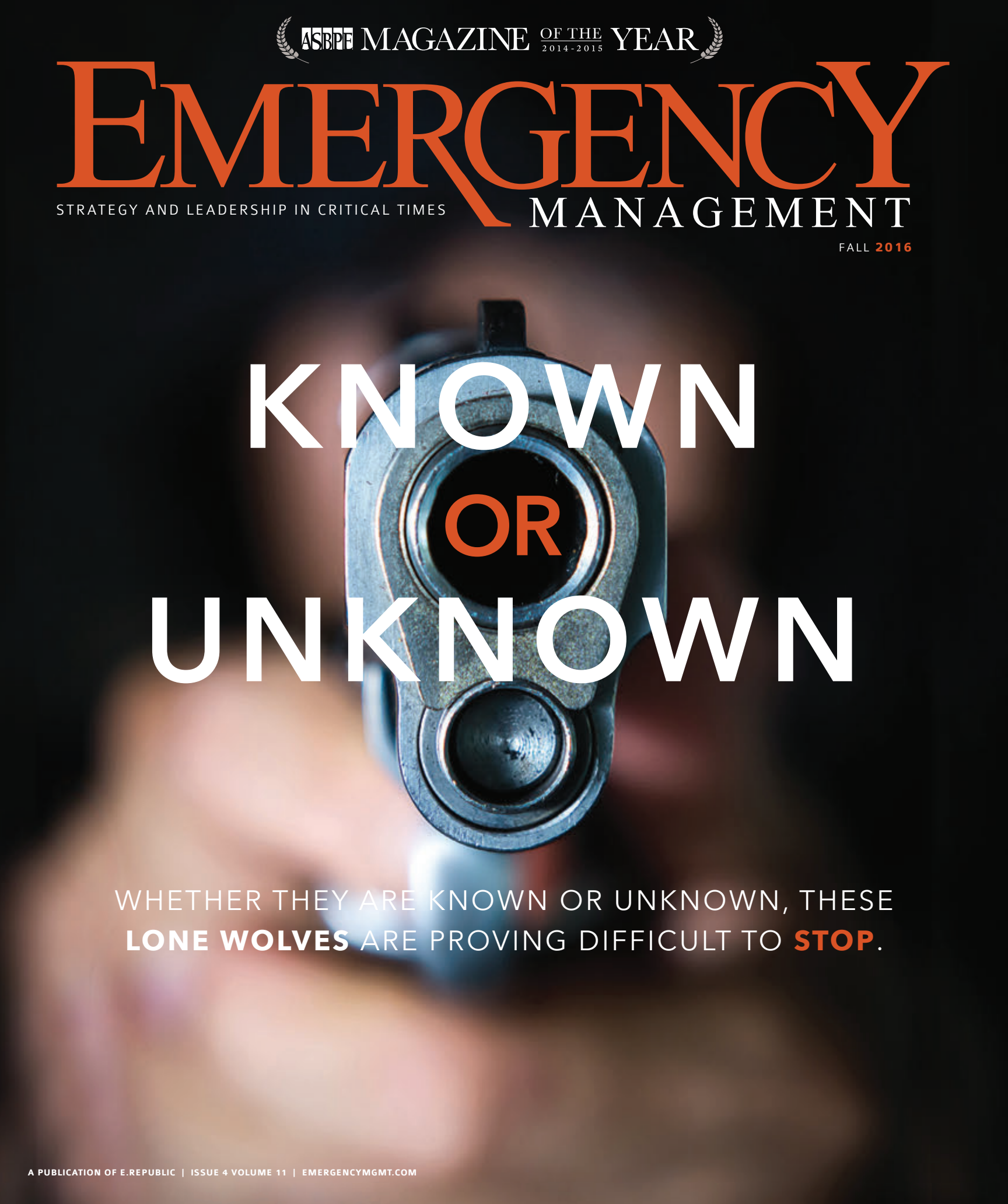
ASBPE MAGAZINE OF THE YEAR 2014-2015

EMERGENCY MANAGEMENT

STRATEGY AND LEADERSHIP IN CRITICAL TIMES

FALL 2016



KNOWN OR UNKNOWN

WHETHER THEY ARE KNOWN OR UNKNOWN, THESE **LONE WOLVES** ARE PROVING DIFFICULT TO **STOP**.

A PUBLICATION OF E.REPUBLIC | ISSUE 4 VOLUME 11 | EMERGENCYMGMT.COM

Knowledge center™

The Incident Management Software Solution

WHEN SECONDS MATTER

Emergency Management Incident Command
Incident Command System (ICS)
Critical Infrastructure/Key Resources (CI/KR)
Situational Reporting (SITREP)
Geographic Information Systems (GIS)

Hospital Incident Command
Hospital Incident Command System
Hazard Vulnerability Assessment (HVA)
Patient/Triage Tracking
Reunification
Hospital Available Beds (HAvBED)

Fusion Center
Optimized Intelligence Sharing
Secure, Tiered Access Control
Dynamic, Configurable Reporting
Inter-operable with CADs/Mass Notification

Our Mission
To build, provide and maintain highly available incident management software solutions that enhance real time critical decision making and response time **when seconds matter**.

Knowledge Center Software PERFORMS FLAWLESSLY.


Hoboken Train Derailment

Republican National Convention


Democratic National Convention

"We looked at the leading systems out there and the decision was unanimous that Knowledge Center provided us with the best value for our region."

– Judson Freed, Director, Ramsey County EMHS

WHY KNOWLEDGE CENTER?

- Ease of Integration
- Software and System Availability
- Unmatched On-site and Remote Support
- Comprehensive Offering
- Dedicated Account Team
- Depth of Experience in Incident Management Solutions

Request a demo or contact us!

412-206-2993 | Sales@Knowledge-Center.com | Knowledge-Center.com

Contents

COVER IMAGE : SHUTTERSTOCK.COM

APIMAGES.COM

FEATURES

80% of elected and appointed officials and their staff say they do not know if their state has a cyber-emergency incident plan in place.

Learn more by downloading a complimentary copy of the cybersecurity policy guide at:

governing.com/cyberguide

Produced by: GOVERNING INSTITUTE

AT&T

NATIONAL CYBERSECURITY ALLIANCE

Contents

SHUTTERSTOCK.COM

DEPARTMENTS

REST OF THE BOOK

Publisher — **Alan Cox** alanc@erepublic.com

EDITORIAL
Editor: **Jim McKay** jmckay@govtech.com
Managing Editor: **Elaine Pittman** epittman@govtech.com
GT Editor: **Noelle Knell** nknell@govtech.com
Chief Copy Editor: **Miriam Jones** mjones@govtech.com
Copy Editor: **Lauren Harrison** lharrison@govtech.com
Staff Writers: **Jason Shueh** jshueh@govtech.com; **Colin Wood** cwood@govtech.com; **Eyragon Eidam** eeidam@govtech.com
Editorial Assistant: **Ryan McCauley** rmccauley@govtech.com

DESIGN
Chief Design Officer: **Kelly Martinelli** kmartinelli@govtech.com
Graphic Designer Pubs: **Kimi Rinchak** krinchak@govtech.com
Senior Designer Custom: **Crystal Hopson** chopson@govtech.com
Production Director: **Stephan Widmaier** swidm@govtech.com
Production Manager: production@govtech.com

PUBLISHING
VP Strategic Accounts: **Kim Frame** kframe@govtech.com; **Stacy Ward-Probst** sward@govtech.com; **Arlene Boeger** aboeger@govtech.com; **Shelley Ballard** sballard@govtech.com; **Karen Hardison** khardison@govtech.com
Sales Directors: **Tracy Meisler** tmeisler@govtech.com; **Melissa Sellers** msellers@govtech.com; **Audrey Young** ayoung@govtech.com; **Lara Roebbelen** lroebbelen@govtech.com; **Carmen Mendoza** cmendoza@govtech.com; **Deanne Stupek** dstupek@govtech.com; **Lynn Gallagher** lgallagher@govtech.com; **Kelly Schieding** kschieding@govtech.com
Account Executives: **Paul Dangberg** pauld@govtech.com; **Christine Childs** cchilds@govtech.com; **Rebecca Regrut** rregrut@govtech.com
Bus. Dev. Managers: **Lindsey Albery** lalbery@govtech.com; **Kathryn Nichols** knichols@govtech.com
Sr. Sales Administrator: **Kelly Kashuba** kkashuba@govtech.com
Sales Administrators: **Alexis Hart** ahart@govtech.com; **Jamie Barger** jbarger@govtech.com; **Jane Mandel** jmandel@govtech.com; **Morgan Rothenbaum** mrothenbaum@govtech.com; **Ashley Flynn** aflynn@govtech.com
Sr. Dir. of Sales Operations: **Andrea Kleinbardt** akleinbardt@govtech.com
Custom Media
Managing Editor: **Jeana Bigham** jbigham@govtech.com
Dir. of Web Marketing: **Zach Presnall** zpresnall@govtech.com
Web Advertising Mgr.: **Adam Fowler** afowler@govtech.com
Subscription Coord.: **Eenie Yang** subscriptions@govtech.com

CORPORATE
CEO: **Dennis McKenna** dmckenna@govtech.com
President: **Cathilea Robinett** crobinett@govtech.com
CAO: **Lisa Bernard** lbernard@govtech.com
CFO: **Paul Harney** pharney@govtech.com
Executive VP: **Alan Cox** alanc@govtech.com
Chief Content Officer: **Paul W. Taylor** ptaylor@govtech.com
Deputy Chief Content Officer: **Steve Towns** stowns@govtech.com
VP Research: **Todd Sander** tsander@govtech.com

Emergency Management (ISSN 2156-2490) is published quarterly by e.Republic Inc. 100 Blue Ravine Road, Folsom, CA 95630. Periodicals Postage paid at Folsom, CA and additional offices. Postmaster: Send address changes to Emergency Management 100 Blue Ravine Road, Folsom, CA 95630.

Article submissions should be sent to the attention of the Managing Editor. Reprints of all articles in this issue and past issues are available (500 minimum). Please direct inquiries for reprints and licensing to Wright's Media: (877) 652-5295, sales@wrightsmedia.com.

Subscription Information: Requests for subscriptions may be directed to subscription coordinator by phone or fax to the numbers below. You can also subscribe online at **www.emergencymgmt.com**

100 Blue Ravine Road, Folsom, CA 95630
Phone: (916)932-1300 Fax: (916)932-1470
www.emergencymgmt.com

A publication of e.Republic

Connectivity. Anywhere.

Secure, Reliable Access. Where You Need It. When You Need It The Most.

The Plum™ family of products' patent pending technology provides high-speed internet access to mission critical data and voice communications in really remote areas where cellular service is limited or unavailable with existing equipment.

Completely self contained. Extremely rugged and dependable. Easy to use and deploy.

Turn it on and in five minutes or less you have one to four secure wireless networks supporting 32 to 256 simultaneous users with battery life for one to three days.

The best continuity of operations solution available. See it in action at

PLUM · CASE™
PLUM LABORATORIES, LLC

www.plumlaboratories.com

Plum Laboratories, LLC, 513 Memorial Drive #208, Springfield, TN 37172 (855) 537-9990

"Excellent article! PREPARE, PREPARE, PREPARE!"

Preparingtx — in response to the article *Time Bomb* in the Summer 2016 issue

This article was well written, but omits some important details. Recent studies indicate that the southern portion of the fault (from near Eureka, Calif., to near Florence, Ore.) ruptures on average every 250 years, generating a quake of magnitude 8 to 9. The entire fault ruptures every 500 years on average, resulting in the magnitude 9 quake. It has been 316 years since the last one. The south coast is well within the window for this event. There may be more time in the north, but that is only a guess, and it is a fool's errand to rely upon that assumption.

The Northern California/southern Oregon area gets twice as many of these earthquakes as our northern brethren. It is critical that citizens prepare for themselves. The responder community will do its best to assist, but we are too few in number and not well funded.

No seaports will be left, not much for airports, roads out, bridges down, power down for a long time, water and wastewater systems inoperative, medical facilities damaged. It is not all doom and gloom, however. Look at the recent experience in Japan. "Their" subduction zone fault is similar to our own. Even in the devastated area, 95 percent of their citizens survived the disaster. With proper education and preparation, we can do the same thing here.

We need to educate our people (those who will accept the information), and get them to prepare for at least a few days without help. I strongly urge people to educate themselves about the potential disaster. Learn as much as possible about it and the effects it is likely to have on us.

Michael — in response to the article *Time Bomb* in the Summer 2016 issue

Yes ... I'm a geologist and physical geographer who specializes in hazards and mitigation. This will be worst disaster the U.S. has ever seen and probably ever will.

Sherry Young — in response to the article *Time Bomb* in the Summer 2016 issue

Insulated concrete-form homes add strength. Though they cost a little more than a concrete block home. Compared to building a wood frame home, which is far less, these type of homes are stronger and over time can save the owner money through heating/cooling costs.

I think insurance companies and possibly some other initiative to help offset the additional costs could get people to build this way especially in tornado- and hurricane-prone areas.

Robert G. Brookens Jr. — in response to the article *Joplin Study Spawns Recommendations* in the Spring 2016 issue

Disaster Preparedness

SHUTTERSTOCK.COM

One of the most 'terrifying' disasters in the offing is a Cascadia Subduction Zone earthquake in the Pacific Northwest.

By Jim McKay | Editor

The Weather Network identified in a March report four "terrifying disasters waiting to happen."

One was deadly, exploding lakes in Africa. These are rare events known as limnic eruption and happen when CO2 builds up over time from nearby volcanic activity. Another potentially catastrophic event would be the onset of giant space rocks hitting the Earth. This would be a global catastrophe, because particles in the atmosphere would block up to 70 percent of sunlight for the first couple

those on the coasts. The good news is that the last time this happened was 70,000 years ago and the "repeat" time would be 700,000 years.

The other disaster potentially in the offing is the Cascadia Subduction Zone earthquake. This scenario involves a magnitude 9.0 or worse earthquake in the Pacific Northwest that would be felt all the way down to Northern California. The Pacific Coast would have perhaps an hour of warning before the tsunami hit. As a reference point to how bad this earthquake will be, the recent earth-

ample time to prepare, and that preparation has begun. A similar quake is thought to have occurred in or before January 1700.

Scientists estimate that a recurrence would be due in about 500 to 600 years. But they don't know for sure. They also don't know how much seismic slip occurred during that quake in 1700. Did the subduction zone save anything?

"Faults tend to be pretty good at this. They don't always spend everything they have," said Brian Atwater of the U.S. Geological Survey Earthquake Hazards Program. There may have been a lot of "breakage" during the last quake or there could be parts of the fault that didn't break. That would be a way to get "better than 500 years' worth of slip in 300 years," Atwater said. Or maybe the earlier quake spent the "whole bank account" and the future event won't amount to much.

"That's part of the challenge of trying to present to a public audience scenarios for future earthquakes and their unknowns," said Atwater. "They don't happen like clockwork."

Rebekah Paci-Green is the director of the Resilience Institute and a professor at Western Washington University. She helped put together *Cascadia Rising*, a 182-page document that goes into alarming detail about the impending Cascadia earthquake and tsunami.

The document takes you through the scenario of The Quake. The daytime quake will sneak up on the region's population, feeling somewhat like a semi-truck passing by. As the shaking continues, some will forget their initial training. Some may run, but will make it only a few steps before falling. After about a minute, the shaking will begin to toss people about. Things not anchored will fall. Some people will have gotten under chairs, tables or something they think will protect them. Many will not.

The document says that coastal areas will likely feel it the worst. But down in Oregon and even Northern California, residents will know something is afoot.

SHUTTERSTOCK.COM

We appreciate your feedback, and we invite you to join the conversation at www.emergencymgmt.com or on our Facebook page at www.facebook.com/emergencymgmt

Genetec™

genetec.com

Pixels need perspective.

The details definitely matter, but security shouldn't be short sighted. At Genetec we realize that systems that work are systems that work together. Our software is the only one to bring together video surveillance, access control, license-plate recognition and enterprise security applications via a unified, cloud-enabled platform. Whether you're a security specialist, a police chief or a CEO, successful solutions see the whole picture, today and tomorrow.

Find out why Genetec fits at genetec.com/urbansecurity

By Jim McKay

Another Suspect Slips the FBI

Accused bomber Ahmad Khan Rahami is yet another example of someone with FBI facetime who has turned around to allegedly commit a terrorist act. It's also another example of the difficulties investigators face in our cover story. *Lone or Known Wolves?* examines the recent history — prior to Rahami being accused of planting explosives in New York City and New Jersey on Sept. 19 — of the task of uncovering potential terror suspects before they act.

... THE FBI NEVER INTERVIEWED ACCUSED BOMBER AHMAD KHAN RAHAMI, ALTHOUGH HIS FATHER SPOKE OF HIS FASCINATION WITH AL-QAIDA AND JIHADIST VIDEOS.

Apparently the FBI investigated Rahami in 2014. His father told the agency that his son was a terrorist and to watch him. The FBI was also told that Rahami was possibly trying to obtain explosives and was associating with bad people. He spent time in jail for assault, but the FBI found no evidence that he was radicalized. According to *The New York Times*, the FBI never interviewed Rahami, although his father spoke of his fascination with *al-Qaida* and jihadist videos.

This case exhibits the same type of pattern, where the FBI finds a reason to investigate an individual but deems him not to be a threat, only to have the individual prove to have been radicalized and carry out a terrorist act.

In the cases that you will read about in the cover story, the FBI has taken heat for not continuing to track the individuals, or at least alerting local law enforcement about the possibilities.

Certain Fate

One thing is for certain: Despite what some have said of the path forward for Rahami, if he is convicted of the bombings, he faces certain and grim punishment.

Consider where previously convicted terrorists have gone: Richard Reid, the "shoe bomber"; Ted Kaczynski, the "Unabomber"; Ramzi Yousef, involved in the 1993 bombing of the World Trade Center; and Boston Marathon bomber Dzhokhar Tsarnaev — all, among others, reside at ADX, the United States Penitentiary Administrative Maximum Facility in Florence, Colo. The emphasis here is on "maximum."

ADX is known as the country's secure supermax prison. Inmates here are housed in 7 x 12 concrete cells with concrete beds and concrete walls with no chance to see outside or to see other inmates. Many spend 23 hours a day in the cell.

Inmates are shackled when taken beyond their cells, and by design there is very little contact with guards, other prisoners or anyone else.

This is where Rahami could find himself if he is convicted — a concrete cell with no opportunity to see or feel the outside world ever again.

QUESTIONS OR COMMENTS?
PLEASE GIVE US YOUR INPUT BY CONTACTING OUR EDITORIAL DEPARTMENT AT EDITORIAL@EMERGENCYMGMT.COM, OR VISIT OUR WEBSITE AT WWW.EMERGENCYMGMT.COM.

GEORGETOWN UNIVERSITY
School of Continuing Studies

Hands-On + In Demand

MASTER'S IN **EMERGENCY & DISASTER MANAGEMENT**

Develop the skills needed to take action and lead response efforts when disaster strikes.

Explore our online, on-campus, and executive formats:

scs.georgetown.edu/edm2016

In the News

An "unprecedented" mid-August deluge of more than 20 inches of rain battered Baton Rouge, La., leaving at least 13 dead and forcing the rescue of more than 20,000 people by the Coast Guard and other first responders. At least 40,000 homes sustained at least some damage, according to a CNN report, and nearly half of the state's 64 parishes had to be closed. The Louisiana National Guard deployed 1,700 soldiers on a search-and-rescue operation.

APIMAGES.COM


15
M.P.H.

BIOMETRICS: RELIABLE, QUICK AND EFFICIENT — BUT NOT FOOLPROOF

In 1996, moviegoers watched as Ethan Hunt peeled off a lifelike mask and slinked through U.S. Embassy security and facial recognition systems in *Mission Impossible*. As one of those moviegoers, I absolutely lost my mind. Nothing was safe from someone who could steal your face and wear it around. Nothing.

At the time, biometric security measures looked so far away, seemingly relegated to government agencies like the CIA, classified military facilities and spy films. But today we live in a world that very much relies on our fingerprints, faces, voices and other markers to verify that we are who we say we are.

But all of this information being collected forces you to consider, what about those Ethan Hunt/James Bond-types clever enough to steal passwords you can never change? What happens when someone steals your biometric data and tricks a machine into believing they are you?

Believe it or not, it has already happened: A dead man's phone was unlocked using a fingerprint reprinted in a lab. It took some doing, but Michigan State University's biometrics expert Dr. Anil Jain and his team made it happen.

Jain was recently approached by detectives who asked him to unlock a murder victim's phone for potential evidence. With only the victim's full set of prints, he did.

When you ask Jain what he thinks the larger implications of biometrics are, he will tell you that as security measures go, biometrics offer something PIN codes and passwords can't. A thumbprint or an iris scan are not only harder to fake, they're also impossible to guess — but they still aren't perfect.

"Credential-based systems, ID card, passwords, PINs — they all sort of have their own weaknesses, right? Documents can be forged; documents can be stolen. Passwords and PINs, even though they are supposed to be random characters, people, if they want to remember it, [make it a] relatively simple combination of characters," he said. "That's why for higher security, we have started adopting biometrics. And there are some places where biometrics are the only way to find a solution."

—Eyragon Eidam

Future Buildings May Be Tough as Coconuts

If you've ever tried cracking open a coconut, then you're no doubt aware of how structurally strong they are. Scientists from Germany's University of Freiburg recently analyzed coconut shells to see what makes them so tough, and their findings could lead the way to building materials that are better able to withstand earthquakes.

Coconut shells consist of three distinct layers: the leathery exocarp on the outside, the fibrous mesocarp in the middle and the hard endocarp on the inside, which protects the developing seedling at the heart of the coconut. Using compression machines and an impact pendulum, the scientists observed the manner in which the endocarp distributes impact energy.

What they found was that the vessels that make up a coconut's vascular system — which take the form of angled, ladder-like structures known as vascular bundles — dissipate energy by deflecting cracks lengthwise, instead of allowing them to travel straight through to the inside.

It is now hoped that these vascular bundles could be replicated using textile fibers embedded within concrete. SOURCE: SOCIETY FOR EXPERIMENTAL BIOLOGY

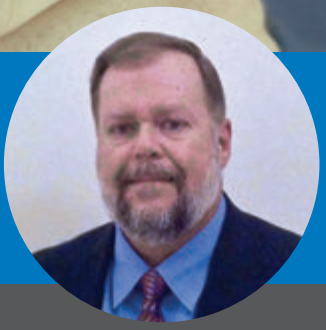
FATAL 'JIHADIST' ATTACKS IN THE U.S. SINCE 9/11

	Number of deaths
2016 / ORLANDO, FLA., NIGHTCLUB SHOOTING	49
2015 / SAN BERNARDINO, CALIF., SHOOTING	14
2015 / CHATTANOOGA, TENN., MILITARY SHOOTING	5
2014 / OKLAHOMA BEHEADING	1
2013 / BOSTON MARATHON BOMBING	4
2009 / LITTLE ROCK, ARK., SHOOTING	1
2009 / FORT HOOD, TEXAS, SHOOTING	13
2006 / SEATTLE JEWISH FEDERATION SHOOTING	1
2002 / LOS ANGELES AIRPORT SHOOTING	2

SOURCE: NEW AMERICA

As adoption of body cameras increases, many police departments are overwhelmed with how, when and where to store video. Adding to the challenge are various storage myths, which can cause agency leaders to believe they will be unable to afford the storage needed to support body cameras or that they will need to hire additional staff to manage the solution. In this Q&A, Ted Hayduk, a global consulting solution architect specializing in video surveillance, explains why body camera video storage is simpler than you may think.

TED HAYDUK, *Global Consulting Solution Architect, NetApp*



DEBUNKING THE MYTHS OF BODY CAMERA VIDEO STORAGE

Q: What are some common assumptions about body camera storage?

A: There are myths that body camera storage is complicated because: 1) cameras generate a significant amount of data; 2) you have to hire people who specialize in how to handle video data and; 3) it's a large project that touches all aspects of management. However, video is just another type of information that needs to be managed, similar to what agencies are already handling in paper, audio or still-picture form. Body camera information can flow through a department's standard policies and procedures with some minor changes. There are techniques and technologies that allow departments to easily control the video throughout its life cycle.

Q: What are some perceived challenges around body camera implementations?

A: There's a perception that when you take pictures, video or audio, you have to use the best technology available. Body cameras are intended to capture the interaction between citizens and officers — agencies don't need the best quality video to achieve this. A high-definition camera allows you to see images that are farther away, but the body camera range should be 10 feet and inward. The Department of Justice requires video footage used to identify an individual to have an image density of just 40 pixels per each foot of distance. By using the right tool for the right job, agencies can reduce their file size by four to five times.

Q: What are some best practices for capturing, handling and storing body camera video?

A: Agencies need to consider:

- **What is the mission of our body camera program?** This will help them determine what officers should be capturing and how cameras should be used.
- **How will cameras be assigned?** It's best to assign each officer a camera to create a sense of ownership and simplify the chain of evidence.
- **How much data will our cameras generate?** Officers should only use the camera while they are interacting with citizens. On average, between 1.75 and 3 hours of footage are captured per shift — that's about 1 GB or less per hour.
- **What are our data storage policies?** There are 29 states that have legislation on how body camera video should be stored and used, which can vary between 30 days and 1 year.

Q: What criteria should agency leaders use when selecting a data storage provider?

A: The cloud is one option and it's the preferred method for several vendors. However, the agency needs to understand what that means in terms of risk. Who encrypts the data? Who stores and processes it? It's the agency's responsibility to certify that CJIS-compliant vendors are actually following rules and procedures. Additionally, some agencies that sign up for long-term agreements find there are terms and conditions they didn't fully understand. Even if the cloud looks easy and affordable, consider the potential risks and look at your fixed costs over a five-year period. There are several environments that allow agencies to handle all of the data on premises. With an on-premises solution, agencies can determine who and what data is added or removed. Then, they can leverage the cloud to make safety copies because the encryption of that data is rendered by the in-house software before it goes to the cloud. In my experience, you can save 40 to 60 percent by going with an on-premises solution. It's important that police departments look at all available options, understand the issues about how body camera data is captured, and consider how to archive and manage it over time.

ENHANCING CAMPUS SAFETY

THE U.S. DEPARTMENT OF EDUCATION HOPES EMERGENCY PLANNING ON CAMPUS GOES BEYOND THE HISTORIC NORM. BY ADAM STONE

This spring, the U.S. Department of Education released its third version of the *Handbook for Campus Safety and Security Reporting* to help guide colleges in their continued implementation of the Clery Act.

Originally intended to bring greater transparency to campus crime reporting, especially around crimes against women, that law has been expanded in the decades since its inception. It now contains substantial language compelling schools to organize and document specific plans for issuing timely warnings and emergency notifications.

The Clery Act applies to some 6,000 colleges and universities that participate in federal financial aid programs. With the release of its latest handbook, the Department of Education says it is looking for these schools to take their emergency planning beyond the historic norms of academia.

"For years there wasn't much activism on campus and so schools stopped planning for those issues. Now we look at Occupy Wall Street and we see those things are back on the table," said James Moore, senior adviser for Clery compliance and campus safety operations in the Department of Education.

"Some schools haven't really thought about things like pandemic flu and how you would deal with 10,000 sick kids on your campus. And then there are things like terrorism, but not in the traditional sense: We have schools that do animal research, and that is potentially a target," he said. "We want to make sure that schools are thinking about all of this on a larger scale."

Around the nation, emergency managers at both large and small schools say they are taking the big view. They're using the Clery handbook as a springboard to hone their emergency communications plans and also as a means to deepen ties with emergency leaders in their surrounding communities.

The Clery Act doesn't say when or how a campus emergency team should initiate critical communications. It doesn't lay out the precise scenarios that might require a timely notification or prescribe specific means for reaching out to students and faculty. All it says, in effect, is that campus leaders need to have a well documented plan.

APIMAGES.COM

Emergency managers at colleges large and small are taking a wider view of emergencies and plans on campus.

At the University of Massachusetts Amherst, that plan rests largely in the hands of Jeffrey Hescock, director of university emergency management and business continuity for Amherst and four other UMass campuses. While Hescock uses an emergency text notification system powered by Rave Mobile Safety software, he said the technology is not the most important piece of the emergency communications puzzle.

"The texting is great, but you also have to have the plans and procedures and protocols behind it," he said. In most cases his emphasis is on timeliness, a process that ensures emergency messages don't get held up by bureaucratic roadblocks. That means ensuring frontline campus police dispatchers are authorized — and trained — to call a general alert. "We make sure we can get that message out as quickly as possible and not have multiple layers of people needing to review it."

Having the policy is great; having it documented, as per the Clery handbook, is even better. "We are big on standards — accreditation standards, best practices. We see a tremendous value in having a document that spells out clearly: Here is what we are going to do," Hescock said. "Going through that exercise helps us to define our processes even better."

At the five-campus University of Minnesota system, whose Twin Cities branch alone is host to some 80,000 individuals on any given day, Emergency Management Director Lisa Dressler depends on multiple levels of notification when urgent alerts are needed. In addition to sirens and an on-campus PA system, she also uses some email and — primarily — a text alert system to spread word of emergencies.

Her team pulled the alarm in early June during a severe weather event. While the heavy winds and dangerous thunderstorms hadn't reached the Twin Cities yet, the timing looked bad, with the storm due to arrive just as people were leaving work. "It was coming in fast and coming in hard. We knew there would be downed trees and power lines," Dressler said. "So even though it didn't meet the threshold for an emergency in terms of wind severity, which is what we would normally use, we still wanted to get that message out."

The incident went smoothly, with students, faculty and staff all alerted to seek shelter and keep themselves informed. It's the kind of thing Dressler plans for all the time, and she said the Clery requirements help her to lay those plans. "As part of the annual planning process my emergency management team will cross-reference what we are doing to the new handbook as well as to all of our other requirements. We'll make sure that we are collecting that information and rolling it into our already existing plans," she said. "It is all part of the same continuous improvement process."

At the Washington State University campus in Pullman, meanwhile, Director of the Office of Emergency Management Michael Gaffney casts a wide net to ensure he can get the word out to the roughly 28,000 individuals who populate the campus at the height of the school year.

Try to log into the main university portal for things like registration and finances, and you'll be redirected to a site asking you to first choose your preferred mode of emergency contact. For those who don't get pulled into the system this way, Gaffney also reaches out via the all-campus email list. He can push emergency messages on the university's apps that normally deliver bus information and campus maps, and there's also an emergency alert website. Miss all that, and there are still the loudspeakers and the sirens.

The annual review of Clery compliance gives Gaffney an opportunity to run through all these outreach efforts afresh. "The minimum threshold level is compliance, but we want to know: Can we provide even better information? Do we learn lessons from our tests that ought to be captured?" he said. In fact, yes. In one recent test of a confirm-receipt function, his team found that students, more so than faculty, needed to be sent test messages more than once in order to gain their attention. Now he's adding follow-up notifications into the broader warning procedure.

At the same time, Gaffney is working closely to communicate those changes to local emergency managers in the community. Campus emergency managers, along with their peers in city and county positions, agree that the Clery requirements can form a helpful foundation for their collaborative planning and communications efforts.

When Gary Jenkins took over as the Pullman, Wash., police chief and emergency management director in 2010 the city's emergency plan had just been rejected by FEMA as insufficient. As he set out to reformulate it, Jenkins saw that despite its massive population base, the university had never been effectively included in the city's emergency plan: In fact, the two had separate emergency plans.

As Jenkins set out to improve that situation, he found in the Clery Act a helpful ally. "Because of the requirements the schools have, they had a lot of things already put together, so that we just had to reformulate in terms of how FEMA wanted them to look, and that could then be the basis of our plans," he said.

The cooperative planning proved so effective that the city and surrounding county eventually joined the university's contract for emergency communications services. The Everbridge system allows university emergency leaders to

send high-volume text, email and telephone notifications. As co-users on the same contract, city and county emergency managers can reach across in support of one another. "Each of the emergency managers for each of the entities has the ability to send an emergency notification to anyone on the system," Jenkins said. "So if my staff or I were not available to send an emergency notification for whatever reason, one of the others could actually do it for me."

That level of closeness makes sense to Gaffney. "Anything that affects us is likely to have an effect on the city and the county," he said. As of mid-June the school's Board of Regents, the City Council and County Board of Commissioners all were in the process of reviewing a first-ever joint emergency management plan. Gaffney said Clery's documentation requirements were instrumental in bringing all the players together.

"The process of having to work out the details, to get it all written down, is really important. It requires strategic and tactical agreement on how things must and will operate between principle players," he said. "And now, if the personalities change, if there is a new mayor or a new City Council member, we won't have to repeat all of that process. We have the documentation as a starting point."

While these Minnesota and Washington campuses may dominate their local scene, with their tens of thousands of students, faculty and staff, these same town-and-gown issues play out at smaller colleges as well.

Take for instance Michigan Technological University: With its 7,000 students, mostly non-residential, it's located on the farther reaches of Michigan's Upper Peninsula, some 10 driving hours from Detroit. While it may seem remote, this small school has many of the same cares as its big-city siblings.

"If there is an armed intruder, a hostile intruder, if there is a fire or a chemical spill, we plan for all of that. We have written scripts for bomb threats, hostile intruder," said Jennifer Donovan, who as part of the public affairs team on campus also serves on the incident command team. "After Virginia Tech, campuses really started paying attention to all of these things. That was when our incident command team was developed."

One of her team's roles is to share what it knows with those off campus, supported in part by the Department of Education handbook. "It keeps us all on the same page. When we talk about what is required of us, our county emergency management people can see exactly what we are doing and why. The fire and police and ambulance people can see what viewpoint we're coming at it from," she said.

The Clery Act's emphasis on communications has been especially helpful in allowing the school to work out crisis response protocols with the surrounding health-care community. "If we have an emergency that involves injuries or fatalities, we have to work very closely with the hospital on who tells the media what," Donovan said. "So it helps to have that written policy that says what we are going to do. Then we don't have to figure it out on the fly."

Others point to the specificity of language as a boon. "It's the difference between 'lockdown' and 'shelter in place.' A high school will use the terminology 'lockdown,' because it is just one or two buildings with controlled access — one way in and one way out. A campus like ours with 352 buildings, there is no button to push to lock that down. So we talk about sheltering in place," Hescock said.

That can matter to an outside responder arriving on scene. "They need to know whether all the doors are going to be locked when they get here or whether those doors will be open," he said. With help from the school's Clery compliance, "that's something they can know before they get here."

As the new security handbook begins to circulate, Moore at the Department of Education said he is hopeful that city and county emergency leaders will engage with the document, using it as a springboard to strengthen emergency planning both for themselves and for their local colleges and universities.

"If you look at a small liberal arts college, a lot of them have never had to go through the steps. They may have a very small police force. They don't know where their closest Level 1 trauma center is because they have never thought about it," he said. "If that county or city emergency manager knows that, they might be able to help that campus emergency manager to fix the hole. Then they can bring the schools into their larger programs to make sure there are seamless connections between the plan for the large community and the plan for the school."

adam.stone@newsroom42.com

AT A GLANCE

The Clery Act requires that campuses have documented plans for issuing both emergency notifications and timely warnings. What's the difference?

EMERGENCY NOTIFICATION

Scope:
Wide focus on any significant emergency or dangerous situation

Why:
Triggered by an event that is currently occurring on or imminently threatening the campus. Initiate emergency notification for any situation involving an immediate threat to the health or safety of students or employees.

Where:
Applies to situations that occur on campus.

When:
Initiate immediately upon confirmation that a dangerous situation or emergency exists or threatens.

TIMELY WARNING

Scope:
Narrow focus on Clery crimes

Why:
Triggered by crimes that have already occurred but represent an ongoing threat. Issue a timely warning for any Clery crime committed on campus that is reported to campus security authorities or a local law enforcement agency and is considered by the institution to represent a serious or continuing threat to students and employees.

Where:
Applies to crimes that occur anywhere on Clery geography.

When:
Issue a warning as soon as the pertinent information is available.

Source: *Handbook for Campus Safety and Security Reporting*

CORPORATE PREPARED

WELLS FARGO

NESS

The Mobile Response Unit is a 75-foot, heavy-duty "office on wheels" that takes banking services directly to customers after a disaster.

By Adam Stone

Wells Fargo's regional emergency managers embrace resilience.

Is corporate America ready to cope during a disaster? Arguably not. In one recent survey, 22 percent of private-sector workers told CareerBuilder their companies don't have plans in place to deal with fire or flood. Increase the severity of the event, and confidence plummets further. For example, 41 percent said their company isn't prepared to deal with "physical attack from another person."

Wells Fargo Bank likes to think of itself as an exception to the rule. With a 2015 net income of $23 billion, and 265,000 employees in 9,000 locations, there is much to safeguard here. The burden falls largely to Vice President of Incident Management Christopher Terzich and his team of 26 strategically distributed emergency managers. Together they anticipate crises, ensure employee safety and help customers gain access to their finances even in times of disaster.

The team can cite the usual round of fundamentals in explaining its approach to driving business continuity. There's experience: FEMA-trained managers, some with three decades' police work to their credit. There's the ongoing preparedness program, supported by a corporate intelligence unit that tracks a range of potential hazards on a global scale. Topmost, though, is the matter of outreach. Wells Fargo emergency professionals say their ties to the community are the bedrock that underlies their efforts.

During an emergency, businesses worry about employees, customers and community — usually in that order. "In most companies it is fairly sequential, and community outreach is the third priority," said Peter Ohtaki, the bank's San Francisco Bay Area regional emergency manager. "At Wells Fargo it is very much at the front of our work efforts and priorities."

The bank has done extensive work to build up its credibility in the emergency management community, to make itself a trusted partner. In return Wells Fargo has become a go-to player. It has struck formal relationships with regional emergency organizations, and its crisis teams routinely are invited into the emergency operations center.

Things didn't always run this smoothly, said Terzich, who has been with the bank for almost 30 years. He recalled the mood of self-congratulation when the emergency team unveiled its first corporate disaster preparedness plan on Sept. 10, 2001. "We were quite proud of ourselves — until the very next day, when we realized how much more there still was to do," he said.

In the ensuing years, Terzich has become an embodiment of the bank's outreach approach to emergency readiness.

He has served as president of the InfraGard Minnesota Members Alliance, a partnership between the FBI and the private sector that shares information and tactics for protecting critical infrastructure and key resources. He chairs the Regional Consortium Coordinating Council, one of the partnership councils recognized by the U.S. Department of Homeland Security in the National Infrastructure Protection Plan. He also served as a working group member on the National Infrastructure Advisory Council, giving input on critical infrastructure and the National Incident Management System.

What all those activities add up to, he said, is the ability to get timely information and make smart decisions. Terzich pointed for example to the recent papal visit to Philadelphia, a mass crowd event in an area rich with Wells Fargo assets. "We had team members taking part in the planning effort for months and months, looking to see how we could all come to work, while still maintaining security," he said.

Those relationships can make a tangible difference in times of actual emergency. In the midst of 2012's Hurricane Sandy, when some groups made a premature call for evacuation, Terzich was able to tell his people to stay put, based on information from more trustworthy sources. "At a time when there was all sorts of conflicting information, we were able to push back," he said. "When information was ambiguous we were able to ask for clarification."

That same experience has played out among the bank's regional emergency management leaders across the nation.

FLICKR/ERIK DROST

The Republican National Convention in Cleveland raised concerns that brought a needed coordination between Wells Fargo and agencies like the Secret Service, and DHS, plus state emergency managers and city public safety officials.

Wells Fargo's emergency management effort may stretch across the global enterprise, but it is structured to play out at the local level, with regional managers situated centrally to the bank's activities, including the United States corps, plus one in Hong Kong. "Our goal is to mirror where our customers are and where our communities are," Terzich said. "A foot of snow in Minneapolis in winter is not a significant issue, whereas three inches of snow in Charlotte [N.C.] can bring the city to a standstill. So we want to have as much local control as possible."

CORPORATE CONTINUITY CORE

The Incident Management Team makes up the heart of the Wells Fargo emergency management operation, which is responsible for keeping employees safe and ensuring business continues even in times of crisis. Specifically, emergency managers are charged with providing:

- An enterprise focus to ensure that team members respond safely during an emergency at work and for the enterprise to prudently respond to crises of any origin and scope.
- Situational awareness obtained through monitoring and expert review of available information and strong information-sharing partnerships and relationships within communities and public agencies.
- Consistency of messages internally and externally.
- Consistency in team member safety and well-being issues.
- Effective prioritization of resources in response.

Source: Wells Fargo Team Member Handbook January 2016

Chris Cowart exercised that local control when the Republican National Committee came to Cleveland this summer. Based in Georgia, he's a regional emergency manager overseeing 93 site emergency plans covering 20,000 employees in seven states.

The convention fell in his territory, a mass event that raised concerns about everything from transportation disruptions to public demonstrations. To prepare, he coordinated with Homeland Security, the Secret Service, state emergency managers and city's public safety. "We want to be as prepared as we can be, and that means we want to share as much information as we can, to make sure everybody has the same information and shares the same messages," he said.

The bank shares more than information. In response to disasters, such as the Texas flooding in spring 2015, it has sometimes deployed a Mobile Response Unit. This 75-foot, heavy-duty "office on wheels" takes banking services directly to customers after a disaster. The unit has private offices and is equipped with computers, a cellular data feed with satellite backup and self-contained generators. Bank employees can offer mortgage assistance, process insurance claim checks and deliver other recovery-related services.

Cowart said the preparedness community has welcomed the participation of a private-sector partner. "Many of the state emergency management agencies now have a business-sector liaison. They recognize the value of working with the private sector," he said. "If a community is going to recover quickly after a disaster, businesses have to be open. Commerce has to be flowing."

It flows first at the local level and so that's how the bank organizes its incident management efforts. At the same time, though, there are some advantages that come with being a global entity. Wells Fargo's emergency managers say they will frequently tap the organization for higher-level expertise.

"We have a number of experts — from corporate properties, from risk and insurance, from business continuity. There are a lot of people who can assist us when we have something that takes a lot of horsepower," Cowart said. "That allows us to manage it at the local level, and then to escalate information up through those established channels."

In fact, that high-level expertise may even help Cowart and other emergency managers to pre-empt crises, by preparing them with a deeper level of threat intelligence than a typical corporate incident manager might enjoy. Specifically, the bank's emergency apparatus includes a threat intelligence unit composed of four individuals: one in Minnesota, one in Arizona and two in Washington, D.C., whose job is to track any and all threat activity that could impact bank interests.

They watch for hurricanes and track wildfires. They monitor disease outbreaks and keep tabs on political unrest — "any kind of emerging external danger to our customers and our team members," Terzich said. "They don't attempt to be all-seeing, but they do attempt to identify when a situation is changing. They watch when there is instability, and they look at the possible trajectories."

The team sends out travel advisories and weather watches. It offers economic updates, and it churned out a steady stream of reports around Brexit, Britain's recent vote to leave the European Union. Does all of this touch on emergency management? The point is: It could. "If you see a threat, you don't necessarily have to respond to it, but you do have to make sure somebody has the ball. You have to get it to the right place," said Terzich. The threat intelligence unit fills in that piece of the puzzle.

Resources such as these have helped the bank to establish itself as an integral element of the emergency team in many communities.

In the South, for example, the Contingency Planning Association of the Carolinas numbers Wells Fargo among its sponsors, alongside corporations like Duke Energy and Lowe's, as well as other financial institutions including BB&T and Bank of America.

In the Midwest, Regional Incident Manager Jeff McClaran chairs the Safeguard Iowa Partnership. He brings a sterling pedigree to both tasks: An emergency medical technician, he is also a certified master anti-terrorism specialist, certified homeland security level IV, a search-and-recovery diver and a weapons-of-mass-destruction-rated first responder.

In Northern California, Ohtaki said the bank is deeply integrated into the local emergency response community — a level of involvement that has been in the making for some time. In 2012 the bank signed a memorandum of understanding with the California Emergency Management Agency (now the Governor's Office of Emergency Services), agreeing to provide mutual assistance and share resources.

"Our private partners play a critical role in emergency response," Mark Ghilarducci, the agency's director, said at the time. "Having organizations such as Wells Fargo who are

willing and able to help provide emergency assistance and resources to affected communities in times of need is a benefit to all Californians. These partnerships increase our resources, help us better coordinate and deliver the services our residents will need during times of emergency, and they help our local communities get back on their feet."

As a result, the Wells Fargo team is often invited to be a part of the EOC to help coordinate emergency response. The bank can help to deploy mobile ATMs, for example, to ensure residents can access cash during a crisis.

Ohtaki's role goes beyond the financial sector. He teams with technology partners to help deliver mobile communications, and he works with the food and beverage industry to coordinate delivery of emergency supplies. "We can help mobilize resources in the private sector across all our partners, to help make sure those things can be accessed and deployed in the way that they are most needed, without getting in the way of what the public sector is doing," he said.

Ohtaki got all those gears turning when Super Bowl 50 came to the region in February, bringing with it two weeks of frenetic activity in and around the San Francisco Bay Area.

"We had to make sure that our employees could get in and out of work safely, that they were well prepared and knew what was going on," he said. Teaming with multiple municipalities as well as authorities from transit, public works and elsewhere, Ohtaki generated a steady stream of information around the event. "Many of these activities took place during work hours and we wanted people to be knowledgeable about the resources that were available to them."

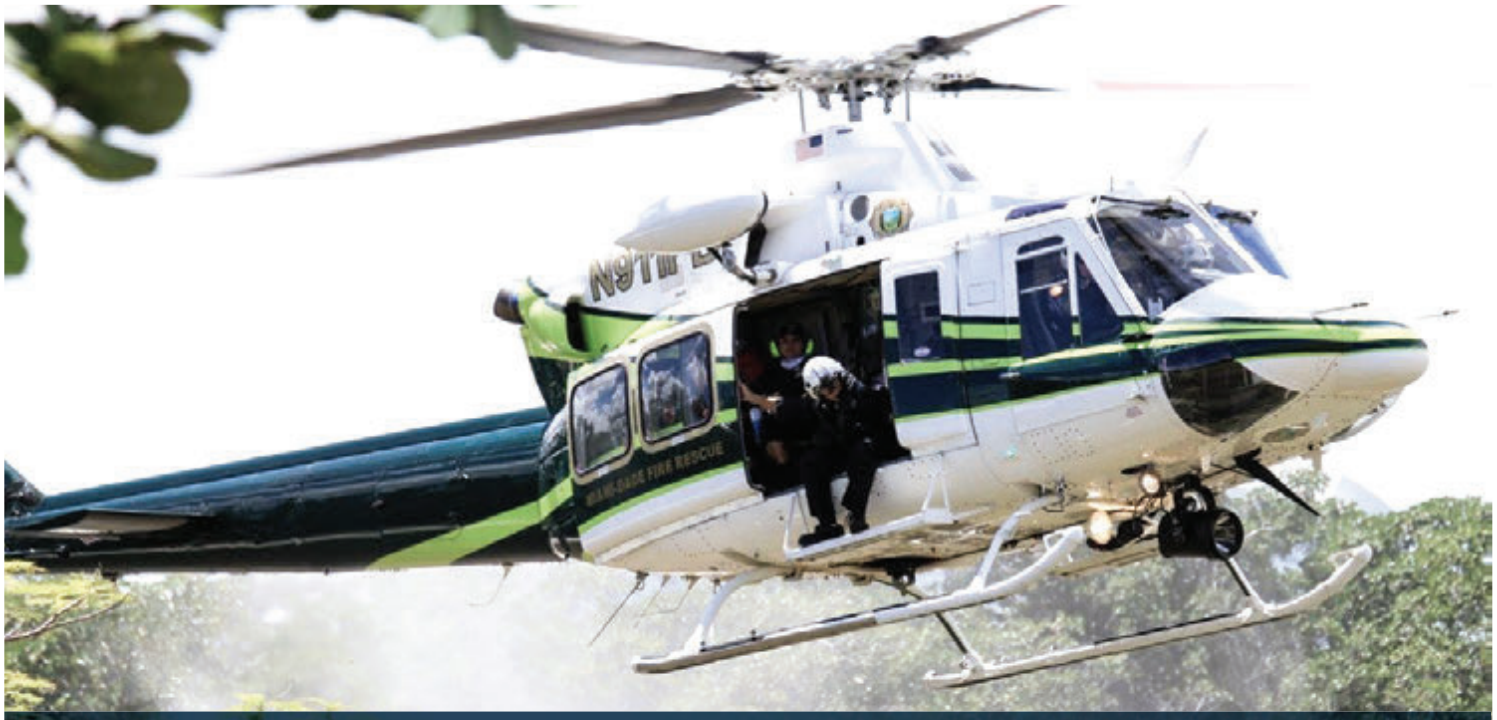
A former councilmember and mayor of Menlo Park, Calif., Ohtaki chaired the California Resiliency Alliance before joining Wells Fargo. Other members of the bank's emergency management cadre come directly from the first responder world, some with nearly 30 years' experience in police and fire work.

That hands-on background can be a valuable asset in translating corporate emergency priorities into tangible action.

"Because they have experience as first responders, they bring that special expertise to the table. They understand how it all works and especially where to find the resources," said Terzich. As disaster professionals, they know where to find the latest threat data and when to ring the alarm. They know how to keep employees safe, and just as important, how to keep them calm. "My team's job is also to vet the information, to make sure we are not acting just because somebody tweeted something."

adam.stone@newsroom42.com


Don’t Wait.
Communicate.
Make your emergency plan today.
Visit Ready.gov/communicate
Ad Council
Ready
FEMA



FIELD TESTED AND READY

At one school, the final exam includes heat, mosquitoes and MREs. **DAVID SILVERBERG**

PHOTOS BY DAVID SILVERBERG

Bockistan lies in ruins.

A magnitude 7.8 earthquake has rocked the country, killing hundreds. Large apartment buildings have collapsed, communications are out, airports and seaports are closed, electricity is dead, and water isn't flowing.

Into this situation come 42 Americans ranging in age from their early 20s to their late 50s, full of enthusiasm and determination to do good and carrying bags of gear. But they're entering an unfamiliar world in a state of disaster, full of cultural pitfalls and government red tape.

What's more, this is their final exam — not to add any pressure.

Bockistan, of course, is fictional. Supposedly situated between Pakistan, Nepal and India, it should be surrounded by the towering mountains of the Himalayas. The temperature should be cold and the air should be thin. Instead, the rescue of Bockistan will take place under a blazing sun in a flat Florida field amid rampant mosquitoes and thick, humid, 100-degree air, only occasionally relieved by a light breeze or a pounding tropical rain.

But the exact details of the response to the great Bockistani earthquake of July 2016 are less important than the larger purpose: a sophisticated master's-level course in disaster management that culminates in a unique field exercise. It's a course and an exercise that physically and mentally test its students, teach them some of the pitfalls of international response, and at the same time build larger organizational resilience in the school and the surrounding community.

THE RESPONDER AND THE SCHOOL

On the bookshelf in Ruben Almaguer's office are the relics of a life spent responding to disasters.

There's a chunk of brick from the Alfred P. Murrah Federal Building in Oklahoma City, a hunk of steel from the World Trade Center and a partially melted engine part from Flight 77, which hit the Pentagon on Sept. 11, 2001. There are relics from earthquakes in Venezuela, Colombia, Armenia, Turkey and Taiwan. Hurricanes Katrina, Opal and Mitch yielded their artifacts, as did floods in Mozambique.

Almaguer served at all of them.

It's an impressive collection for a man who started his career in the Miami-Dade County, Fla., Fire Rescue Department, rising to division chief before going to Florida's Division of Emergency Management, where he served as deputy director and interim director. From there he served a stint heading up air operations and emergency medical operations for Monroe County, Fla.'s southernmost jurisdiction, which includes the town of Key West, the other Florida Keys and vast expanses of Everglades National Park. Along the way, Almaguer collected a master's degree in public administration and one in homeland security and defense from the Naval Postgraduate School.

BOCKISTAN IN RUINS
A magnitude 7.8 earthquake rocks a fictitious country, and master's-level Florida International University students respond.

In March 2012 Almaguer joined Florida International University (FIU) as assistant vice president for disaster management and emergency operations.

This was a coming together of a unique institution and a unique individual, and the two complemented each other in unusual ways.

FIU is a young school, founded in 1965 as Miami's first public research institution and initially situated on the site of an abandoned airfield. From these humble beginnings it has grown to include seven campuses around the Miami area. The student population has grown by leaps and bounds, from an initial enrollment of 5,667 in 1972 to more than 54,000 today, and it's still expanding.

With 190 degree programs, the school has a very practical bent and an entrepreneurial spirit. It serves a heavily immigrant, working population — 61 percent of the student body is Hispanic — and they bring an eagerness and earnestness to their studies that can be felt on campus. Likewise, the administration is unafraid of new ideas and actively seeks new fields of endeavor.

So when Almaguer proposed a new Academy for International Disaster Preparedness, the administration was ready to listen.

In 1992 Hurricane Andrew blasted through the campus, shearing trees and ripping off roofs, doing $6.3 million worth of damage. In characteristic purposeful fashion, FIU students responded by organizing relief efforts focused on a campus center. In the longer term, the National Hurricane Center, which had its physical radar dome and instruments destroyed at its usual site, moved to a hurricane-resistant facility on the FIU campus. The school hosted a conference of hurricane experts six months after the disaster and created an International Hurricane Research Center. In 2012 it unveiled the country's most powerful hurricane simulator, known as the "Wall of Wind," on its engineering campus. It also created an entire disaster management

department complete with a sophisticated, hardened campus EOC.

When Hurricane Isaac approached south Florida in 2012, FIU shut down the campus for two weeks.

"The provost said that they made the best decision with the information they had, and when you're in emergency management, that's what you want to hear," recalled Amy Aiken, the school's director of emergency operations. "The big takeaway was that the policymakers understood that it was important to make a clear decision with the information we had. This administration takes emergency management very seriously and they're engaged."

Indeed, in contrast to many schools that have haphazard or low-priority emergency management offices, here emergency management sits high in the university's hierarchy as a stand-alone department and a key priority. Twice a year the school conducts tabletop exercises based on scenarios from the U.S. Department of Homeland Security and top university officials participate.

"University management is disciplined," said Aiken. "The focus is clear. We're pretty high up in the food chain, which makes it possible to build the program."

Or, as Almaguer put it: "This is the best prepared university before it happens, while it happens and after it happens."

THE MISSING YELLOW TEAM

The Bockistanis are pissed.

Instead of reporting first to the United Nations' On-Site Operations Coordination Center (OSOCC) before establishing a base camp like they were supposed to do, the Yellow Team has wandered off to parts unknown.

That's a no-no in this devastated country. Having gone through bag checks and medical examinations at their initial gathering point in a university building, the entire class was transported to Bockistan — in this case, FIU's Biscayne Bay Campus. The initial OSOCC visit after arriving in the country is very important. There, team leaders are briefed on the situation and issued satellite phones and radios, which the Bockistani government insists operate on only a single frequency, and given the GPS coordinates to their base camps.

The Green, Red, Orange and Blue teams managed to get through border security despite a lot of hassles — a border guard found ammunition in one of their packs — and find their way to the OSOCC. They did this despite bulky GPS devices whose batteries didn't work.

But somewhere out there, the eight-person Yellow Team, representing European Relief, a fictional nongovernmental organization, is missing.

What's more, these students are old enough and experienced enough to know better.

The academy's first cohort is a mixed bag, but all are coming with real-world professional experience. Nearly all — 96 percent — are currently employed. Of the 42 people accepted into the class (out of 62 applicants), 34 percent come from law enforcement, 18 percent from fire service and 14 percent are in the military, with the largest group coming from the U.S. Marines. The private sector contributes 24 percent, nongovernment organizations 8 percent and 2 percent are already in emergency management. The average age is 43.

Imani Bradford, 24, is an example of a private-sector student. In her day job, she handles logistics for one of the 18 cruise lines that operate from Miami. "I do a lot of logistical coordination in my job and I like it. I realized that emergency management is a lot of coordination too," she said. Another cruise line employee taking the course is Oscar Celorio, 42, a claims adjuster who is also part of his line's "go-team" that responds to crises wherever they occur.

Christine Kruse, 46, is a crime scene detective with the Miami-Dade County Police Department. Learning disaster management fit in with her additional law enforcement responsibility for disaster mortuary response. Darwin Villavicencio, 42, is also a detective, a Marine Corps veteran and an FIU undergraduate. He's seen disaster up close: He has been deployed to both New York and Haiti.

Jose Herrera, 53, is a chief fire officer and nurse with Miami-Dade Fire Rescue. Arriving to the United States from Cuba at the age of 4, the treatment he received for a job-related injury while working at an airport so impressed him that he switched his career from aeronautical engineering to emergency medicine. He's spent 33 years in fire and rescue and loves it, but is now seeking to transition into emergency management. "It's a little bit difficult but just as rewarding," he said.

Rod Elkins retired after 26 years of active duty in the U.S. Coast Guard and now works for the service in a civilian capacity. A member of the Coast Guard's strike team responding to worldwide disasters, during Hurricane Katrina

AFFORDABLE AND ACHIEVABLE

Nearly all of the program's students are employed and most in first responder-type professions, a big factor in designing the course.

he was in charge of the agency's response in Mobile, Ala. Now he's seeking to add an emergency management degree to his resume.

Understanding the time demands and requirements of a working, professional student body like this, Almaguer and his team designed the course to be both affordable and achievable. Tuition is $25,000 and includes teaching materials like books, which can run an additional $4,000. The class meets every Saturday for one year with only four holidays and is culminating in this three-day exercise. That's in contrast to most master's programs, which can range in cost from $30,000 to $120,000 and take anywhere from a year and a half to three years — something especially difficult for working students.

That single year of coursework is one of the most attractive aspects of the program, the students said.

During the class, students take nine courses with titles like Comparative Disaster Management Systems, Disaster Response and Recovery, Introduction to Vulnerability Analysis and Hazard Mitigation, and Field Operations.

In any other program, all this would culminate in a written examination or thesis. But here it ends in lugging heavy bags through sweltering heat and trying to figure out what is going on in Bockistan as the students apply everything they've learned in the classroom and are graded on their responses.

Finally, the Yellow Team shows up at the OSOCC. The United Nations representative, played by Jennifer Beatty, a serving official in the Office of U.S. Foreign Disaster Assistance, attached to the U.S. Southern Command and a veteran of Afghanistan, has grim news for the Yellow Team leaders: The entire team has been declared persona non grata by the Bockistanis and is being kicked out of the country.

It will take a trek back to border security and the intervention of the U.S. ambassador to Bockistan to keep them in the country. But the lesson is learned: When deploying abroad to provide disaster relief, good intentions are not enough. Strict protocols and procedures must be observed, particularly when it comes to credentialing and host country acceptance — not a mistake they're likely to make again.

THE BONDS OF BOCKISTAN

Over the next two days, the students go through the hurdles of international disaster relief. They speak to Bockistani officials — portrayed by veteran responders — about the situation on the ground, trying to get a comprehensive view of the disaster. Emergency medical care instruction is provided by world-recognized exotic disease expert Dr. Aileen Marty, and water purification and sanitation are covered by Franklin Broadhurst, speaking from his own experiences in Afghanistan. They receive instruction in satellite communications, erect tents and chow down on meals-ready-to-eat (MREs). They're pounded by rain that falls in cascades and struggle to stay hydrated in the suffocating heat. And they work both early in the morning and late into the night, collecting information and filing reports.

Given the close relations between the FIU faculty and local emergency response agencies, they're also visited by Miami-Dade responders and get instruction in helicopter operations and safety before being taken to remote locations to continue their situational reporting. The U.S. Coast Guard provides a boat to ferry them, and they receive instructions in maritime operations.

A string of VIPs come by to view the exercise: Curtis Sommerhoff, director of the Miami-Dade County Office of Emergency Management, who has used FIU interns in his office and worked with the university to develop software programs, test products and study threats such as storm surge; David Paulison, former administrator of FEMA, who worked with a number of FIU faculty during his time in Washington; and Dave Downey, chief of Miami-Dade Fire Rescue.

The visits and personal contacts being made help cement the relationship between the surrounding response agencies and the students, as well as among the students themselves, who will be the fire and police chiefs and emergency managers of the future.

Then, after three days, it is over. In a moving nighttime ceremony under an open tent, huddling from sheets of rain, the students exchange gifts, receive challenge coins, and speak about the meaning of the course in their personal lives and their pride in being the first cohort. The next morning, they dismantle the tents, pack the equipment and eat their last MREs.

From there the students are bused to the university's EOC for an evaluation. They fill out forms rating the experience and the entire course, and make suggestions for the next cohort.

It's an emotional farewell. Over the year, and especially the last three days, they've bonded and shared a formative experience. The faculty provides statements praising their achievements and recounting how far they've come. The feeling in the EOC is warm and fuzzy as well as collegial. The sense of accomplishment is palpable. New friendships have been made.

Then someone turns on the EOC monitors and into the room comes breaking news: Three police officers have been ambushed and killed in Baton Rouge, La.

The talk freezes and a silent chill descends. This is real and immediate. The responders in this room will be returning to streets where disasters can occur at any time. But they will be that much more prepared for both the big events and the little ones. And so will the school and the broader community.

Reality has returned. Bockistan is suddenly very far away.

SHUTTERSTOCK.COM

The 911 Cyber Challenge

Increased connectivity brings cybersecurity threats to 911 call centers.

By David Raths | Contributing Writer

Emergency Management has published several articles about the movement toward a next-generation 911 (NG911) system based on modern Internet protocols that will allow responders to take advantage of capabilities such as text and video messaging.

Beyond the capability to send and receive texts and multimedia, there are other benefits to the new types of networks. Public safety answering points (PSAPs) will be able to transfer calls and activate alternative routing to share the burden during an emergency or when they are closed by disaster.

But accompanying all these important benefits of the switch from analog to digital, one challenge looms large: the increased risk of cyberattacks on 911 call centers once they are connected to so many devices and other networks.

With the current generation of 911 networks, PSAPs have seen telephony denial-of-service attacks in which attackers flood a call center with calls to disrupt service. There have been more than 300 telephony denial-of-service attacks against public safety organizations, including PSAPs, police departments, hospitals and fire departments in the last couple of years. Along with the high-profile ransomware attacks on hospitals, several police departments also have been victims.

Jay English, the Association of Public-Safety Communications Officials International's (APCO) director of communications center and 911 services, said PSAPs could be vulnerable to distributed denial-of-service attacks, which attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. "In order to take out a police department, the attacker has to obtain access to that police department and make a dedicated attack," he said. "But in order to take out five police departments and five fire departments, a hospital and an EMS agency, all they really have to do is find one PSAP that serves all of them. A single attack could affect multiple responding agencies."

English, who is a former PSAP director, said that as we move toward NG911, PSAPs are going to become just as vulnerable as any home computer or wireless phone, laptop or tablet.

"If you talk to directors of the largest PSAPs in the country, even they are not aware of the level of the threat they face today," English said. "We have operated in a very secure, closed-loop analog environment for decades, and now as we move to an open IP environment we will be subject to the same kind of threats and multiple-vector attacks that any IP-based system is vulnerable to. So we have to start educating our folks and rethinking our defensive strategy."

The interconnection with other systems and networks adds to the level of complexity. "Not only do you have the 911 inbound traffic, you also have the computer-aided dispatch [CAD] system, and both are dependent on GIS databases," said English. "You have records management systems for all the agencies that tie into that CAD. All these are becoming IP-based and integrated, and for good measure throw in FirstNet, which is IP-based. All of a sudden you have end-to-end IP networks and end-to-end vulnerabilities. We have to defend not just a single element, but multiple elements across the enterprise. And we have to do it 6,000 times, because there are 6,200 to 6,700 PSAPs and every one of them has to be defended."

Scott Somers, a professor in Arizona State University's College of Public Service and Community Solutions, agreed with English that this is a far more complex and dynamic problem than we have seen historically.

"It is going to take money and expertise to stay vigilant," said Somers, who is a senior fellow at George Washington University's Center for Cyber and Homeland Security. "This is not a one-time thing. It is not buying a device in order to protect a system; it is monitoring threats and addressing them as they emerge. It is a very dynamic concern."

One approach PSAPs can take is to start collaborating more to share best practices and threat information, Somers said. "PSAP operators tend to be in law enforcement, EMS or fire bureaus, and their business is being first responders, so they may not have much knowledge about potential cyberthreats, and those threats are always evolving," said Somers, who also served on the FirstNet Public Safety Advisory Committee and SAFECOM Executive Committee.

Somers recommended that the federal government work with PSAPs and the private sector to share information on threats. One model already in place is the Multi-State Information Sharing and Analysis Center, which offers cyberthreat prevention, protection, response and recovery for state and local governments.

Somers also is concerned that PSAPs with fewer financial and manpower resources may fall behind. "If you look at 911 call centers as they convert to NG911, you will find great diversity in approaches to confronting the cybersecurity threat," he said. "Cities like New York and other large metropolitan areas are putting a lot of money into it because they have more revenue and more resources. The smaller ones may not have the funding or expertise to address the emerging cyberthreat. We see that a lot in other areas of preparedness, so why would this be any different?"

The nation's 911 call center executives must see their function as part of the country's critical infrastructure, said Keith Fricke, a principal consultant with Overland Park, Kan.-based tw-Security and a former health system chief security officer. "As they move to an IP-based infrastructure, it is crucial that security is baked into that evolution. They will be subject to the same digital threats affecting all other members of the critical infrastructure." He recommended they become active members of the local chapter of InfraGard, a partnership between the FBI and the private sector to share information and intelligence to prevent hostile acts against the United States. "They can network with other people in their industry and in other industries to tap into the collective knowledge out there to guide them in securing themselves," Fricke said.

APCO's English, who served on the cybersecurity working group of the Federal Communications Commission's Task Force on Optimal PSAP Architecture (TFOPA), said the task force recognized that security has to be baked into the architecture upfront.

"You can't build a system and then decide we have to protect it," he said. "By then it's too late. The PSAP community is very good at being flexible and scalable as long as they are educated and know the threat they are facing. Like anyone in public safety, we are used to addressing threats head on, but we have to know what it is and how to defend against it."

A January 2016 TFOPA report proposed the creation of an Emergency Communications Cybersecurity Center. The idea is to create a security operations center designed to tie together information from multiple PSAPs and defend PSAPs as an enterprise rather than a stand-alone element.

As they work on NG911 networks, English said, PSAP directors should prepare lists of questions for vendor partners. "I approach vendors as partners because I don't want someone to sell me hardware and drop it off at the front door and leave. I want someone who is going to be working with me on a solution. To do that, they have to be willing to answer those tough questions and help me defend my enterprise," he said. "For PSAPs that are updating from analog systems that have been in place for 10 years, this is a brave new world. They should draw up a checklist from the TFOPA report and the NIST [National Institute of Standards and Technology] cybersecurity framework for creating an RFP and better understand which vendor is going to be a partner versus which just wants to sell you some hardware."

English said that if this transition is to take place over the next five to 10 years, PSAPs have to start talking about it now. "As with anything in government, if you start talking about it and planning for it now, you just might get it three years from now and it will take two years to implement, so five years from now we may be able to do something."

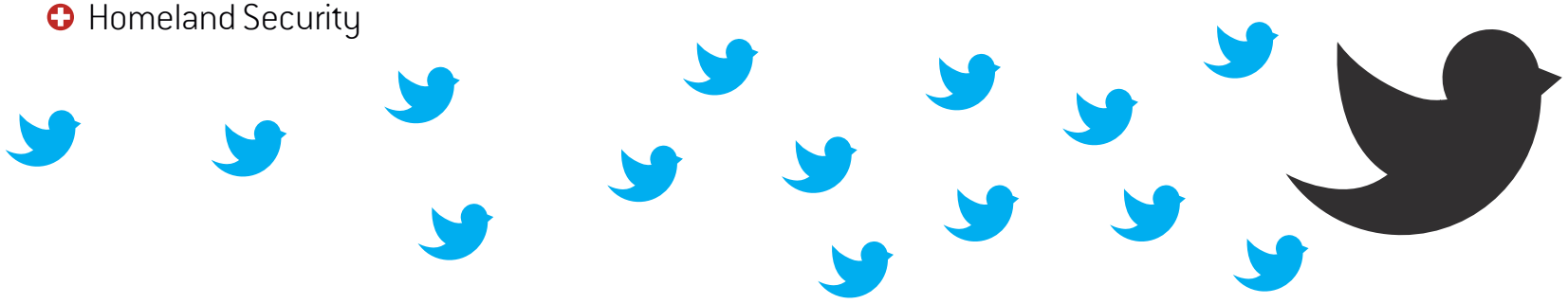
draths@mac.com

University of Houston Is Researching NG911 Cyber Solutions

Computer scientists at the University of Houston (UH) have experience researching how to protect critical infrastructure from a cyberattack. Now with a $2.6 million grant from the U.S. Department of Homeland Security Science and Technology Directorate, the UH researchers are studying technology and best practices to protect emergency response systems, including both current and next-generation 911 systems, against distributed denial-of-service attacks. The UH computer scientists also are working on responses to ransomware.

"We have a long research history and effort related to the resiliency of critical infrastructure," said Larry Shi, the principal investigator on the grant and assistant professor of computer science at UH. "Part of our mission is to engage and talk with the emergency management community about their needs and their road map in terms of NG911, and the integration of cyberdefense with emergency management. Over the last 12 months, we have done a lot of outreach to understand the needs of the community. We are trying to understand the risks and vulnerabilities of NG911."

UH researchers are seeking to understand the most likely places where cyberactors could attack the NG911 system. They plan to develop mitigation strategies or technology components that can be integrated with NG911 systems or infrastructure, Shi said. "In the very beginning of NG911, the cyberthreats were not well understood," he added. "More people are starting to see this is an important issue."



Quelling ISIS on Twitter

Researchers are looking at ways to thwart the Islamic State's social media recruiting.

By Eyragon Eidam | Staff Writer

New insights are now available into the Twitter networks of the Islamic State and those who oppose them, thanks to a study by the RAND Corp.

Efforts to thwart the group on the social media site have made headlines in recent months, but researchers are also interested in filling the vacuum created by suspended pro-ISIS accounts by using targeted messaging that focuses on avoiding radicalization in the first place.

Since the San Francisco-based company first began banning accounts of ISIS supporters in 2015, more than 360,000 accounts have been removed from the microblogging site.

In the study, *U.S. Social Media Strategy Can Weaken ISIS Influence on Twitter*, researchers used advanced network and lexical analysis to look at more than 23 million Arabic language tweets to determine their support or opposition for ISIS, who they are and what they are saying, and how they are connected across the larger network.

RAND Corp. engineer Elizabeth Bodine-Baron explained that the process was more than simply categorizing those who supported or opposed the radical militant group. The study also required a deep dive into the respective communities of the people on either end of the conversation.

By looking at the differences in how account holders referred to the West or ISIS, analysts were able to separate them into pro- and anti-ISIS categories with considerable accuracy.

"We had anecdotal evidence that people who were opposed to the Islamic State would use the term 'Daesh,' and people who were pro would use the term 'Islamic State,'" Bodine-Baron said. "By separating out whether you are using primarily the term 'Daesh' or primarily 'Islamic State,' we were actually able to quickly identify an account as pro-ISIS or anti-ISIS."

The moniker "Daesh" is unfavorable to the group because of its similarity to the Arabic word for "to crush or trample," but it can also mean "bigot," according to an NBC News report. "By comparing these two buckets, the people using 'Daesh' and the people using 'Islamic State,' we could definitely say that, in aggregate, if you are using one term predominantly, you are going to be opposed or pro," Bodine-Baron said.

What began as the identification of some 20,000 different communities was honed down, through advanced networking algorithms, to what researchers identify as four main metacommunities: Shia, Syrian mujahideen, ISIS supporters and Sunni.

The team was then able to determine how the individuals involved in the conversation were connected by examining not only the position various account holders took on ISIS, but also the "edges" that connect the networks and the key issues participants care about.

This piece of the research is important, Bodine-Baron said, because it could ultimately allow for the development of more targeted counter-ISIS messaging that could help to quell the recruitment of supporters.

"The issue is you can't just design a one-size-fits-all message for everyone," she said. "It has to be tailored to the different concerns of the different populations that could potentially be at risk for radicalization, and furthermore, it needs to be coming from credible Muslim voices, possibly even regional Muslim voices."

As for the removal of active extremist accounts, the research team said the effort to date seems to have had an effect on the overall social media campaign. "We really want to see the account suspension campaign continue because that denies them their platform of being able to just spread their propaganda without hindrance," Bodine-Baron said. "It forces them into less public spaces."

In examining the data set, Bodine-Baron said supporters were initially outnumbered 6 to 1, which would grow to nearly 30 to 1 by the end of the research period. She said the shrinking support for the group on Twitter was likely due to the aggressive deletion of associated accounts, but she qualified that more research would be needed to confirm that hypothesis.

In the larger network's analytics environment, this research is significant in that it could extend into other areas outside of examining polarizing organizations. It proves that big data sets can be analyzed quickly and effectively.

"One of the coolest things about what we've done is essentially do this proof of concept of where can these automated techniques for analyzing a big data set really help?" Bodine-Baron said. "By using these tools and specifically combining the network analysis and lexical analysis, we get these powerful results where we can say, 'OK, here is this group of users and here is what they care about,' and being able to more or less automatically ... figure out that these are the key themes we should be focusing our counter-messaging effort on."

eeidam@emergencymgmt.com

SHUTTERSTOCK.COM

RESILIENCY, EMERGENCY RESPONSE AND DISASTER RECOVERY SOLUTIONS

CB&I is a trusted partner in the design and execution of program management services. We provide turnkey solutions to expedite and maximize recovery efforts. Our experience helping customers solve complex problems before, during and after a disaster sets us apart in the industry.

PROGRAM DESIGN AND MANAGEMENT
CONSTRUCTION MANAGEMENT AND INSPECTIONS
RESILIENCY AND REDEVELOPMENT PLANNING
COMPREHENSIVE PLANNING
GRANTS MANAGEMENT AND INSURANCE RECOVERY
FEMA PUBLIC ASSISTANCE AND POLICY ADVICE
CDBG HOUSING AND INFRASTRUCTURE PROJECTS
FLOODPLAIN AND COASTAL EXPERTISE

A World of **Solutions**
Visit **www.CBI.com**

CB&I

12M092016H

At War With Terror

Malcolm Nance has a deep understanding of terrorism and the people who commit these acts.

Malcolm Nance is an intelligence specialist who speaks five languages, including Arabic. He has been deployed on counterterrorism operations for the U.S. Government's Special Operations, Homeland Security and Intelligence agencies in the Balkans, the Middle East and sub-Saharan Africa. He is a former master instructor and chief of training at the U.S. Navy's Survival, Evasion Resistance and Escape school. Nance is the author of several books, including: Terrorism Recognition Handbook: A Practitioner's Manual for Predicting and Identifying Terrorist Activities. *He spoke to* Emergency Management *the day after Mohamed Lahouaiej-Bouhlel ran a truck through a crowd on a famous waterfront in Nice, France, on July 14, killing 84 people.*

By Jim McKay | Editor

Very early in the investigation into Mohamed Lahouaiej-Bouhlel after he rammed a truck through a crowd in Nice, France, there was no obvious history of radicalization.

APIMAGES.COM

At this early stage of the investigation, what do you make of the man who drove a truck though the crowd in France? Was he what you'd call a "lone wolf?"
First off I don't like the term "lone wolf." ISIS themselves actually use the phrase "lone jihadi." They like that. We also categorize these guys as lone wolves and known wolves. Known wolves are those that have actually come under the counterterrorism umbrella, have a record related to radicalization and things like that. People we should have had our eye on like Omar Mateen down in Orlando. People who have been interviewed by the FBI.

Then you have the unknown wolves: people who self-radicalize, operationalize whatever plan that is in their heads and then execute that plan without any communication with anybody. Or their communications are so covert and successful that they didn't become known wolves.

In taking a look at this guy in Nice, the chief prosecutor says we have no indications of his radicalization or communications with known entities. That tells you it happened in his head or the communication structure they set up was so covert, they've yet to be detected.

That leans us away from the known-wolf picture because he had no record. The only thing he had been picked up on was weapons smuggling charges or charges relating to illicit weapons. If you're in Europe, everyone has illicit weapons. They are highly envious of the American access to weapons. For them these are status symbols — having access to weapons — and they are also very good sources of money. So that must have been attractive to him.

He was a recent Tunisian immigrant to France. Not everybody [there] can get a job — it's about the size of New York state. For these guys, they're concentrated in these places where there aren't a lot of jobs, there's a very young immigrant community there, and a lot of them don't assimilate into society like American Muslims. And they aren't French, either in culture or mindset, so they play along the fringes to make money however they can.

The difference between him and the Paris attackers and the Brussels attackers is that when those guys became radicalized they did their *hijra*, their migration to Iraq and Syria, and became combat commanders, they became soldiers and fighters. Then they reinfiltrated France as clandestine agents, carried out an operation as a cell, and did these operations both in Paris and Brussels.

This guy is an unknown wolf. In intelligence parlance he's sort of a clean-skin operative — no contact with law enforcement other than one charge. No history of radicalization, although there were some indicators that he was along the radicalization pathway.

Usually they find some trace of these people on social media. Is it relatively uncommon for them to be really unknown?
It depends on the individual. Some people watch the videos and adore them and they become entranced by these operations. On the other hand, you have knuckleheads who see one and they're going to do that. The Navy Seals have a phrase: We have wannabes and gonnabes. There are guys who really get radicalized [over time], and then there's those who wake up one morning and say, "I'm going to be a jihadi."

Here's my ideological path to radicalization: The first step is admiration. That's when they watch videos and such, that's internal. No. 2 is inspiration, where the images and religious rhetoric overwhelm you and make you feel like you should be a part or could be a part of that. Then comes step three, radicalization, when you affiliate with the terrorist philosophy. We call this the "fan boy stage." You're making tweets and things like that. Next is isolation. It's a cult technique. ISIS is a cult.

Isolation is where these guys perform *hijra*, where you go and emigrate overseas. That isolation could put you in Syria or Iraq fighting with them, and you cut yourself off from the land of the unbelievers. But they also have this thing called mental *hijra*, where if you can't make it to us, cut yourself off from the land of disbelievers around you, like the San Bernardino [Calif.] killers cut themselves off from their mother and child. They stopped going to mosque. Stopping mosque is a key indicator, especially if they were religious before that. That means they want no part in people that they think are dirty.

Step five is identification, where you adopt the trappings, hold up pictures of you holding guns, etc. Step six is dedication where you swear your loyalty oath, and that's close to when you die. Seven is execution.

These could be months, years or minutes apart.

You described ISIS and the West as two heavyweight boxers exchanging blows. Every time we drop a bomb, they counter. Can you elaborate?
We've killed more than 23,000 ISIS fighters in the last two years. We believe that their

combat strength of foreign fighters is down from 35,000 to 40,000 to about 12,500, so we've degraded that organization. [We have a] kinetic ground war, where we have surrounded them with four different armies, our special forces and our day/night bombing of just about everything that looks bigger than a pile of rocks. But ISIS can inspire a mentally deranged person in the United States or a guy who's having a psycho-sexual crisis like the guy in Orlando, to act out and kill people in the United States and then equate that act of terrorism in the United States as a failure of the tens of thousands of 2,000-pound laser-guided bombs where we are literally vaporizing that group. They're terrorists. Their job is to terrorize in any capacity. And we terrorize ourselves. Emergency managers are the one class of people that have to ground themselves in hard facts about who the enemy is. They have to get rid of the political jargon of radical Islam and things like that.

There should be a recognition of threat capacity, then response based on the best capacity of your organization and its inherent skills and training. That could have been a runaway truck. A runaway truck goes over a cliff, falls into a baseball stadium and crushes everybody in the stands. You don't know. You deal with the situation at hand. All of this requires you to have good intelligence, and that means intelligence that's detached from the political noise that is out there.

Do Americans misunderstand this fight?

First off the terms that people are using — "radical Islam," "Sharia Law" — we are not fighting Islam. If that's the case, why did we go to Afghanistan and put in an America-friendly government and get rid of the brutal Taliban? Why did we lose 2,600 soldiers there?

We lost 4,493 American soldiers in Iraq. If you believe that we're at war with Islam, then you believe that those wars were worthless and that we should leave there and leave the Muslim worlds to ISIS and al-Qaida.

Let's discuss information sharing. There has been criticism of the FBI after the Boston bombings and the Orlando shootings that information wasn't shared with locals.

I'm here in New York state and just in the last eight months I've done six conferences. I saw every joint terrorism task force in the state, including the SWAT, dog handling teams and all the maritime teams here, and they have pushed the joint terrorism task force link down to the precinct liaison level. There is a terrorism liaison officer in every law enforcement and emergency management jurisdiction in the state.

When I did the liaison officer's program a few months ago, it was all fire and emergency managers and they got the exact same information the SWAT guys got except how to kick that door down. They got the same intelligence, and that's what we need to do nationally. Every state should be creating an intelligence liaison organization where information gets pushed down to the street level.

jmckay@emergencymgmt.com

The MOBILE FRIENDLY
emergencymgmt.com

2015 Winner

MAGGIE AWARDS
2015 / BEST WEB PUBLICATION TRADE
Emergency Management Magazine

MAGGIE AWARDS
2015 / BEST OVERALL PUBLICATION
Emergency Management Magazine

ASBPE AWARDS
2015 / MAGAZINE OF THE YEAR
Emergency Management Magazine

SHUTTERSTOCK.COM

Secret Resource

The federal government stockpiles emergency medicines and supplies in several locations throughout the U.S.

By Margaret Steen | Contributing Writer

How would emergency management and public health officials handle a catastrophe that taxed local supplies of vaccines or medical equipment? Since 1999, the federal government has had a way to help: the Strategic National Stockpile.

The stockpile consists of warehouses that contain medicines — both those that prevent the onset of an illness and those that can treat illnesses — and medical supplies and equipment. It is not meant to be the first line of defense, but rather to supplement resources when state and local supplies run short.

"The underlying premise of the Strategic National Stockpile is to respond to primarily chemical, biological, radiological and nuclear events," said Greg Burel, director of the Division of Strategic National Stockpile at the Centers for Disease Control and Prevention (CDC). "We also hold material that would be useful in an influenza event."

The exact number of warehouses, the contents and the locations are not made public, though the CDC's website describes the contents as "antibiotics, chemical antidotes, antitoxins, life-support medications, IV administration, airway maintenance supplies and medical/surgical items."

"There are multiple locations across the country," Burel said. The sites are selected after considering factors such as population density, the availability of major transportation hubs and risk factors like natural disasters. "We try to balance products in a way across these warehouses to get the most rapid distribution anywhere in the country we need to get to."

There's a reason for the secrecy.

"If you know what's in it, you know what's not in it, which could suggest some vulnerabilities," said Rocco Casagrande, managing director of Gryphon Scientific in Takoma Park, Md. "It would describe exactly which attacks we don't have preparations for."

The way the stockpile's contents are chosen illustrates the complexity of the decisions officials face when preparing for public health emergencies.

Irwin Redlener, director of the National Center for Disaster Preparedness at Columbia University, said choosing items for the stockpile is one of the key challenges. The other is what happens at the end of the process: the management of the so-called last mile, where supplies are distributed to those who need them.

The Big Picture

The Strategic National Stockpile is just one part of the overall plan for getting supplemental emergency assistance to areas that need it. The process begins with the Public Health Emergency Medical Countermeasures Enterprise (PHEMCE), the government organization that makes decisions about what should be in the stockpile.

"What conditions will it respond to? What supplies and medical countermeasures need to be in the stockpiles?" Redlener said. PHEMCE makes this determination.

Although the original goal of the Strategic National Stockpile was to respond to chemical, biological, radiological and nuclear threats, Burel said, "we have expanded our mission to an all-hazards perspective, so we do hold some products that are useful, for example, in response to hurricanes and earthquakes."

The list of what goes into the Strategic National Stockpile is based on material threat assessments from the Department of Homeland Security, as well as medical information.

"The content changes over time based on scientific understanding of what is needed to combat the material threats," Burel said. The threats themselves don't change dramatically very often, he said, but "if some new threat appeared and became the highest priority, we could have to make rapid changes in our holdings to address that."

The Strategic National Stockpile is responsible for the middle part of the process: maintaining the inventory and making sure it can get where it's needed. But the stockpile's responsibility for the materials ends once it is delivered to the local authorities, who distribute them to the people who need them.

"The [Strategic National Stockpile] portion is important, but it depends on what happens before and after," Redlener said.

Critical Inventory

The current valuation of the stockpile's inventory, which includes enough medicine for the populations of several large cities, is about $7.5 billion, and the average annual appropriation for it is about $500 million.

Experts deciding what should go into the stockpile have to consider many factors, including current threats, the availability of products, how easily the products can be distributed and the medical vulnerability of the population, according to the CDC. They also look at how useful specific items will be in a range of situations.

For example, some antibiotics may be useful to combat a broad range of threats — though not always with a big impact — whereas an antitoxin may be more effective but useful in just one type of emergency. In addition, "there might be certain agents that act so fast that it doesn't make sense to stockpile countermeasures for them because you can't get them there," said Casagrande.

Some of the products may also serve multiple purposes: Oral antibiotics, for example, may be put in the stockpile in preparation for a particular type of biological weapon attack. "It may be that they would be useful for a large-scale emerging infectious disease or some man-made event that we didn't plan for," Burel said. "We are constantly looking for ways to make sure we can get the most use out of everything we own."

The program works with commercial vendors to provide some of the material, sometimes in response to emerging threats.

For example, during the Ebola outbreak, the Strategic National Stockpile used the commercial supply chain to provide protective gear to health-care workers, according to a report prepared for a PHEMCE workshop in January.

"With Ebola, we did acquire on the fly a small stock of personal protective equipment," said Burel. After officials determined which hospitals would play which role in treating Ebola patients, "we worked with hospitals directly to determine what their status was to be able to support patients."

One key aspect of the stockpile program is quality assurance. This means rotating the stock to replace anything that has expired, for example, and performing quarterly quality assurance checks. In addition, changes are made due to new drugs that have been developed to combat certain diseases.

A Complex Process

The materials in the stockpile will only be effective in an emergency if they actually get to the people who need them in time.

Casagrande said the key is the "three D's": delivery, or getting the material from the stockpile to the local area; distribution, which means getting it to the specific place where it will be used; and dispensing, or administering it to the patient. "All three are important," he said.

This process starts once local and state resources are exhausted. The governor of the affected state requests material from the stockpile from the CDC or the U.S. Department of Health and Human Services, starting a rapid decision-making process to determine what type of help can be provided. At the end of the chain, local communities receive the materials from the state and provide them to those who need them in the community.

"We work with state and local officials to determine where to deliver it and how to do that," Burel said. For most situations, plans are already in place for the local agencies to distribute the products once they receive them.

The level of preparation among states and local governments varies. "We have some states and localities where the coordination is very advanced," Burel said. "There are some that probably need a little more work in that area."

Once the material arrives at the affected area, state and local officials take control of it. However, the stockpile does provide technical advisers who can assist the local jurisdictions in getting the material to where it's needed.

"Once we hand off the material, we don't just walk away," Burel said. "But it becomes the responsibility of state and local officials to put material into distribution plans they already have in place."

The stockpile has several ways of getting material to those who need it. For immediate response, it has 12-hour Push Packages, which the CDC describes as "caches of pharmaceuticals, antidotes and medical supplies designed to provide rapid delivery of a broad spectrum of assets for an ill-defined threat in the early hours of an event." They can be loaded onto trucks or cargo planes to be delivered within 12 hours of the decision to use them.

The CDC also uses vendor-managed inventory, which can get to an affected location within 24 to 36 hours.

The stockpile staff also provides assistance to public health and emergency management departments to handle emerging threats. "We've been able to work through our capability to manage medical supply chain logistics and try to help make sure that interventions are conducted in the most rational way," Burel said.

Looking to the Future

As the Strategic National Stockpile moves into the future, there are questions about what might change.

"We don't really have an agency that has the job of overseeing, end to end, the determination of threats, selection of countermeasures, the stockpile and the last mile. I do believe there could be an agency with end-to-end responsibility," said Redlener. The management structure of the entire process is "one of the open questions for a new administration."

"We're constantly looking for ways to do better, to make things move faster," Burel said. For example, they are starting to do exercises with external partner groups such as the Health Industry Distributors Association. "Whether it's a natural or man-made disaster, a weather event or an earthquake or a disease — what is the best way we can all work together make decisions?"

For now and in the future, communication among agencies is key.

"It's very important for the public health community and the emergency management community to talk in advance about how they can support each other," Burel said. "Even these natural disasters all have significant public health implications. If you're in emergency management, you can't think of emergency management in a vacuum. You have to think about how it's going to impact public health."

msteen@margaretsteen.com

SHUTTERSTOCK.COM

Prepare Your Business

DHS launches site to get the emergency preparedness message to businesses.

By Adam Stone | Contributing Writer

At the U.S. Department of Homeland Security (DHS), Assistant Secretary for the Office of Infrastructure Protection Caitlin Durkovich recognizes how hard it can be for emergency managers to distill the message of preparedness for citizens and businesses.

With the rise of global terror, the threat landscape has become exponentially more complex, making it harder for first responders and others to communicate even basic security information. "But this is the new normal, this is the world that we are living in now, where we are going to see attacks on soft targets with frequency," she said.

To convey the significance of that reality, emergency managers need a concise message.

The new DHS website Hometown Security (www.dhs.gov/hometown-security) aims to deliver just that. "Keeping it simple is sometimes the most important thing you can do in this business, and that's what this is: just a very simple framework, a very simple message," Durkovich said.

Launched this spring, Hometown Security gathers a range of existing DHS incident-preparedness tools along with a new fact sheet to help direct small and mid-sized businesses to free tools and resources. DHS says the intended audience includes restaurants, clubs, grocery stores, places of worship and other venues where people may congregate.

Easy-access tabs encourage businesses to Connect, Plan, Train and Report, defining these four basic concepts as the rudiments of preparedness. Each tab gives concise instructions in the essentials of the craft: Exercise your emergency communications plan; report unattended vehicles or suspicious visitors; and develop evacuation and shelter-in-place plans.

This basic guidance is surrounded by links to more detailed information. Visitors can drill down for direction on active shooter preparedness, chemical security, cybersecurity and several other topics.

Early users within the emergency management community say they see a place for the new DHS asset in their toolkits.

'It's Quick'

Kevin Cleary is more or less up to his neck in mass-crowd events. As director of preparedness in the Baltimore Mayor's Office of Emergency Management, he stood watch as a record 135,256 people gathered for the Preakness Stakes in May to see Exaggerator cut short Nyquist's undefeated record. In July more than 350,000 braved sweltering heat to take part in the annual Artscape cultural celebration. Thousands gathered for a series of some two dozen gay pride happenings at the end of July. And this fall the city is slated to host a weeklong series of events leading up to the christening of the USS Zumwalt, a new Navy warship. Cleary calls it "a robust special events season," which seems an understatement.

To ride the swell, he has all the usual tools of emergency management at his disposal, including online resources from FEMA and the city's own Corporate Emergency Access System. He said he welcomes the new DHS tool.

"It is good because it's quick. The business folks don't want to be overwhelmed with stuff they don't need," said Cleary. It's helpful too that he can send the public to a site that he and they are ready to trust. "It's good to have something we can point people to that isn't just 'Oh, I asked my neighbor across the street who is a retired police officer.' You can Google something and get 20 different links, but this is a much more definitive source. This is an authority figure."

Members of the first responder community likewise are giving the site a warm reception.

"I think people will find this empowering. To get on this site and find this information, and be ready to take that back and act on it: The value of that can be just incredible," said Col. Melissa Hyatt, formerly chief of patrol

and now chief of special operations and development in the Baltimore Police Department.

In her experience, business leaders especially are eager to get the kind of information offered here, and she's always ready to welcome a new means of providing it to them.

"We present at these business forums on things like active shooter preparedness, and people will always ask: How do I plan? What do I do for my business? We assist them with making those plans, but this offers a one-stop resource. It gives people an added level of preparation," she said.

Hyatt said it's important, too, that the website is more than just a one-off. From the emergency manager's office, down through the first responders and across the preparedness community, the new site builds on an existing relationship between emergency planners and DHS, at least in Baltimore.

She pointed to 2014's Star Spangled Spectacular, which drew more than a million people to the city to view tall ships, Navy gray hulls and the Blue Angels flying squadron. "There were events in the city and county," she said. "There were events across an enormous footprint, things happening at all hours involving people from all over the world, things happening on the water, entities in the air."

DHS was deeply engaged, providing expertise in areas like threat assessments, critical infrastructure assessments and threat mapping, said Hyatt. "When you are the incident commander, these are priceless resources."

More recently, DHS Protective Security Adviser Ray Hanna was on hand this spring to help prepare for Light City. This inaugural festival drew some 400,000 people to more than 50 attractions including performances, concerts, food vendors and a children's area. It was the first big public event following weeks of civic disruption around race issues.

"This was our first major event after the unrest, and we worked very closely with DHS," Hyatt said. "It made us want to be proactive, to talk about things from the local level all the way up to the federal level."

Hyatt said that kind of collaboration in the early stages, aided by tools like the new website, helps local officials make best use of DHS resources.

"It benefits all of us to have these partnerships active and ongoing, during the planning process. That way we're not trying to involve them in our plans at the point where something has already occurred," she said. "The more people you can have at the table for brainstorming, the better it is."

DHS officials say that's the spirit they're hoping to engender in the emergency management community, and they hope the emergency management professionals in turn will utilize the new website to light that same spark among business leaders.

"We hope they will use this site to work with businesses and the public," Durkovich said. "We have to work together to create a culture of resilience."

adam.stone@newsroom42.com

PUBLISHER'S STATEMENT

Statement of Ownership, Management, and Circulation

(Required by 39 U.S.C. 3685)

Title of publication: Emergency Management. Publication No.: 5710. Date of filing October 1, 2016. Frequency of issue: Quarterly. No. of issues published annually: 4. Complete mailing address of known office of publication: 100 Blue Ravine Road, Folsom, CA 95630. Complete mailing address of general business offices of publisher: 100 Blue Ravine Road, Folsom, CA 95630. Full names and complete mailing addresses of publisher, editor and managing editor; Publisher: Alan Cox, 100 Blue Ravine Road, Folsom, CA 95630. Editor: Jim McKay, 100 Blue Ravine Road, Folsom CA 95630. Managing Editor: Elaine Pittman: 100 Blue Ravine Road, Folsom, CA 95630. Owner: e.Republic, Inc. dba Government Technology: Dennis McKenna and Robert Graves, 100 Blue Ravine Road, Folsom, CA 95630. Known bondholders, mortgages and other security holders owning 1 percent or more of the total amount of bonds, mortgages or other securities, none.

Extent and Nature of Circulation

		Average No. Copies Each Issue During Preceding 12 Months	No. Copies of Single Issue Published Nearest to Filing Date
A.	Total No. of copies (Net Press Run)	29,751	29,847
B.	Legitimate Paid and/or Requested Copies		
1.	Outside County Paid/Requested Mail Subscriptions Stated on PS Form 3541	21,949	21,979
2.	In-County Paid/Requested Mail Subscriptions stated on Form PS 3541	0	0
3.	Sales Through Dealers and Carriers, Street Vendors, Counter Sales, and Other Paid or Requested Distribution Outside USPS	0	0
4.	Requested Copies Distributed by Other Mail Classes Through the USPS	0	0
C.	Total Paid and/or Requested Circulation	21,949	21,979
D.	Nonrequested Distribution		
1.	Outside County Nonrequested Copies Stated on PS Form 3541	6,449	6,938
2.	In-County Nonrequested Copies Stated on PS Form 3541	0	0
3.	Nonrequested Copies Distributed Through the USPS by Other Classes of Mail	0	0
4.	Nonrequested Copies Distributed Outside the Mail	175	0
E.	Total Nonrequested Distribution	6,624	6,938
F.	Total Distribution	28,573	28,917
G.	Copies not Distributed	1,178	930
H.	Total	29,751	29,847
I.	Percent Paid and/or Requested Circulation	76.82%	76.01%
a.	Requested and Paid Electronic Copies	12,752	8,020
b.	Total Requested and Paid Print Copies + Requested/Paid Electronic Copies	34,701	29,999
c.	Total Requested Copy Distribution + Requested/Paid Electronic Copies	41,325	36,937
d.	Percent Paid and/or Requested Circulation (Both Print & Electronic Copies)	83.97%	81.22%

I certify that all information furnished on this form is true and complete.
Elaine Pittman, Managing Editor

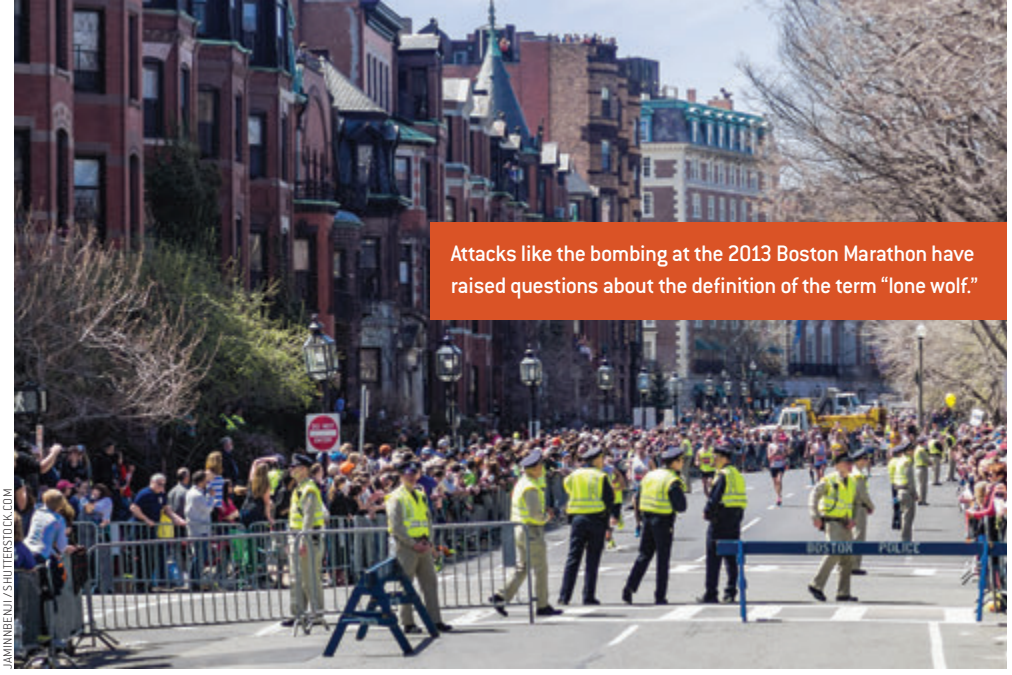
LONE OR KNO

WHATEVER YOU CALL THEM, THEY CONTINUE TO CHALLENGE COUNTER-TERRORISM OFFICIALS.

BY JIM MCKAY / EDITOR

SHUTTERSTOCK.COM

WN WOLVES?



Attacks like the bombing at the 2013 Boston Marathon have raised questions about the definition of the term "lone wolf."

JAMINNBENJI/SHUTTERSTOCK.COM

After Tamerlan Tsarnaev and his brother, Dzhokhar, detonated bombs that killed three people at the 2013 Boston Marathon, details about the FBI's previous monitoring of the two prompted criticism of the agency.

When Omar Mateen took out his rage on 49 souls at an Orlando, Fla., nightclub earlier this year, there were again questions about why he was flying under the radar after having been investigated by the FBI.

Then there were Rizwan Farook and Tashfeen Malik, who shot 14 in San Bernardino, Calif., and Micah Johnson, who gunned down five Dallas police officers. These instances demonstrate not only the distance our intelligence apparatus has to cover to gain necessary ground, but also the difficulty in stopping attacks from these so-called lone wolves and determining who will turn from angry and disenfranchised to radicalized killer.

The lone wolf by definition is one who acts without any co-conspirators — one who either becomes self-radicalized and acts alone or, increasingly, follows the online preaching of groups like ISIS.

In many cases, they leave a trail of clues that could indicate radicalization or a shift in that direction. But it's difficult to know what clues portend danger, as was the case with the Boston bombers and Mateen.

KNOWN OR UNKNOWN?

"First of all, I don't like the term 'lone wolf,'" said Malcolm Nance, an intelligence specialist and former master instructor and chief of training at the U.S. Navy's Survival, Evasion, Resistance and Escape school. "ISIS themselves actually use the term 'lone jihadi.' They like that."

Nance said he categorizes them as "known wolves" and "unknown wolves." "Known wolves are those who have come under the counterterrorism umbrella." They have a record related to radicalization, such as Mateen. "People who we should have had our eyes on. People who have been interviewed by the FBI."

The Boston Police Department had four members within the local Joint Terrorism Task Force, which, led by the FBI, investigated Tsarnaev. The task force acted on a tip from the Russian government that the elder brother was engaging in radical behavior.

But after the FBI concluded the investigation, it left the four Boston Police members in the dark about Tsarnaev and any possible threats. The former Boston Police commissioner was highly critical of the FBI, saying there should be some sort of mandate requiring federal authorities to share with local law enforcement to protect the community.

The same appears to have happened with Mateen, who was investigated by the FBI after telling co-workers about ties to terror groups. But again, the FBI appears not to have been very aggressive about keeping local agencies updated.

Then there are the unknown wolves, those who self-radicalize, "operationalize whatever plan is in their head and execute it without ever communicating with anybody," Nance said.

Both are hard to stop, but the known wolves, as Nance refers to them, at least provide a trail. That's because they don't usually have the wherewithal to act out before dropping hints along the way, said Scott Decker, Arizona State University's director of the Center for Public Criminology. "It requires a lot more discipline than most of these young men are capable of," said Decker. "The idea that they are true lone wolves is difficult for me to get my arms around. Most of these guys are not good at keeping secrets, and they're not very well disciplined."

They often leave behind blogs and messages on social media indicating their extremist views, but it's difficult to know when a viewpoint will cross over into violence.

Decker said most of the time the motivation for an attack comes from an external focus, whether it's the Internet or interaction with other people, and is rarely, if ever, intrinsic to the individual. The Internet also eliminates that need for face -to-face contact with others, changing the game and making it difficult to track without Internet-based surveillance.

A SIGN OF WEAKNESS

The term "lone wolf" is nothing new, but is being treated as if it were, said Michael German, a former FBI agent specializing in domestic terrorism and now a fellow with the Brennan Center for Justice's Liberty and National Security Program.

German joined far-right groups as an undercover agent in the 1990s, and those groups had a lone-wolf manual. When authorities tamped down on these groups they were powerless, forced into a situation where they had to rely on encouraging outsiders to commit violent acts and credit their cause.

"Part of the problem is every time a new terrorist group emerges, policymakers and analysts tend to suggest this is a brand-new phenomenon," he said. "And it's done somewhat to avoid having to look at how these instances have played out in the past."

Treating it as a growing problem tends to suggest that more aggressive policies will be effective, which was shown not to be the case in the past. "The indiscriminate use of violence by terrorist groups is an indication of weakness," German said. And when we attribute acts of violence to these groups we give them recognition, he said, which is counterproductive.

German cited as an example the Colorado movie theater shooter who claimed he was Batman's nemesis, the Joker, yet no meaning was attributed to that, whereas

when Mateen cited ISIS, it received a lot of attention. Attaching some meaning to their actions gives those who may be "misguided, angry, contemplating suicide," a chance to go out like a soldier for a cause, said German. "The recognition is an incentive to commit violence, and we want to remove that."

He said the solution is to focus on violence and not ideology. In its information analysis role, the FBI had investigated Tamerlan Tsarnaev and ultimately found him not to fit the profile of someone who might commit a terrorist act. But the elder Tsarnaev had prior acts of violence, including domestic violence, and was implicated in a triple homicide. Tamerlan Tsarnaev was cooperative with the FBI and even offered to help in the investigation.

"The FBI has transitioned into a domestic intelligence agency," German said. "If you look at that investigation, it wasn't designed to determine whether his violation of criminal law was true or not. Instead they were trying to assess whether he was a threat based on his ideology and response to the FBI inquiry."

If investigators would focus on violent crime, German said, they would be more likely to stumble onto someone like Tsarnaev rather than looking at huge numbers based on ideology. "What we have to do first is recognize that mass shooters or bombers who don't have links to a wider conspiracy are, in methodology, no different from other mass shooters or bombers," he said. "If we look at the data, these mass killings are only a small fraction of the violence that is perpetrated in American society on a daily basis, and we have to recognize that we have to address the violence."

JUST GET BETTER

Matt Mayer, visiting fellow at the American Enterprise Institute, said there should be a debate in Washington about how to reform intelligence operations and how to better deal with the small-cell or lone-wolf threat.

Part of that discussion involves the FBI, which after 9/11 took on the task of information analysis, whereas it had always been in the business of compiling evidence for prosecution. It is with mixed reviews that the agency continues on in this role, where improvement is necessary.

Should the FBI continue doing both analysis as a domestic intelligence agency and also conduct investigations for the purpose of obtaining prosecution?

"I believe so, because if they don't, it puts us in a position where we are housing that function in two separate places, which makes me nervous about the information getting to the right places within the FBI," Mayer said.

Mayer said that both procedural and substantive improvement needs to happen and that a cultural change is still necessary. "They just have to get better at what they do."

It's been said the old guard of the FBI won't change, but as new, younger agents emerge, efforts to change the agency's culture will improve and so will intelligence analysis and information sharing.

But the message from the top, including the president, has to be consistent, and that hasn't been the case. Mayer said it started with the development of U.S. Department of Homeland Security-funded fusion centers. "It seemed to cause a competition between homeland security and the FBI over who would 'own' state and local information and intelligence."

That sent a message, according to Mayer, that the FBI shouldn't share because it was competing and not coordinating. Mayer advocates eliminating the fusion centers and consolidating those with the FBI's joint terrorism task forces, which he said are where the bulk of the activity happens anyway.

"It just doesn't make sense to have two different pipelines where information could be lost, held [or] not shared."

He said in the case of the Orlando shooter, Mateen, local law enforcement had information and sent it to the terrorism task force, but "it doesn't appear that there was much of a partnership going on."

What should have happened in that case and others, Mayer said, is that the information is shared with multiple partners across the spectrum of local, state and federal agencies to get the best results. "It's not just an FBI case, not just an FBI activity. You have to figure out who has the best resources in that situation and who has the most contacts and penetration points and use them accordingly."

Decker also thinks the fusion centers have missed the mark, failing to really partner with local law enforcement, and thus underutilizing a valuable resource. "It's really unfortunate because there's so much that local law enforcement knows and can do and yet they're still left on the sideline in this."

He said the "trifurcated" federal, state and local justice systems have been bad at sharing information and, especially, using one of the most valuable resources of all: the cop on the beat who sees and interacts with locals and knows what "normal in the neighborhood looks like."

Decker added that some of these attacks are preventable, but that it would take levels of surveillance and security that Americans may not be ready for. "If you travel and go through TSA, people mumble and complain about being stopped and going through a metal detector, whereas in European countries and certainly Israel, you get in line and you wait and you come to expect that."

"PART OF THE PROBLEM IS EVERY TIME A NEW TERRORIST GROUP EMERGES, POLICYMAKERS AND ANALYSTS TEND TO SUGGEST THIS IS A BRAND-NEW PHENOMENON. AND IT'S DONE SOMEWHAT TO AVOID HAVING TO LOOK AT HOW THESE INSTANCES HAVE PLAYED OUT IN THE PAST."

jmckay@emergencymgmt.com

By Eric Holdeman

Living History

I have always thought my grandparents lived in historic times. They went from horses and buggies to automobiles to airplanes to man landing on the moon. Similarly, we watch emergency management leadership transition from baby boomers to Gen Xers to millennials and ponder our own living history.

Modern emergency management was born with the creation of FEMA on April 1, 1979, by President Jimmy Carter. This move came from a need to have a single federal agency coordinating the disaster response of others. The primary focus of FEMA in the early 1980s was not on natural disasters, but civil defense.

AS I LOOK INTO MY CRYSTAL BALL I SEE CLIMATE CHANGE IMPACTS CAUSING A WHOLE HOST OF HIGH-IMPACT DISASTERS.

This focus didn't end until the Berlin Wall fell in November 1989 and we saw the collapse of the Soviet Union. It was at that point that civil defense at the federal, state and local levels began to take a backseat to natural hazards. This era also saw the appointment of James Lee Witt as the first professional emergency manager leading FEMA as its director (1993) and the establishment of FEMA as a cabinet agency (1996). I began my civilian career as an emergency manager on Sept. 1, 1991, so this transition has been etched in my memory.

It was at this time that we first saw a real emphasis on disaster mitigation, with Witt birthing a program called Project Impact in 1996. Back then I would say, "Emergency managers can't even spell 'mitigation.'" While it was part of our doctrine, there had been little to no emphasis on that aspect of the profession. At that time the only higher education program in the nation with an emergency management focus was at North Central Texas College.

We took a significant step back in 2001 when the George W. Bush administration took control of emergency management. We once again had a political appointee, Joe Allbaugh, assume the role of FEMA director. Project Impact was canceled as a FEMA program on the same date that western Washington state experienced the Nisqually earthquake, Feb. 28, 2001. FEMA was first given the expanded mission of "homeland defense" in May of that year, preceding the terrorist attacks of 9/11.

The creation of the U.S. Department of Homeland Security (DHS) in 2002 has had the most impact on emergency management and FEMA of any event since the agency's creation. FEMA became part of the DHS and quickly took a backseat to other elements within the department. The creation of the Homeland Security Grant Program in 2003, with its terrorism focus, made state and local emergency management agencies take a hard turn toward terrorism response.

It took Hurricane Katrina in 2005 and the obvious failure of FEMA, along with Louisiana and New Orleans, to provide a course correction that allowed the pendulum to start to shift back toward an all-hazard approach. Grant funds following Katrina were allowed to have a "dual-use" function, with terrorism still being the priority.

Now as we are about to end the Craig Fugate era of FEMA, we have a more balanced approach to disaster mitigation, response and recovery, although recovery planning still lags at the state and local levels. Today there is a college or university program with an emergency management focus in every state.

Emergency management history continues to be written every day. As I look into my crystal ball I see climate change impacts causing a whole host of high-impact disasters. The next decade and beyond will be an era of hyper technology formation and adoption by emergency management agencies. Are you ready?

ERIC HOLDEMAN IS THE FORMER DIRECTOR OF THE KING COUNTY, WASH., OFFICE OF EMERGENCY MANAGEMENT. HIS BLOG IS LOCATED AT WWW.DISASTER-ZONE.COM.

Enova DGX 3200

Enova DGX 100 Series
Purpose Built for Video Distribution Designed For Maximum Uptime

The successful distribution of AV content can often mean the success or failure of a military mission, a surgical procedure, or a launch into space. It's these types of applications that have led teams faced with mission critical operation to rely solely on Enova DGX dedicated AV switching and distribution to get content from source to destination without fail.

- Fully redundant power supplies with independent power paths ensure maximum reliability for applications requiring 24/7 uptime.
- Field/hot swappable video input/output boards and power supplies empower quick, easy replacement at any time.
- Modular-based, isolated component architecture design isolates system components to ensure maximum uptime.

AMX by HARMAN

MILITARY-GRADE MOBILE TABLETS

DT Research announced its military-grade 2-in-1 mobile tablets with detachable keyboards designed to withstand extreme outdoor environments with integrated, customizable options built into a slim, lightweight tablet that's well suited for the office. These new rugged tablets deliver seamless field-to-office use.

FEATURES INCLUDE:

- Water-resistant detachable keyboards
- Advanced hardware-software security — Media Sanitization and Windows 10 IoT Enterprise security
- Hot-swappable internal batteries
- High-resolution capacitive touch outdoor displays in two sizes: 10.1 inch and 11.6 inch
- Lightweight — a fully loaded 10.1-inch tablet weighs 2.86 pounds

BUILT-IN OPTIONS:

- 3G WWAN or 4G LTE
- 2-D Barcode Scanner
- 2 Megapixel front camera and 5 Megapixel back camera with LED flash
- NFC/RFID 13.56MHz reader (ISO 15693 and 14443 A/B compliant)
- Wi-Fi and Bluetooth

www.dtresearch.com

UNVEILING THE DRONEBOX

DRONEBOX is a new system that converges professional drone-enabled services with the industrial Internet of Things. It is an all-inclusive, self-powered system that can be deployed anywhere, including in remote areas where industrial assets, borders or sensitive installations require constant monitoring.

Designed as an evolution over today's many unattended sensors and CCTV cameras installed in cities, borders or large industrial estates, DRONEBOX gives sensors freedom of movement using drones as their vehicles. End users can deploy flying sensor systems at different locations and measure just about anything, anywhere, anytime. They offer 24/7 reactivity, providing critical information to operators — even to those located thousands of miles away. www.h3dynamics.com

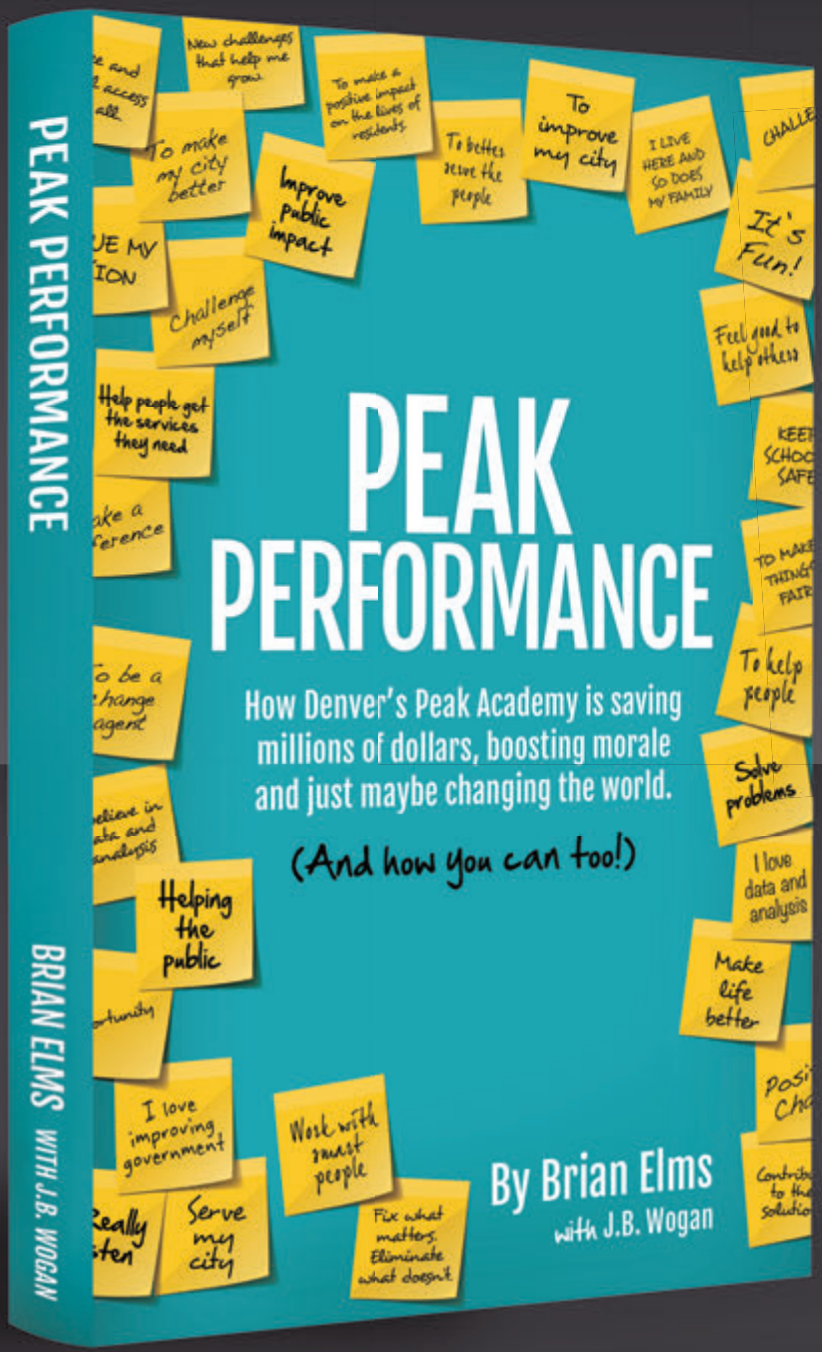
PINPOINTING CRIME

RedZone is a new tool that will help law enforcement track and bust crime. The app populates with real-time pins powered by crime reports and crowd-sourced updates, and it uses proprietary geo-fencing technology to guide people safely around cities. "Red zones" are considered highly concentrated areas of crime where many pins have been dropped. Upon locating these zones, the app will provide users with safe and "risky" routes to get to their desired destinations.

Law enforcement agencies or officers can use the app when they are low-staffed or when they want to monitor key sections of their cities. This includes dispatching cars to areas sprouting crime or using the app as a secondary neighborhood watch system. www.redzonemap.com

"This book is a must for anyone who believes government can make a difference in our lives. ... *Peak Performance* details how a courageous and visionary mayor and a highly dedicated workforce can give their citizens a more efficient and effective government ..."

Former Pennsylvania Gov. Edward G. Rendell,
author of *A Nation of Wusses: How America's Leaders Lost the Guts to Make Us Great*



A quick, honest & fun must-read for anyone who lives in a city or works in an organization!

Theresa Reno-Weber,
Chief of Performance & Technology,
Louisville, Ky.

Order today at
governing.com/peakperformance

Also available on amazon.com.
Bulk discounts available.

GOVERNING BOOKS

By Ken Burris

The Keys to Corporate Resiliency

One of the most critical responsibilities of an executive is building corporate resilience through an effective crisis management process. Corporate resiliency is derived from three specific processes: awareness, action and preparation. Most executives recognize the impacts of known events such as, fires, floods, cyberattacks, workplace violence, etc., and have developed plans for dealing with such events.

Crises arise from being faced with an unknown or unimaginable event for which there is no mitigation strategy. The inability to effectively deal with an event, known or unknown, subsequently impacts reputation, employee morale and company value.

Corporate resiliency, in its simplest terms, is an organization's ability to return to a normal operational tempo — including throughout its entire web of suppliers, manufacturers, distributors, retailers, transportation carriers and the other participating partners — after some period of time following an incident. Creating corporate resiliency contains two unknowns that are imperative to understanding and developing an actionable planning process: What constitutes normal operational tempo? What is the period of time?

Awareness as it relates to resiliency is the process of establishing a clear understanding of normal operational tempo and identifying risk. What are the baselines, both qualitative and quantitative, of the critical inputs or outputs constituting normalcy? These can be environmental conditions, just-in-time delivery schedules, production or service expectations of clients, or financial solvency.

Awareness can also enable leaders to identify and handle unexpected, non-normative events and their subsequent solutions. In a recent World Economic Forum survey, participants were asked to identify situations or threats they believed had the highest consequences for their companies. They were:

- large-scale involuntary migration
- extreme weather events
- failure of climate-change mitigation and adaptation
- interstate conflict
- natural catastrophes
- failure of national governance
- unemployment or under-employment
- data fraud or theft
- water crisis
- illicit trade

The action process is the influencer of time. Time has an exponential impact on an organization, both tangible and intangible. Staff morale, internal and external trust, company value, and goodwill impartment are all influenced by time. The process of determining time then identifies the surge capacity required to: return to normal; identify the resources needed to accelerate the return to normal; and inform executives charged with the decision-making process with implementable options that maximize corporate strategies for recovery as well as impact value and reputation of the company.

Once awareness has been established and actions taken, only then can an effective preparedness process begin.

Once appropriate and effective strategies for mitigation of an incident are identified, emergency action plans should be developed for implementation during an event. Business continuity plans should be established after correctly identifying the business-essential and critical operations necessary to maintain as near-normal operations as possible during an event.

Crisis communications plans must be shaped to take advantage of known actions, timelines and pre-identified stakeholder groups, to better inform stakeholders and remain transparent during and after an event.

Become aware, understand necessary actions and their influence on time, and prepare today for a crisis of tomorrow. Your organization's reputation and value depend on it.

KEN BURRIS IS VICE CHAIRMAN AT WITT O'BRIEN'S.

PROTECTING YOU WHILE YOU'RE PROTECTING THEM.

SHI's Video Surveillance Solution deploys cutting-edge technologies and program expertise to address **ALL FOUR** required stages of any complete video surveillance program:

CAPTURE
desired footage on a fixed or mobile camera or device

COMMUNICATE
and convey critical information from device to primary location

STORE
video footage in compliance with data retention policies

SECURE
encrypted footage in accordance with FBI Criminal Justice Information Services (CJIS) standards

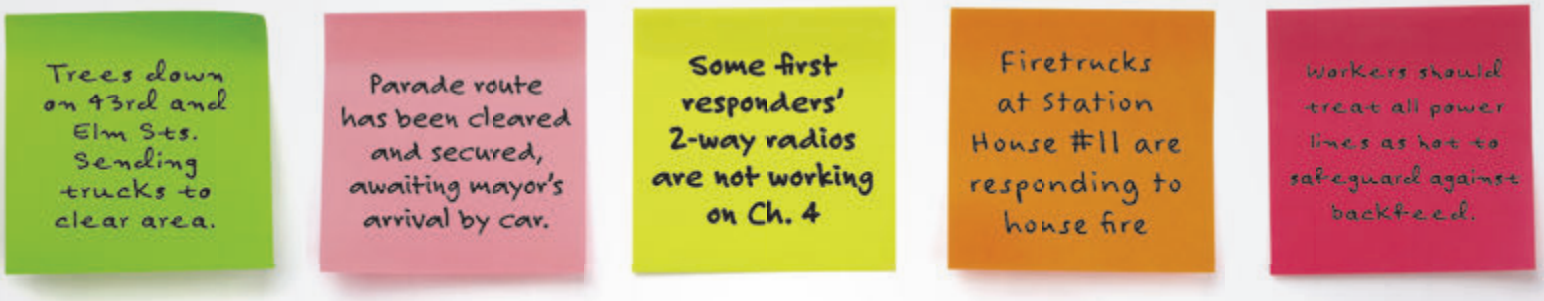
HELP PROTECT THOSE WHO HELP PROTECT US!

Contact SHI for more information about our Video Surveillance Solution, or go to SHI.com/VideoSecurity today!

shi™

SHI.com 888-764-8888

YOU CAN'T EXPECT THIS:



TO KEEP TRACK OF THIS:

In today's complex, fast-paced world of emergency operations, you need an Incident management system that can help your team work as efficiently as possible. Designed to meet all FEMA regulations and offer 100% interoperability, DisasterLAN (DLAN) from Buffalo Computer Graphics is a fully integrated solution advanced enough to handle all emergency situations, yet simple enough to perform day-to-day tasks and non-emergency event management. Plus, the DLAN platform can be customized to meet the needs and budgets of states, counties, and municipalities.

Don't risk another moment — update your system today. Visit DisasterLAN.com or call (716) 822-8668 to request a free demonstration.

DisasterLAN