domestic preparedness .com

DomPrep Journal

Subscribe Volume 10 Issue 2, February 2014

Connections

Business Office
517 Benfield Road, Suite 303
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Susan Collins
Associate Publisher
scollins@domprep.com

James D. Hessman
Editor in Chief
JamesD@domprep.com

Catherine Feinman
Editor
cfeinman@domprep.com

Judith Lawless
Director of Corporate Development
lawless@plcouncil.org

Carole Parker
Business Development Manager
cparker@domprep.com

John Morton
Senior Strategic Advisor
jmorton@domprep.com

David Van Gasbeck
Strategic Advisor
vangasbeck@plcouncil.org

Advertisers in This Issue:

American Military University (AMU)

BioFire Diagnostics Inc.
(previously Idaho Technology)

FLIR Systems

GovSec 2014

Preparedness, Emergency, Response, and Recovery (PERRC) Conference

PROENGIN Inc.

DomPrep Journal is electronically delivered by the IMR Group Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for their use or interpretation.

IMR GROUP

Editor's Notes

By Catherine Feinman

A common characteristic of almost all disasters – natural, human-caused, and technological – is the need for information before, during, and after the incident. However, agencies and jurisdictions not only need to share this information, they also must ensure its protection. As technology facilitates interconnectedness between planning and response agencies as well as the public, incidents like the leaks at the U.S. National Security Agency highlight the balance between gathering/sharing data and protecting personal/corporate privacy.

In this month's issue of the *DomPrep Journal*, authors share the benefits of and concerns related to building better connections. Tom Ridge leads this issue with a warning: The consequences of not making cybersecurity an integral part of risk management and strategic decision-making plans can be devastating. He recognizes that interconnected technologies, communities, and infrastructures create greater efficiencies, but also greater concerns. Craig DeAtley illustrates how electronic healthcare information systems at hospitals offer advanced capabilities, but stresses that the added benefits involve certain risks.

Bonnie Butlin offers one example of how Canada is pooling resources to leverage human networks and professional information sharing to combat cyberthreats. Across the border in the United States, the Naval Criminal Investigative Service (NCIS) protects the homeland from such threats as described in Aaron Sean Poynton's interview with NCIS's former Director Thomas Betro. Raphael M. Barishansky and Seth J. Komansky describe how fusion centers are connecting more than just law enforcement agencies and how these new partnerships are able to better protect the nation from public health threats.

As threats change, the programs and policies to counter those threats must also change. Timothy Stephens cites the existing CHEMPACK program, which connects U.S. communities with necessary medical countermeasures, as one program that is due for an update. Social media is another tool that is constantly changing. By sharing her vocal talents with social media connections, Tanya Ferraro brings out the human side of emergency management and prepares the public to shelter in place when needed.

Regardless of the exact threat, all key stakeholders must plan, train, and exercise for small- and large-scale disasters. Ken Lerner and George Yantosik suggest building connections and agreements well in advance of a disaster to promote successful joint exercises. Unfortunately, when situations change, valuable resources may be lost. Joseph Cahill presents ways to simultaneously maintain resources and raise the level of emergency medical care.

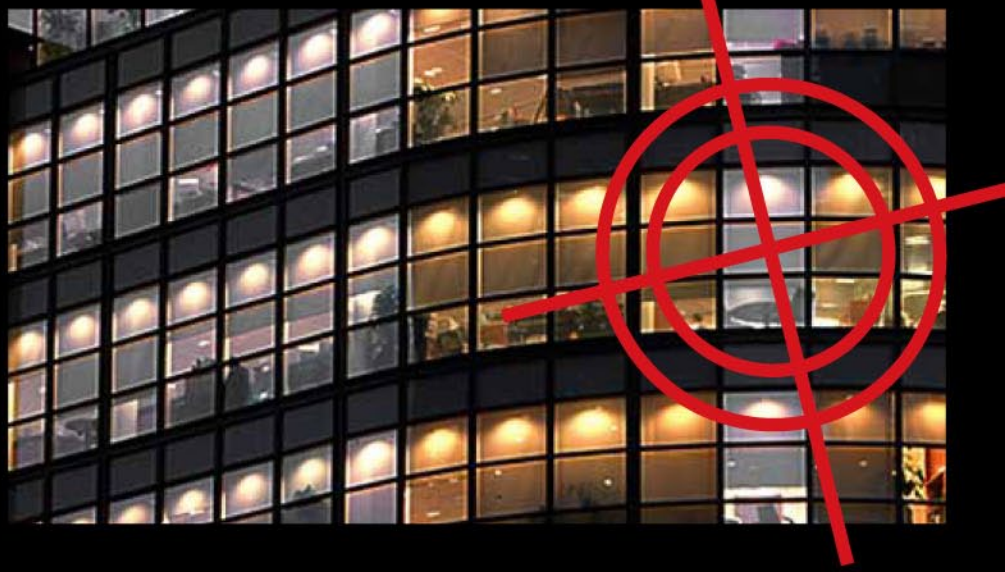
About the Cover: In today's interconnected society, technology plays a large role in emergency preparedness and response. However, the human resources and social networks are critical for the success of such efforts. (iStock Photo)

Unknown Chemical or BioHazard?

AP4C Handheld Chemical Detector

Known Solutions

AP4C-F Fixed Location Chemical Detector



- Unlimited, Simultaneous Detection
- Fast and Easy to Use
- Always Ready with Very Low Operation Cost
- Rugged Construction for Harsh Environments

PROENGIN

Chemical and Biological Detection System

PROENGIN, inc. | 140 S. University Dr, Suite F, | Plantation, FL 33324 USA
Ph: 954.760.9990 | contactusa@proengin.com | www.proenginusa.com

DomPrep Writers

Raphael M. Barishansky
Public Health

Joseph Cahill
EMS

Craig DeAtley
Public Health

Kay C. Goss
Emergency Management

Stephen Grainer
Fire/HazMat

Rodrigo (Roddy) Moscoso
Law Enforcement

Glen Rudner
Fire/HazMat

Richard Schoeberl
Law Enforcement

Joseph Trindal
Law Enforcement

The Operational Imperative of Cybersecurity & Resilience

By Tom Ridge, Viewpoint

Technology has changed the world at a speed never before seen in human history. In a span of just two decades, the Internet has become the backbone for the way people live, do business, and communicate. Therefore, concerns about cybersecurity are illuminating not just community and state interconnectedness, but global interdependence and its accompanying hazards. Leaders in both government and business must plan to meet these challenges as cyber risk-management practices continue to mature.

High-Consequence Incidents

A mass-effect cyber incident is more than just a narrow scenario for which emergency response and management officials need to plan. The use of Internet Protocol-based devices and systems further amplifies the vast interdependencies between critical infrastructure sectors. From hand-held devices to large operating systems, and from smart grids to financial mechanisms, these devices and systems are the basis for all government and commercial activity. If exploited, the potential exists for a resoundingly detrimental impact on both U.S. national security and economic vitality.

And should the nation's worst fears be realized – critical infrastructure failures as a result of a cyber attack – the impact would not only affect the jurisdictions and citizens that emergency professionals serve, but their very own systems and operations as well. In an instant, power, communications, and other vital capabilities could be lost for extended periods.

There has never been a time when the need for public and private collaboration has been greater, primarily because of the overlay of infrastructure assets. The public-private partnerships and industry working groups that provide an excellent forum for collaborating on natural disasters, accidents, and other threats in the physical domain also must fully integrate cyber resilience. However, external relationships are just one part of this important equation.

Business Imperatives & Leadership Priorities

For multinational businesses, Ridge-Schmidt Cyber counsels chief executive officers that they can no longer view cybersecurity, preparedness, and resilience as an issue for the chief information officer or "tech shop." If cyber threats can affect every aspect of an enterprise – from data and communications to logistics and, ultimately, reputation – then cybersecurity must be an internal business imperative and leadership priority.

The same holds true for leaders of public institutions, particularly the emergency management and crisis response agencies that respond to

large-scale incidents. Cyber awareness inside public sector agencies must be an operational imperative.

Leaders such as John Madden, Alaska Homeland Security and Emergency Management Director, understand this imperative not only for his home state, but also for the emergency management profession. Madden made cybersecurity a key focus during his 2012-2013 presidency of the National Emergency Management Association. Across the broader homeland security community, agencies and organizations should continue to challenge themselves to become more educated about the cyber domain and to continuously assess its impact on their own operations. Furthermore, everyone should be prepared to evolve as cyber threats evolve.

Although the intersection of the physical and cyber domains raise complex questions, ironically, many of the answers for dealing with the threats and potential consequences begin with basic risk management principles. Leaders need to carefully assess what enterprise assets are vulnerable, prioritize mitigation activities, properly resource these activities, and take action with an eye toward continuous improvement.

For all organizations, both public and private, cyber resilience is not simply the responsibility of the chief information officer or other information technology executives. It is a critical business and operational challenge that the highest levels of leadership must address. As technology integrates into seemingly all critical business and governmental undertakings, cybersecurity must be an integral part of enterprise risk management plans and entrenched in the broader strategic decision-making processes.

Tom Ridge, the nation's first secretary of the U.S. Department of Homeland Security and 43rd Governor of Pennsylvania, is the chief executive officer of Ridge Global and co-founder of Ridge-Schmidt Cyber, a consultancy helping leaders in business and government solve complex cybersecurity challenges.

Cyber Grand Strategies: Technology vs. Human Interaction

By Bonnie Butlin, Cyber & IT

The National Security Agency (NSA) leaks by former NSA contractor Edward Snowden became public on 5 June 2013 in *The Guardian* and revealed more than just classified documents. They revealed a U.S. cyber grand strategy intended to secure the homeland from terrorist attacks, employing NSA programs based on an extrapolation of Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, and on Section 702 of the Foreign Intelligence Surveillance Act of 1978. The cyber strategy was grand-strategic, having been applied in a global security context, during peacetime operations, on U.S. soil, with resources beyond a military scope.

The U.S. Approach to Cybersecurity

Counterterrorism arguably requires a grand-strategic approach: it aims to protect civilians on U.S. soil in peacetime; requires extra-military means, such as law enforcement and intelligence resources, and cooperation of the telecommunications companies; and entails a global element. The Privacy and Civil Liberties Oversight Board (PCLOB) found, in its 23 January 2014 report, that there was no identified U.S. terror nexus, rather that the threat had a global dimension. Once revealed, the technology-driven cyber grand strategy proved unpalatable to the people in the United States, and the associated programs are currently under review and/or NSA is rolling them back.

The NSA's 215 and 702 programs were the basis for the cyber grand strategy with a light footprint launched against a strategic terrorist threat within U.S. domestic space that also had a light footprint. Similar to using air power to find enemy operatives in a large area of military activity, cyber grand strategy employed a nonphysical presence that allowed the United States to find single terrorist "needles" within the U.S. domestic "haystacks" using cyber technology. The new cyber technology allowed for unprecedented scope, scale, and duration of the search and, like air power, enhanced awareness and control of the domestic multidimensional battlefield, or "battlespace."

As terrorists could blend into the population and potentially could strike anywhere, U.S. cyber surveillance – through the 215 and 702 programs – could monitor their communications everywhere. By using bulk collection without specified reasonable articulated suspicion (RAS) and by employing sophisticated computational analysis of metadata, the NSA was able to conduct surveillance without the knowledge of the U.S. public.

The two NSA programs could corroborate existing intelligence on terrorists and terrorist activities, generate new lines of investigation, and identify and monitor persons of interest. Even with this enhanced domestic battlespace awareness, given domestic restrictions, the programs had little likelihood of success. The terrorists were still "needles," and the data trove enormous and growing. According to the 23 January 2014 PCLOB report, the NSA programs neither identified nor disrupted any active plots, but did identify one previously unknown terrorist. The collateral damage from the programs quickly became apparent in the form of privacy concerns, fears of abuse, and deterrent effects on free speech and association.

Lightening the Cyber Grand Strategy's Footprint

The technology-driven programs emerged from a weak legal footing. Section 215 of the USA PATRIOT Act (originally intended for handover of specific existing business records in relation to specific investigations) was loosely extrapolated to allow for broad and continuous cyber bulk collection, without applicable Supreme Court jurisprudence dealing with cyber collection, retention, and analysis of comparable scope and duration. Terrorists, who were anywhere in the United States, were certainly communicating by telephone, so the NSA looked everywhere, treading increasingly heavily through the metadata to find them: collecting records in bulk, contact chaining with three "hops," using sophisticated computational metadata analysis, and leveraging the historical connections contained within years of stored data. The programs quietly expanded into what was arguably a strategic, full-saturation surveillance presence – well beyond the light-footprint approach originally envisioned.

Following the Snowden leaks, President Barack Obama met with the PCLOB on 21 June 2013 to discuss the imbalance between the NSA's counterterrorism operations

and growing privacy concerns. In the 17 January 2014 Presidential Policy Directive PPD-28, to safeguard personal information, Obama ordered a number of reports and studies from the PCLOB, the Office of the Director of National Intelligence, and the President's Intelligence Advisory Board. He sought additional protections that include the use of special advocates, fewer "hops" and greater oversight, increased publication of government requests, and additional protections for non-U.S. citizens. Also requested was a study on the feasibility of software that could target with more focus and accuracy within the NSA programs – a more-surgical technological solution. Obama also encouraged the prioritization of collection methods other than bulk collection, but did not go so far as to shut down the programs. These responses strive to reduce the weight of the cyber grand strategy's footprint to its intended light footprint, without foregoing the unique vantage point and awareness that the NSA programs provide, albeit with mixed results.

The Canadian Approach to Cybersecurity

An alternative cyber grand strategy has emerged in Canada (where the intelligence community also received ministerial approval to collect metadata in both 2005 and 2011). Also a broad cyber approach with a light footprint, it relies not on technological solutions such as bulk data collection and metadata analysis, but rather on human networks and professional information sharing, which carry less risk to personal information and privacy than the NSA programs.

The Inter-Association Working Group on Cyber Security (IAWGCS) of the Canadian Security Partners' Forum focuses on networked information sharing among cyber professionals. The IAWGCS has brought together the Canadian professional associations with a stake in cybersecurity – 50 distinct associations from a total of some 120 identified security-related associations across Canada.

Professional association memberships bridge the private and public sectors, all levels of government, and all geographic regions of Canada, as well as reflect 50 unique association perspectives on cybersecurity issues – including but not limited to terrorism. Approaching issues from 50 different professional angles provides unprecedented contextualized understanding of the cyber landscape and unmatched depth of expertise that is credible, transparent, and nonintrusive. The resulting battlespace awareness does not target individual persons of interest, but arguably leaves decreasing room for terrorist activity to slip between seams and operate undetected within Canadian space.

The NSA programs focus technology on identification and attribution at the individual level for preventive and even pre-emptive counterterror efforts, whereas the IAWGCS – through the engagement of many diverse cyber professionals – provides a multivector, high-level, strategic, and shared understanding of the cyber landscape in Canada. The Canadian approach has little risk of developing a heavy-footprint presence because the existing expertise can achieve results without infringing on additional personal privacy space. The Canadian Security Partners' Forum focuses on information sharing among security professionals to build the general Canadian security capacity, whereas the IAWGCS specifically focuses on building the Canadian cybersecurity capacity. Unlike the one-way NSA bulk collection, storage, and analysis of data, the IAWGCS can both push and pull information through its network, similar to the "work-related access" model of intelligence sharing that Obama proposed in his 17 January 2014 address to the nation. The IAWGCS is a broad, flat-structure network of cyber professionals that supports more-fluid information sharing, with a light but comprehensive national presence.

Both cyber grand strategies are enhancing security domestically in peacetime – the NSA programs using technology-driven metadata, and the IAWGCS leveraging human-networked interactions among cyber professionals. The NSA programs are more immediate in their objective of disrupting terrorist activities, whereas the IAWGCS focuses on long-run strategic effect in building capacity and resilience within Canadian security. Although the IAWGCS appears to be more palatable to the public in the short run, the two cyber grand strategies (technology- and human-based) may in the long run be complementary in securing the homeland.

Bonnie Butlin is executive director of the Canadian Security Partners' Forum (CSPF), and managing director of the Canadian Security Executive Forum (CSEF). She has a diverse background in the fields of defence, intelligence, and security; and she was the sole author of a commissioned study for the Federal Court of Canada on National Security and the Administration of Justice. She also was named one of Security Magazine's "Most Influential in Security" for 2013. She holds an MA in international affairs, with a specialization in conflict analysis and resolution. Her focus areas include: domestic threat networks; gray-area threats (including synergies among insurgency, terrorism and organized crime); and military and counterinsurgency strategy.

The Real NCIS: An Interview With Thomas Betro

By Aaron Sean Poynton, Interviews

More than a decade after it originally premiered, CBS network's "NCIS" is still one of the most watched television shows in the United States. To better understand the nonfictional Naval Criminal Investigative Service (NCIS), the *DomPrep Journal's* Aaron Poynton spoke to Thomas Betro, former director of the NCIS and current vice president of national security with NTT Data (a data communications business), on 6 February 2014 in Washington, D.C.

Aaron Sean Poynton: *What were your primary and most interesting responsibilities when you served as director of the Naval Criminal Investigative Service?*

Thomas Betro: My primary mission was to ensure that the people within the organization had the resources, the training, the information, the environment, and the guidance needed to succeed. Secondary to that, my responsibilities were:

- To make sure that our resource sponsors and our customers recognized and understood the great work that our people – be it special agents, intelligence analysts, or operational support personnel – were doing; and

- To emphasize why this work was so important to the safety and security of sailors, Marines and their families, and the civilians they served.

The NCIS mission is to identify, investigate, and disrupt criminal, terrorist, and foreign intelligence threats to the U.S. Navy and Marine Corps – ashore, afloat, and in cyberspace. Each one of the operational disciplines, criminal investigations, counterintelligence, and counterterrorism is critical; and NCIS takes great pride in the work that they do and understand the relevance, importance, and value of that work. I had the pleasure over the course of my 27 years of service to participate in all of the different types of work that we did. Whatever assignment I had at any given time, I always considered that as the most important and critical to the mission, and to the organization.

In the end, I sat in a position where I could interact with and admire the work of all of the talented and dedicated people of NCIS on a daily basis. NCIS, in my opinion, would not be the same organization if we did not have the variety of missions along with a very diverse work force, and if all the people were not performing in harmony and at such a high level.

We had overarching strategic goals of preventing terrorism, protecting sensitive information, and reducing crime. Our leading priority during my tenure, however, was counterterrorism. After the terrorist attack on the *USS Cole* in October 2000, the Department of the Navy made force protection and counterterrorism a strategic priority, and so did NCIS. NCIS played a very important role in investigating that attack. We saw and experienced the impact of terrorism on the Navy firsthand. All of the other missions fed our ability to execute our counterterrorism mission. Day to day, we wanted everyone to understand that all of our missions were important but counterterrorism was the leading priority.

Poynton: *When you were director, what specific efforts did you lead at NCIS that directly contributed to keeping the U.S. homeland safe?*

Betro: My role was to assign strategic and mission priorities and, as I mentioned earlier, make sure our people were trained and equipped for success. With respect to supporting homeland security, we contributed several ways. Our overseas missions may have brought the greatest value to the country's counterterrorism, antiterrorism, and homeland security efforts. We assisted in defending the homeland by taking the fight to the "bad guys" and disrupting them on their turf before they could get to U.S. soil. In addition to the thousands of NCIS personnel who deployed to Iraq and Afghanistan where they conducted counterterrorism operations and investigations, NCIS is a global law enforcement organization – and approximately one-third of NCIS special agents are located overseas at any time. NCIS has been operating daily in and around foreign ports for decades and has built not only a deep understanding of the maritime domain, but also strong relationships with foreign law enforcement and security organizations that operate in those areas.

Former Director Thomas Betro, Naval Criminal Investigative Service (NCIS)

In the early 2000s, after the attack on the *USS Cole*, we began to understand how these relationships that had served our local criminal investigative and counterintelligence missions for so many years could be leveraged to gather intelligence that could support not only NCIS's counterterrorism mission, but the broader U.S. counterterrorism effort to defend the homeland as well. The maritime domain, in particular the international shipping that operates in it, represents a huge opportunity for terrorists to move contraband, money, and people around the world – including into the United States.

NCIS was and is well-positioned to gather critical intelligence and conduct counterterrorism operations in the maritime domain and overseas, all of which contributes to the security of the U.S. homeland. In the United States, we contributed to homeland security on a daily basis through our own investigations of suspected terrorists, and through our participation in FBI [Federal Bureau of Investigation] Joint Terrorism Task Forces, as well as numerous joint task forces at the state and local levels.

Poynton: *How has the use of technology helped NCIS conduct its mission, especially when it comes to forward-deployed forensics and exploitation?*

Betro: Technology has fundamentally changed the way that NCIS and most other law enforcement and intelligence organizations do business – from headquarters to the far ends of the world where "the rubber meets the road," so to speak. Technology is woven into every process and every action that NCIS agents, analysts, and support personnel do everyday – from the front end on the operational side with evidence collection to computer software and hardware that analysts use to process information and conduct data analysis. This is particularly true in the area of forensics, cyber forensics, and digital forensics.

There is not one single investigation that NCIS works today that does not have a digital component – not one; whether it is a computer, tablet, cell phone, camera, or email. In every instance, there is a need to understand the digital environment and the digital trail of evidence available through the use of modern technology, and to take advantage of all that information in a legal and productive way.

One good example of how technology affected operations when I was director was how it enhanced our ability to safely and effectively accomplish the mission in combat and combat-contingency environments. For example, in Iraq and Afghanistan, there would be crime scenes that were in hostile environments off base. Because of the dangerous nature of the environment, a security detail of Marines or soldiers would have to escort our personnel to and from the scene, and would stand guard while our people were at the scene.

Obviously, due to the threat of attack, we did not have the same amount of time as we would in noncombat environments to conduct crime-scene examination. We could not put up the crime scene tape and secure the scene and possible evidence for days. In these cases, we would put a mission plan together that would determine the amount of time on scene; sometimes we were lucky to get only a few hours. This does not mean the investigation, collection, and processing was any less important; rather, we relied on the technology and it enabled us to develop procedures that allowed us to get to those scenes, document and process the scenes quickly, and get out safely, without sacrificing the quality of the examination.

When I look at what gaps exist and where the potential is for industry, it is in the area of "big data." Technology

has allowed us to gather more information, in more different forms, than ever before. It is becoming harder to find the important bits of information, rapidly, in that large reservoir of data that is collected. Synthesizing all of that data and processing the data into a form that is searchable and analyzable are challenging. We have made great strides, but there is more room to grow solutions in that area.

Poynton: *In 2008, the U.S. Department of Defense suffered the worst breach of cybersecurity in history. As a result, the Department of Defense dramatically increased focus on cybersecurity. Cyber is now one of several core mission areas of NCIS. What is NCIS's role in cybersecurity?*

Betro: People use the term "cybersecurity" broadly, but there are many components to cybersecurity. NCIS is not directly responsible for cybersecurity. By that I mean, NCIS is not responsible for information assurance. We are not responsible for hardening the networks; we are not responsible for software being secure and clean; and we are not responsible for ensuring that firewalls were in place. NCIS operates in cyberspace while fulfilling its primary missions of law enforcement, counterintelligence, and counterterrorism.
Under its criminal investigative hat, NCIS investigates actual or attempted hacks into DON [Department Of Navy] Networks and crimes conducted in cyberspace. From a counterintelligence perspective, NCIS was responsible for investigating suspicious and/or illegal activities occurring on DON Networks that might be attributed to foreign intelligence services. We endeavored to find out: Who was behind the activity? What tools and techniques facilitated their activities? What were the networks and/or the information they were interested in and why?

Poynton: *Edward Snowden, Robert Patrick Hoffman, Nidal Hasan, and Aaron Alexis are recent notable examples that demonstrate how some of the United States' most significant threats come from within. How do you assess the insider threat and what efforts did you undertake at NCIS to mitigate this threat?*

Betro: The concept of insider threats is not a new phenomenon. Use espionage as a great historic example. Go all the way back to the revolutionary war and Benedict Arnold. George Washington himself was certainly aware of the harm that could be caused by a trusted insider. More recently, Robert Hanssen and Aldrich Ames are notable examples of the damage insiders with authorized access to information and IT [information technology] systems can do to harm national security.

The wide adoption of the term "insider threat" was initially driven, in my opinion, primarily by a concern about the harm that a trusted insider could do to national security in the digital Internet era. The horrible tragedies at Fort Hood [Texas, 5 November 2009] and the Washington Navy Yard [D.C., 16 September 2013] have opened our eyes to the physical harm that can be perpetrated by a so-called insider. As a result, people who were not thinking about an insider threat before are thinking about it now, and they are thinking about it in different ways than just espionage, which is a good thing.

There have been procedures in place at select agencies for decades to try to prevent insider threats. Procedures such as polygraph examinations and background investigations have been geared toward preventing insider threats. Although, it should be noted that Ames, Hanssen, and even Snowden all had background

NCIS Director Thomas Betro shakes hands with Special Agent Mark Clookie as Chief of Naval Operations Admiral Gary Roughead looks on. Photo taken during a 2009 Washington Navy Yard ceremony honoring NCIS personnel who deployed overseas as part of the Global War on Terror.

U.S. Navy Lt. Dylan Harmon, officer in charge for the Naval Criminal Investigative Service, demonstrates handcuffing procedures with the Authority Port Nationals in Cap-Haitien, Haiti, on 21 February 2012.

investigations and polygraph examinations. Now, many organizations have software tools that enable automated monitoring of computer activity by employees and alerts to anomalous activity. Of course, a balance needs to be struck between security and privacy. Even though in most instances, in both the government and in the private sector, employees agree to be monitored as a condition of employment, the minute an agency actually does that and the employees find out about it, they usually are not very happy.

The concerns about insider threats have driven high-level policy changes as well, such as the requirement for federal departments and agencies to establish formal insider threat programs. The intent of these programs is to ensure there is a concerted effort to understand the environment in order to be able to reasonably detect indications of a possible insider threat.

Poynton: *An NCIS agent was the first to respond to the September 2013 mass shootings inside the Navy Yard's Building 197. Are NCIS agents adequately prepared, trained, and equipped to respond to such attacks?*

Betro: First, let me say, from what I have been told, the NCIS agents on scene did a fabulous job and I give them tremendous credit for the courage they displayed to go in there – in that huge building, with no sense of where the suspect was or how he was armed. These agents were not part of an active-shooter response team or a SWAT [Special Weapons And Tactics] team, they were, more or less, just first responders who wanted to try to save people's lives at the risk of their own. They could have waited for the arrival of the heavily trained, armed, and equipped active-shooter teams, but they knew every minute could possibly result in the death of another innocent victim. So, they went into the building. They exhibited tremendous courage.

Most NCIS agents have a certain degree of tactical training, but they do not go through specialized SWAT or active-shooter training; typically, while carrying out their day-to-day duties, they wear a suit and carry only a handgun and handcuffs. All special agents are issued bulletproof vests, but they normally are not worn unless the agent expects, in advance, that he or she might find themselves in a tactical situation. NCIS special agents go through rigorous firearms and unarmed self-defense training at the Federal Law Enforcement Training Center [Ga.]. Much of NCIS's tactical training is geared toward effecting high-risk apprehensions or executing search warrants in dangerous situations. In many of these cases, NCIS plans ahead of time and executes that activity when they are prepared for the mission – they are equipped and armed properly, and have conducted dry runs. This base level of tactical training is consistent with most federal law enforcement organizations.

Teams that are specifically trained in active-shooter or SWAT tactics are best to respond to these incidents. I think it is important to note that NCIS is not a traditional first responder law enforcement agency. NCIS special agents are investigators who generally respond to scenes that have already been secured by responding uniformed police officers or military personnel. However, as you can see from this event, everyone has to be prepared to become a first responder to an active-shooter incident. It is a mindset change now. The agents involved will likely tell you they never expected to be engaged in such an incident.

I believe the current director, Andrew Traver, has already begun to take steps to change the way agents and the organization are prepared to respond to events

such as this. I believe there are new training courses that the director is pursuing to advance that level of tactical training. The director is widely examining equipment, training, and policy, and there will likely be some changes to enhance readiness posture. After a rare and tragic event like this, you review, assess, and make changes; you also strengthen and sustain what has been validated and worked well.

Poynton: *International maritime piracy remains a significant threat on the open seas. One of the most noteworthy cases is the April 2009 hijacking of MV Maersk Alabama, which occurred during your time as NCIS director and was recently dramatized in the film "Captain Phillips." What role did NCIS play in that incident?*

Betro: NCIS plays a major role in collecting intelligence against pirates, investigating acts of piracy, and supporting prosecutions of pirates. Special agents work aboard U.S. Navy ships that are tasked with defending the shipping and the maritime industry against pirates.

Not everything on television is real. Former director of the Naval Criminal Investigative Service (NCIS) separates fact from fiction.

With *MV Maersk Alabama* specifically, we went to the crime scene of the lifeboat where Captain Phillips was held and the pirates were subdued. We did a full crime-scene investigation and gathered evidence to support prosecution – forensics, interviews, and interrogations. We also had to assist in determining legal jurisdiction – where would a case be prosecuted? Many factors were considered, but the surviving pirate, Abduwali Muse, was ultimately brought to New York for prosecution. The charge of piracy carries a mandatory life sentence without parole but, in a plea deal to lesser charges, Muse received a 33-year sentence and is currently serving time in a U.S. federal prison.

NCIS also recently supported the FBI and members of the Joint Terrorism Task Force in the investigation and prosecution of Somali pirates for acts of piracy [in April 2010] against the *USS Ashland*. This represented the first conviction for piracy in Norfolk [Va.] in more than 150 years. Although there have not been enough prosecutions of pirates to build a dataset to determine if these prosecutions deter piracy, pirates should be warned – if you commit an act of piracy, NCIS will investigate and support prosecution against you.

Poynton: *In addition to your work as vice president at NTT Data, I understand that you recently became an advisor to Governor Thomas Ridge's Flag Bridge Team. What does that role entail and what do you see as the best opportunities for the maritime industry to enhance security?*

Betro: The maritime industry today is so critical to the world economy, especially in the era of just-in-time shipping and globalization. Threats and vulnerabilities to the industry are both internal and external. Like all logistics businesses, there is an emphasis and a business need to keep things moving. In that busy environment, shippers are subject to a lot of criminal activity and fraud. Companies are not always equipped to deal with those things and the tendency is to write them off. Hundreds of millions of dollars each year are lost because of criminal activity and fraud. The other set of threats is external, such as piracy or terrorism. Pirates and terrorists will prey on the vulnerable open waters and exploit the maritime industry for financial gains, such as ransoms or ideological advancement using terrorism.

There is help available from industry experts; companies do not have to be distracted from their core competencies. There are proactive ways to reduce the criminal threat and save money while continuing to run the business smoothly and uninterrupted. I agreed to be an advisor to Governor Ridge in maritime investigation and security because I recognized that some of the resources available to help solve this problem could be former NCIS experts who spent their entire lives in the maritime domain conducting investigations and performing security and antiterrorism operations; they understand that domain and the environment. Governor Ridge also recognized this and added that capability to

identiFINDER® R300
Personal Spectroscopic Radiation Detector (SPRD-CZT)
for under than $10k

BECAUSE IT'S NOT JUST YOUR JOB, IT'S YOUR LIFE.™

The difference between life and death is in your hands. FLIR CBRNE threat detection products provide lab-caliber analysis where you need it most – in the field. When lives are at stake you need fast, accurate results you can trust.

FLIR®

his maritime bridge to enhance his offering to the maritime industry to prevent terrorism and reduce crime with the industry's leading professionals.

Poynton: *Lastly, while serving as Director of NCIS you made a cameo appearance as "Agent Betro" on Season 5, Episode 4 of CBS television's show NCIS. How much is the show like the real thing?*

Betro: I am a big fan and I think it is a great show. You are right – I did a cameo scene, but my role only entailed fetching coffee for Mark Harmon. The show is often based on real cases but, on the other hand, it is entertainment. Like most entertainment, it reflects real life but many aspects of the show are fictionalized and dramatized. The television show does a good job in taking the real types of investigations that NCIS works and spinning them into a very entertaining portrayal of real life. Sometimes this includes accelerating the ability to do certain things that take a lot of time in real life. The things they do in an hour to solve a crime, such as cyber investigations and laboratory analysis, can take days or weeks; it is a more drawn out process to collect and analyze the evidence and report the results.

My other observation is that the television show has individuals that do everything. The real-life NCIS has a lot of talented agents, but many of the functions performed on the show are performed by several different people – specialized professions with tons of education, experience, and credentials. Lastly, and I am asked about this frequently, we do not have our own morgue at NCIS. We use the city and federal facilities and external resources. The ability to go to the basement and have an autopsy done is not real. We do attend autopsies frequently, but not in the basement of the NCIS office.

I can tell you first hand, the show cast and crew are great people and strive to keep the episodes as realistic as possible. They spend time with real NCIS agents and are in close communication with the NCIS communications director. The television show has certain agents and former agents they have worked with over time to add realism in the way the show describes and says things – using much of the actual jargon that you would hear on a typical day at the real NCIS. Either way, real or dramatized, I am glad that the U.S. public gets to see and understand the hard and sometimes dangerous work our agents perform on a regular basis to keep the Navy, Marine Corps, and the citizens of the United States safe.

Thomas A. Betro served as the director of the Naval Criminal Investigative Service from January 2006 to September 2009. Since joining the NCIS in 1982, his assignments have included such unique missions as "Special Agent Afloat" during deployments of the aircraft carriers USS John F. Kennedy and USS Enterprise. Following an appointment as the acting national counterintelligence executive, he returned to the NCIS as assistant director for counterintelligence and was subsequently promoted to deputy director for operations. He holds a BA from Colby College and an MA from the Naval War College. His numerous honors include the Presidential Meritorious Executive Rank Award. Today, he serves as vice president at NTT DATA and advisor to Ridge Global's Flag Bridge strategic maritime team.

Aaron Sean Poynton (pictured at the beginning of the article) is a guest writer for the DomPrep Journal and the director of global safety and security business at Thermo Fisher Scientific. Previously, he served as a director at Smiths Detection, a global technology company in the defense and homeland security markets. Before his civilian career, he served in the U.S. Army Chemical Corps and Special Operations. He is a graduate of the Johns Hopkins University Army ROTC program and holds a bachelor's degree in economics from the University of Maryland UMBC, a master's degree from the George Washington University School of Business, and a doctorate in public administration from the University of Baltimore.

Fusion Centers & the Public Health Advantage

By Raphael M. Barishansky & Seth J. Komansky, Public Health

Across the United States, fusion centers serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial (SLTT), and private sector partners. Currently, there are more than 70 "fusion centers" located across the United States, with a center in every state and most major cities. The U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) recognize these centers as critical elements supporting situational awareness.

Expanding Capabilities & Information Sharing

An element of situational awareness includes collaborating with emergency medical services (EMS), fire services, emergency management, and public health partners. Although initially with an emphasis on the criminal intelligence environment, fusion centers have segued into an all-hazards environment, with the overall focus on building multidisciplinary partnerships. In many cases, these partnerships strengthen public health agencies to better protect the public in disaster situations such as disease epidemics, chemical and radiological releases, severe weather, and natural disasters.

Codifying this operational charge, the National Preparedness Guidelines outline specific capabilities that require action by various public health stakeholders. These capabilities are enhanced by: sharing appropriate information; strengthening chemical, biological, radiological, nuclear, and explosives (CBRNE) detection, response, and decontamination; and strengthening medical surge and mass prophylaxis capabilities. Additionally, Homeland Security Presidential Directive 21 (HSPD-21) requires that DHS develop mechanisms and processes to share both classified and unclassified threat information with the appropriate members of the public health community.

In return, public health partners that represent nontraditional information gatherers can provide fusion centers with both strategic and tactical information, including: (a) crime-related trends (e.g., prescription drug fraud); (b) additional response capabilities; and (c) suspicious activities (e.g., unusual diseases reported at hospitals). Together, public health agencies and fusion centers support the enhancement of the nation's health security by using a variety of surveillance and detection tools to enhance information-sharing activities with homeland security and first responder partners.

The Need to Work Together

Fusion centers bring together expertise from disparate areas of the emergency services community and have been used to: (a) manage Strategic National Stockpile projects; (b) map out potassium iodide provisions for emergency planning zones; (c) maintain registries of dangerous biological agents in a discrete geographic area; (d) coordinate responses to chemical/radiological incidents; and (e) manage the Centers for Disease Control and Prevention's Health Alert Network.

There are four public health scenarios in which fusion center partnerships would be critical for ensuring timely, efficient, and effective preparedness, response, and recovery efforts: bioterrorism attacks, communicable disease outbreaks, suspicious activity reports, and illicit drug hazards.

Bioterrorism – Often, there is a potential failure to consider criminal intent when an infectious disease outbreak begins. Public health and law enforcement agencies can work together for both overt and covert bioterrorism releases. Overt attacks – for example, the 1995 sarin release by Aum Shinrikyo in the Tokyo subway system – are announced soon after they occur. During this type of incident, law enforcement officers and other responders often are the first to arrive. After detecting a bioterrorism incident, public health agencies and the Centers for Disease Control and Prevention (CDC) provide technical assistance to help further threat detection efforts. Expanded medical surveillance and epidemiological investigation follow.

In a covert attack, public health professionals are likely to be the first line of defense. When trending unusual

illnesses or disease clusters, public health officials may be the first to recognize a threat. By sharing this information with a fusion center, this partnership could potentially increase the number of lives saved. An October 2002 article in the CDC's *Emerging Infectious Diseases* online publication cites one example that occurred in 1996, when an outbreak of gastroenteritis among the laboratory staff of St. Paul Medical Center in Dallas, Texas, was caused by *Shigella dysenteriae* type 2 – a pathogen that is not traditionally found in the United States. An epidemiologic investigation linked the infection with pastries that someone had placed in the laboratory break room; the findings matched the *S. dysenteriae* type 2 from the laboratory's stock strain with samples collected from the ill laboratory workers and an uneaten pastry. A portion of the laboratory's stock strains was missing, and subsequent criminal investigation identified a disgruntled former laboratory employee as the perpetrator.

Partnerships between fusion centers and public health agencies could help ensure timely, efficient, and effective preparedness, response, and recovery efforts for a variety of public health threats.

Communicable diseases – One of the key roles of local and state public health agencies is to provide public health "intelligence" in terms of communicable disease trends, surveillance observations of critical symptoms, environmental health findings, and private healthcare-capacity issues regarding medical surge and community mass-prophylaxis strategies. The integration of public health information creates a more robust, comprehensive picture of community readiness and shares the overall homeland security mission within a community. The CDC requires security and transportation assessments related to the Cities Readiness Initiative and Strategic National Stockpile deployment within regional jurisdictions. The partnership and collaboration between public health agencies and local fusion centers directly addresses both of these needs.

The ability of local law enforcement agencies to participate in site security and transportation planning related to Cities Readiness Initiative activities ensures that public health clinics will be safe and effective in providing prophylaxis to large portions of the population over a short period of time. In addition, site-security assessments of this nature are a CDC-defined "accountability target" as related to Strategic National Stockpile plan development. Another advantage of a fusion center is the input of workforce protection information.

In outbreak/epidemic/pandemic situations, it is important to ensure the health of essential services and staff. In 2008, the City of Milwaukee (Wis.) Health Department created a model for "Enhancing Public Health Preparedness Through Participation in Local Intelligence Fusion Centers." In addition, the CDC's Health Alert Network – a collaborative method of sharing cleared information about urgent public health incidents with public information officers, clinicians, public health laboratories, as well as federal, state, territorial, and local public health practitioners – offers public health agencies the ability to share important information with essential personnel, including protective measures and appropriate personal protective equipment.

Suspicious Activity Reports – Public health and human services agencies frequently work together. This results in home-visit scenarios for child and elder abuse by child protective services or adult protective services. Fusion centers can enhance situational awareness for a variety of threats and vulnerabilities that these public health practitioners may face walking into private houses. These could include recognition of human trafficking or clandestine laboratories, preoperational indicators such as bomb-making materials or stockpiling of public safety uniforms, and other conditions that are often hidden when law enforcement is present. This extra training for personnel would promote the ability to act as an intelligence sensor and report findings back to the fusion center.

Illicit Drugs – In the ever-evolving world of illicit drugs, public health agencies and fusion centers can promote new collaborative efforts. Public health

laboratories, for example, have the ability to evaluate the hazards associated with new synthetic drugs and the effects they potentially have on the user. Other warnings also can be shared, including: risks to law enforcement and EMS personnel when handling specific drugs; potential behavior characteristics of users; or requirements for new or altered treatment modalities.

An example of this occurred in May 2013 in Montreal, Canada. The police intercepted 10,000 pills of desmethyl fentanyl – a fentanyl derivative with potential to be 40-times stronger than heroin and 80-times stronger than morphine – slated for delivery to the United States. Handling the drug without proper personal protective equipment – in this case, gloves and masks – caused illness in four officers. This prompted notifications to other law enforcement agencies along with emergency departments and EMS agencies for the possibility of an increased need for opiate antagonists for such cases.

The Next Steps

An all-hazards approach seeks to include and evaluate more than just "terrorism" events. Nontraditional responders such as public health agencies need to have a permanent place at the table. In many instances, the extra surveillance that these agencies can provide is a great workforce multiplier. By including the public health perspective, law enforcement/homeland security officials can enhance their analysis and evaluation of the available information. There also is a significant need to cultivate a responder culture that is open to secure and timely information sharing, rather than the current emphasis on data ownership and privacy concerns.

Lastly, there is a nationwide concern regarding the funding need for various emergency management/homeland security projects; the fusion centers are not immune from this concern. Various grant streams specific to emergency management/homeland security have seen large funding reductions, and there is concern that fusion centers could be next. These cuts have included various funding streams for public health preparedness efforts, specifically the Public Health Emergency Preparedness and Cities Readiness Initiative grants. The cuts also could have a negative impact on the fusion center relationships that have been developed to date.

This move to share information within fusion centers has the potential to significantly benefit the public health preparedness realm. The two sectors – emergency management/homeland security and public health – traditionally seen as separate and distinct disciplines, should work together cohesively to share resources and avoid duplicating efforts.

Raphael M. Barishansky (pictured), MPH, is director of the Connecticut Department of Public Health's Office of Emergency Medical Services (EMS). Before establishing himself in this position, he served as chief of public health emergency preparedness for the Prince George's County (Maryland) Department of Health and as executive director of the Hudson Valley Regional EMS Council, based in Newburgh, N.Y. He is a frequent contributor to the DomPrep Journal and other publications, and can be reached at rbarishansky@gmail.com.

Seth J. Komansky, NREMT-P, is an advanced practice paramedic and the medical intelligence officer for the Wake County EMS (Emergency Medical Services) System in Raleigh, N.C. He was tasked with the implementation and management of Wake County's Medical Intelligence Unit. In addition, he serves as the EMS field liaison officer coordinator to the North Carolina Information Sharing and Analysis Center, the state's fusion center managed by the North Carolina State Bureau of Investigation. In May 2014, he will graduate from the Homeland Security Management Institute at Long Island University, with a Master of Science degree in homeland security management.

CHEMPACK 2.0: A Policy Roadmap

By Timothy Stephens, Standards

The Centers for Disease Control and Prevention (CDC) launched in 2003 the CHEMPACK program, which "forward places" caches of nerve agent antidotes and symptomatic treatments at the local level "to provide a sustainable resource to respond quickly to a nerve agent incident." Since then, the program has had no fundamental renewal, even with the introduction of new monitoring technologies and products over the past decade.

On 23 January 2014, the Emergency Services Coalition for Medical Preparedness – a coalition supported by private and public organizations to help protect providers in the event of a large-scale biological event – held its first public strategic review of the program in Washington, D.C. This review was part of a larger project to develop policies and operational capacities to ensure the health of emergency services personnel when faced with various public health threats. Responders who have adequate protection are better able to protect the communities they serve. On 3 February 2014, the House of Representatives passed – with a vote of 391 to 2 – the Medical Preparedness Allowable Use Act (H.R. 1791), which would help enhance medical preparedness, medical surge capacity, and mass prophylaxis capabilities. Conditions are favorable for a broader examination of national emergency services protection and preparedness.

The Existing CHEMPACK Program

The CHEMPACK program is a critical asset to the hospital and emergency services communities that support the long-term sustainment and further development of this response asset. Funding constraints should not hinder efforts to derive administrative savings, increase local engagement, and introduce proven technology.

Historically, the management of the program has depended on federal staff members remotely monitoring caches and traveling nationwide to and from localities to replenish expiring drug products. This is an unnecessarily costly process. To achieve the stated goal of a sustainable strategy, the Emergency Services Coalition for Medical Preparedness recommends a significant shift of management responsibility to localities and private sector partners, along with sustained funding for expanding the formulary, which is the official list of drug products in the program.

Local pharmacists – with the support of CDC CHEMPACK staff and product manufacturers/distributors – are capable of managing the rotation of "soon-to-expire" stock as needed. Vendor management of pharmaceuticals has proved to provide superior timeliness, cost effectiveness, and efficiency, given this is a core competency of these firms. Local pharmacists are able to make determinations of needs specific to their own communities. The Internet-based remote monitoring capacity has overcome the rationale for in-person federal inspections.

Recommendation 1 – Local Management

- Transfer select routine CHEMPACK sustainment activities to local pharmacists and use resultant cost savings – via reduced federal staff administrative overhead – to further develop a CHEMPACK quality assurance program, enhance exercises, and expand the CHEMPACK formulary to address additional threats.

- Allow localities to determine the appropriate formulary for local conditions and add products to a defined core CHEMPACK cache – for example, cyanide antidotes and potassium iodide.

- Update current CHEMPACK monitoring systems with cost-effective online systems.

Chemical agent antidote and treatment development has not kept up with initial projections. This also has been true of the larger countermeasure development enterprise. Among reasons cited are lack of incentives for private sector research and manufacture, changes in threat analysis, and time since previous intentional events. Nonetheless, there are important new products awaiting introduction into the CHEMPACK.

Recommendation 2 – Renew & Replenish the Formulary

- Use administrative savings to update the protections provided by the CHEMPACK.

- Use advanced purchase commitments and other modern financing options to provide incentives for enhanced and new product lines.

Repackaging concerns have delayed the expansion of the Shelf Life Extension Program (SLEP) beyond the U.S. Department of Defense to include state and local membership. The current SLEP process requires that extended product be turned over to a "state-licensed, drug-repackaging firm" to have the product relabeled with new expiration dates. If repackaging and associated shipping costs can be avoided, the CHEMPACK annual maintenance costs would be greatly reduced.

Recommendation 3 – Simplify Shelf-Life Management

- Work with manufacturers to identify a "CHEMPACK-Only" version of products. Such versions will have longer initial shelf-life dates and accommodate simplified labeling for SLEP administration.

- Propose to the U.S. Food and Drug Administration that "CHEMPACK-Only" products do not include expiration date data on their immediate containers and packaging. Instead, data would be contained in a pouch affixed to the outside of each CHEMPACK container. At the time of activation, pharmacies would fix expiration date adhesive labels to products before releasing them. When new product expiration dates occur due to SLEP, pharmacies would provide new sets of labels. This approach would greatly reduce repackaging overhead costs.

The CHEMPACK program has not changed in the years since it was developed. In the meantime, the nation has added 30 million residents, 70 percent of them in the southern and western United States. Locally maintained CHEMPACK caches must include periodic threat and hazard assessments taking into account shifts in population and chemical industry expansion. To be the sustainable local asset close enough to population centers, CHEMPACK must continuously improve and expand.

Recommendation 4 – Pilot Change Process

- Fund two or more pilot projects to identify innovative practices for the development of the next generation of locally managed CHEMPACK.

- Establish a practitioner-led Board to oversee a continuous quality improvement process.

The CHEMPACK program is an essential part of national resilience required across the whole community to protect emergency responders as well as the residents they serve. It is time to build a second-generation program via local management, engagement of the private sector, implementation of SLEP efficiencies, and improved use of technology to ensure the efficacy and security of the installations. These four recommendations of the Emergency Services Coalition for Medical Preparedness are a starting point.

Timothy Stephens is an advisor to the Emergency Services Coalition for Medical Preparedness. He owns an independent public health and risk management consulting practice, where he has provided strategic advice to numerous organizations and businesses, including Unither Virology, the Centers for Disease Control and Prevention, Association of State and Territorial Health Officials, National Association of County and City Health Officials, and the National Sheriffs Association. He conducts leadership seminars and is certified in numerous educational assessment instruments including Change Style Indicator and the Paper Planes simulation. He is an adjunct instructor at the Vanderbilt University School of Nursing, and has a master's degree in communications from the University of North Carolina at Chapel Hill.

Preparing the Next Generation for War on the Virtual Battlefront

By Rodrigo (Roddy) Moscoso, CIP-R

Although President Barack Obama made only a passing reference to cyberthreats in his State of the Union speech on 28 January 2014, the almost daily instances of high-profile (and mostly successful) cyberattacks on U.S. commercial and governmental organizations demonstrate a growing threat in the borderless digital landscape. From Target and Neiman Marcus to popular web services such as DropBox and Drupal – in addition to government agency websites – the number of compromised organizations continues to grow.

Cyber – A Growing Threat

In 2012, during a speech at the Intrepid Sea, Air, and Space Museum in New York, then Defense Secretary Leon E. Panetta warned of a "cyber Pearl Harbor that would cause physical destruction and the loss of life, an attack that would paralyze and shock the nation and create a profound new sense of vulnerability." He was referring to simultaneous cyberattacks coupled with physical attacks on the nation's critical infrastructure and military that could devastate U.S. operations. Once thought of only as a compelling story for movies or television shows, the U.S. government, corporate leaders, and the public at large are recognizing the real-world implications.

Warning: A cyber Pearl Harbor would cause massive destruction and loss of life, would paralyze and shock the nation, and would create a new sense of vulnerability.

Cisco Inc., a multinational corporation headquartered in San Jose, Calif., noted in its 2014 Annual Security Report the continuing growth in cyberattacks against the infrastructure of the Internet itself – including data centers, web-hosting servers, name servers, and large Internet-supporting corporations. Cisco's monitoring of suspicious traffic from some of the largest multinational organizations shows evidence of ongoing internal compromise, meaning that network penetrations have gone undetected over long periods. The report noted the evolving cyberthreat in 2014, "Simple attacks that caused containable damage have given way to modern cybercrime operations that are sophisticated, well-funded, and capable of causing major disruption to organizations."

After attacks on the electronic industry, the next four highest "industry vertical" malware attacks occurred in the agriculture and mining, pharmaceutical, energy (including oil and gas), and aviation industries, demonstrating that attacks are originating from an organized and mature cybercriminal network. Chief Security Officer John N. Stewart noted in Cisco's report that all organizations need to improve cybersecurity using tools that include, "verification through certified products, integrated development processes, [and] innovative technology," while making it a priority to, "verify the trustworthiness of the technology products they use and the vendors that supply them."

Of course, the ability for organizations to implement these strategies is wholly dependent on human resources with the talent and training to do so. Unfortunately, Cisco noted in its report that, "The sophistication of the technology and tactics used by online criminals, and their nonstop attempts to breach network security and steal data, have outstripped the ability of IT [information technology] and security professionals to address threats." More troubling is Cisco's estimate that there is a shortage of approximately one million security professionals with up-to-date skills in computer science, adding that, "Most organizations do not have the people or the systems to monitor their networks consistently and to determine how they are being infiltrated."

The University-Government-Private Sector Connection

This growing threat highlights the critical need to create the security workforce of the future, both in terms of skill and in the sheer numbers of professionals available

to support government and industry. Universities are paying attention to this need; corporate and government agencies are even enlisting universities to improve the knowledge, skills, and abilities in cybersecurity to the next generation of graduates.

The University of Maryland's Cybersecurity Center (MC2) is one of many new university-based organizations building programs in partnership with government and industry to develop the future cybersecurity workforce through undergraduate and graduate programs, including a masters program that offers mostly evening classes designed for practitioners. Director Jonathan Katz stated in a phone interview on 7 February 2014 that the focus today is, primarily, on research that can be used to develop future standards. However, he recognizes the ultimate need is for "mandatory standards" with "consequences for breaches," adding that, although Target's reputation may suffer from the loss of client data, they may not have any actual legal exposure under current federal law.

Carnegie Mellon University's Cylab in Pennsylvania is another successful partnership between higher education, commercial, and government organizations working collaboratively to close the "talent gap," while at the same time increasing awareness and understanding of current and future cyberthreats among students and practitioners. The National Security Agency (NSA) has recognized Cylab as a Center of Academic Excellence in Cyber Operations, thus helping to protect the nation's infrastructure through the development of cybersecurity professionals.

A PBS NewsHour story released on 19 January 2014 highlighted Cylab's partnership with NSA, including NSA's engagement of Cylab students to develop a computer game to help teach high school students develop hacking skills, and thereby getting even younger students interested in cyberprotection. In October 2013, Cylab joined an alliance between the Army Research Laboratory, Penn State, the University of California (Davis and Riverside), and the University of Illinois to increase cyberthreat detection, manage risk, and achieve the maximum cyberprotection benefits at the lowest possible cost. Although one aspect of the multiyear effort is to support the development of future system capabilities that can automatically respond to

attacks, human intervention and decision-making will always be required.

In addition to university-based programs, other continuing education organizations also are putting cybertraining at the forefront of their offerings in order to meet the need for cyberindustry talent. The SANS Institute has been offering computer security for more than 10 years, including online and classroom trainings on topics including hacker techniques and incident handling to classes focused on students acquiring Global Information Assurance Certifications (GIAC) – for example, GIAC Security Essentials Certification (GSEC). Other professional training organizations, such as the ITT Technical Institute, offer formal degrees and individual training events in cybersecurity and information security. These organizations recognize the training opportunity that the cyber "talent gap" represents.

Legislation & Personal Motivation

On 30 January 2014, U.S. Senators Dianne Feinstein (D-Calif.), John Rockefeller (D-W.Va.), Mark Pryor (D-Ark.), and Bill Nelson (D-Fla.) introduced the Data Security and Breach Notification Act (similar to legislation introduced in prior years), which: establishes security standards for corporate databases where confidential information is stored; requires strict consumer notifications following breaches; imposes civil penalties for violations of the law; and imposes criminal penalties for corporate personnel found to be deliberately concealing such breaches. On 4 February

2014, Assistant U.S. Attorney General Mythili Raman testified in support of the legislation and similar proposals previously recommended by the Obama administration to strengthen the existing Computer Fraud and Abuse Act.

Separately, in the U.S. House of Representatives, a bipartisan group of members has been working on a new Cybersecurity and Critical Infrastructure Protection Act (HR3696) designed to consolidate and strengthen civilian cybersecurity authorities within the Department of Homeland Security and rename the National Protection and Programs Directorate to the "Cybersecurity and Infrastructure Protection Directorate."

On 12 February 2014, the Obama Administration through the National Institute of Standards and Technology (NIST) released a new voluntary Framework for Improving Critical Infrastructure Cybersecurity, designed to strengthen the security and resilience of critical infrastructure through an expanded cooperation between government and the private sector. The Framework incorporates a risk management approach and provides examples on how organizations can implement strategies to identify and work to mitigate cyber threats. The Framework, based on a year-long collaboration between the White House and industry representatives, also seeks to establish a common vocabulary for cybersecurity risks, which should be helpful to the education community when developing new cyber curriculums.

The recent high-profile data breaches at Target and Neiman Marcus may provide sufficient incentive for Congress and the Administration to secure passage to one or both pieces of legislation. All that will be needed is the human capital to implement it. Fortunately, the class bells are ringing for students young and old who are interested in learning more about cyber.

Rodrigo (Roddy) Moscoso currently serves as executive director of the Capital Wireless Information Net (CapWIN) Program at the University of Maryland, which provides software and mission-critical data access services to first responders in and across dozens of jurisdictions, disciplines, and levels of government. Formerly with IBM Business Consulting Services, he has more than 20 years of experience supporting large-scale implementation projects for information technology, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.

Information Systems – Advancing Capabilities & Increasing Risks

By Craig DeAtley, Health Systems

Healthcare facilities across the United States are increasingly using various information technologies (IT) and information systems (IS) to conduct everything from recording patient care activities and tracking inventory to managing fiscal affairs. Information sharing system designs have grown increasingly sophisticated and have become intrinsic to decision making by healthcare facility administrators. Firewalls and other security techniques also are growing in complexity to prevent information thieves from gaining access to data that, if compromised, can lead to financial disaster and embarrassment for both the patients and the facilities.

Information Technologies/ Information Systems Usage

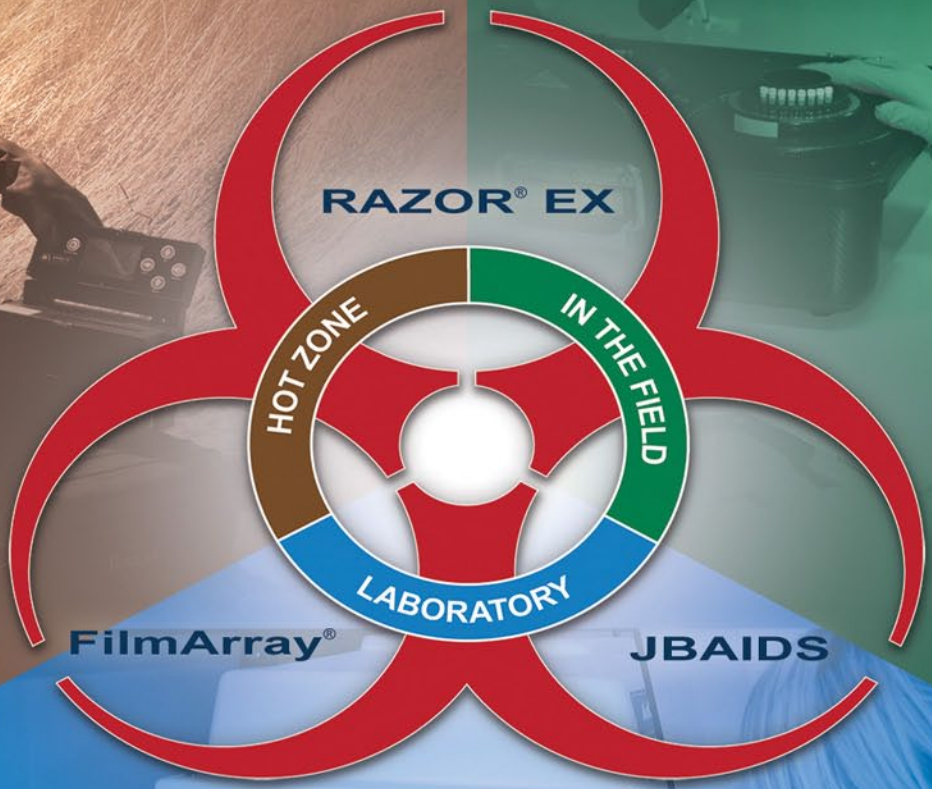
Healthcare facilities are routinely implementing new and better ways to use desktop, mobile, and handheld computers along with their embedded software. Technology use in the hospital setting typically begins with the registration of patients using the traditional desktop computer with predetermined screens of questions, or a computer on wheels with similar software. The patient's electronic medical record grows with each visit to the facility or an affiliated outpatient office. With funding assistance from the federal government, more physician offices are now using electronic medical record systems. As a result, communities increasingly, albeit slowly, are linking information between multiple clinicians and hospitals.

Hospitals, skilled-nursing facilities, and clinics currently use various electronic medical record technologies for their clinicians to record vital signs and medical assessments as well as ordering and sharing laboratory and radiology test results. Increasingly, these facilities also are using hand-held scanning technology to record patient medication administration and medical equipment and supply usage; some software even tracks the location of key equipment to ensure immediate access and enhance security against theft.

BioSurveillance

Flexible, Accurate, Proven Ready

BioFire Diagnostics delivers a fully integrated suite of Biological Agent Identification Systems. Since 1998 we have fielded BioSurveillance products that span the range of operations from the lab to the field, clinical diagnostics to environmental surveillance.



Idaho Technology is now

BIOFIRE DIAGNOSTICS, INC.

Discover the system for your mission.

WWW.BIO-SURVEILLANCE.COM

Bedside use of technology not only helps to better ensure patient safety but also improves inventory management and proper recording of patient charges. Materiel management personnel and their pharmacy colleagues use software programs to manage their inventories and automatically submit replacement orders with their vendors, helping to ensure more timely and accurate ordering of needed items. Similarly, persons responsible for managing a facility's fiscal affairs use software programs to track expenses and reimbursements, and often transmit this data via the intranet to their billers and insurance companies and, when appropriate, to their corporate headquarters.

Growing Risks & Consequences

Although IT/IS programs can help improve a healthcare facility's operations, patient safety, and efficiency, there are risks associated with the growing dependency on this practice – for example, when the IT/IS is temporarily inaccessible. Staff members at each facility that uses IT/IS know the importance of having backup plans in place in case a single program fails to operate or multiple integrated programs fail all at once. A multidisciplinary committee usually develops these "downtime" procedures because the failure of one or more programs could have different consequences for a clinician versus a non-clinician. Trying to determine all of the implications of an outage can take time; even the best plans may require a revision after an unplanned outage highlights a problem that the facility must address.

Complex healthcare information systems are vulnerable to attack when persons outside the system have newer equipment, better ideas, and different business intents.

To maintain an IT/IS, knowledgeable staff members must be available 24/7 to address technology and software failures that can occur at any time. Full-time or part-time staff may meet this need; alternatively, some facilities may use contractors in addition to or in lieu of permanent staff. Because technology and software are always changing, trying to keep up with the modifications is challenging – for example, an update made in one program can disrupt the delicate integration it may share with another program. Updating these systems also can be expensive; therefore, healthcare facilities that already operate on budgets with thin profit margins may need to postpone necessary upgrades.

Although the federal government has tried to promote the use of electronic medical records through guidance documents and financial incentives, many clinicians – especially those in private practice – are finding significant challenges to implementation. Higher operating costs and operational inefficiencies are among the primary complaints voiced by the clinical practices that have completed the transition from paper to technology.

Finally, despite a healthcare facility employing a knowledgeable IT/IS staff member and employing numerous sophisticated security measures, the ability of hackers to "break in" and steal financial or personal information is of great concern and occurs with increasing regularity. These thefts put a healthcare facility at risk for expensive litigation and other public-relations consequences that can produce equal if not greater harm.

Information technology and the accompanying information systems have become an integral part of a healthcare facility's operation on several fronts. Newer versions with better ideas for improving operating efficiencies and bottom lines become available on a daily basis. Also growing are the costs of keeping up with change and operating increasingly complex systems, which are vulnerable to persons with newer equipment, better ideas, and different business intents.

Craig DeAtley, PA-C, is director of the Institute for Public Health Emergency Readiness at the Washington Hospital Center, the National Capital Region's largest hospital; he also is the emergency manager for the National Rehabilitation Hospital, administrator for the District of Columbia Emergency Health Care Coalition, and co-executive director of the Center for HICS (Hospital Incident Command System) Education and Training. He previously served, for 28 years, as an associate professor of emergency medicine at The George Washington University, and now works as an emergency department physician assistant for Best Practices, a large physician group that staffs emergency departments in Northern Virginia. In addition, he has been both a volunteer paramedic with the Fairfax County (Va.) Fire and Rescue Department and a member of the department's Urban Search and Rescue Team. He also has served, since 1991, as the assistant medical director for the Fairfax County Police Department.

Bridging the Medical Ladders

By Joseph Cahill, EMS

The emergency response community should adopt a holistic approach for meeting challenges as a team. For community hospitals, this may mean changes in how they provide emergency medical services (EMS) to surrounding areas and how they hire and train staff. Although many agencies have promotional ladders built into their structures, many medical positions have licensing requirements that create ceilings for advancement. As a result, a staff member who reaches one of these ceilings must start his or her training over in order to advance. For example, an emergency medical technician (EMT) can advance to intermediate EMT, paramedic, supervising paramedic, or EMS educator. However, an EMT cannot apply his or her training and experience to other – better paid and, often more importantly, less physically strenuous – positions such as "physician assistant" (PA).

Retaining Valuable Resources

In addition to the EMT ladder, nurses at the same facility climb another ladder: a certified nursing assistant can progress through licensed practical nurse, registered nurse, and ultimately to nurse practitioner. Without the ability to advance, staff members may leave the employer altogether. However, changes in training programs and planning efforts can help build on the skills and knowledge in which hospitals and communities have already invested.

At the agency level, programs could assist staff in climbing the ladder from the entry level to the highest level of employment – either by paying paramedics to go to PA school, or providing support such as scheduling accommodations. In return, the employee continues to work for that agency with a new title in the available open positions. All training programs must serve the needs of the students and prepare them for the jobs they are training for, but they also should consider the whole picture when planning program structures.

Alignment, Scheduling & Training

The information learned in an EMT program continues to build as the EMT moves through future EMT intermediate or paramedic programs. A bridge from paramedic to PA would require: (a) coursework alignment; (b) flexible scheduling; and (c) added training.

The first step is for training facilities to assess the required accredited coursework for EMT, EMT intermediate, and paramedic degree programs to determine how they align with the prerequisites and course work for the PA programs. Next, PA programs must be more flexible in their scheduling. Currently, the majority of PA programs are cadre based – that is, a group of students start together, take classes full time, and finish together. Unfortunately, a paramedic working full time would have difficulty meeting this requirement. A part-time program, though, could provide more flexibility in scheduling and allow the paramedic to apply credits gained from their past training to the PA program.

Alternatively, hospitals and training facilities could develop a new program above paramedic that would offer training, licensing, and employment as an intermediate step between paramedic and PA. There have been many discussions about a "community paramedic" program, which would include performing primary-care functions within the community. Hospitals then could define additional roles.

Being a paramedic, a leader in EMS, and/or an educator of the next generation of EMS is an admirable goal, but the job is physically demanding – for example, a two-paramedic team must be able to carry 75 pounds of gear plus the patient to the ambulance. Although many EMS providers retire after full careers in EMS, many also suffer disabling injuries or less dramatic but equally career-ending degenerative damage to their joints. With limited supervisor or educator opportunities, it is important to foster other opportunities to keep these experienced professionals working – not only for their own good, but also for the good of the entire community.

Joseph Cahill is the Director of Medicolegal Investigations for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Before that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's paramedic program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

Virginia – Using Social Media the Right Way

By Tanya Ferraro, State Homeland News

Compared to past generations, the public today is receiving information in more ways, and at greater speeds, than ever before. With shifts in technology and the massive uprising of social media, the need to engage the public through innovative and interesting means continues to grow. Social media platforms offer useful solutions for sharing information with community members during disaster incidents as well as for general preparedness.

Social Media & Emergency Management

There are three key benefits for the emergency management professional to use social media effectively before a disaster. First, it humanizes the local emergency management office. Second, it connects important principles to community members who may rarely think of their own personal preparedness. Third, and the ultimate goal of this connection, it can influence the actual preparedness of their community members, which vastly changes the scope of response and mitigation.

Parodies of popular songs are just one way that emergency management agencies can deliver important preparedness messages that community members want to hear and can easily remember.

Social media platforms work well to deliver such messages because social media networks make the information easy to share, are interactive, and offer limitless boundaries for creativity. When an incident or event affects the community, many people share that message. This wealth of information is especially opportunistic for emergency management. With the uprising of zombies, sharknadoes, and many end-of-the-world movies, discussions about disasters have proved to captivate the public. Yet, many people ponder the "end of the world" – or at least the next small or large disaster – without directions on how to properly plan for it.

Creating a song, video, picture, or game that makes the public want to know more about preparedness costs little more than the time invested in creating it. In addition, an agency with a personality sharing friendly suggestions is likely to be far more influential than a formal promotional advertisement with a link. Using social media to build trust fosters the loyalty of community members.

In addition, an interactive agency – with professionals who truly enjoy what they are doing and care about what they are saying – becomes the public's subject matter expert should questions ever arise. Social media tips that come from a credible agency result in greater compliance, thus creating a cycle that can change the preparedness culture of a community over time. Although social media assets have a minimal cost, the return on the investment of time has exponential potential.

Matching the Message With the Platform

Emergency management agencies can use numerous platforms to connect with community members. With relatively user-friendly interfaces, these platforms are already in use by people seeking information. Flash mobs, songs, and other visual recordings of varying lengths are easy to share with platforms like YouTube. Other applications like Vine and Instagram record brief 6- and 15-second video clips, respectively, which force users to state their point quickly, yet with personality.

Facebook and Twitter are good platforms for hosting conversations and responding to community questions, as well as for sharing important emergency updates and news. Applications like Tumblr often host pictures and memes – for example, popular photos with satire written on them. These are just some of the many popular social media platforms available for sharing information and connecting with community members.

When designing messages and using social media platforms, emergency managers must consider the audience they would like to target with each message. This may mean letting go of the idea that seriousness is equivalent to professionalism, or that emergency management is not fun. Scare tactics are often ineffective and "boring" information is inadequate for memory retention. Bullet points, creativity, catchy sayings, and memes grab the public's attention. These brief, easy-to-remember messages are changing the culture of preparedness.

Loyals – A Royal Preparedness Example

The "Loyals – A Royal Preparedness Duet" video was a preparedness message that a group of Virginia emergency management professionals released on 26 November 2013. The parody of the popular song "Royals" by Lorde was the result of approximately two hours of planning, recording, and uploading. Within two months, though, the video had more than 7,000 views from 36 countries on YouTube, not including the many views on agency websites that directly embedded the video.

The largest target demographic for the video included men and women, ages 35-64, who viewed the video on mobile devices and referenced it from third-party sites. By initially sharing the parody through social media – Twitter, Facebook, and LinkedIn – the video gained popularity through "shares" via each of these sites. Local news and national print media also reported on the video as the power of this educational method fueled others to share it with their friends.

Broader Applications

It is not enough to know social media are necessary and useful. Gathering the talents in and around an organization who already are social media savvy has much to offer when designing creative messages. Choosing proper platforms, drafting a social media policy, and obtaining any necessary authorization to disseminate public messaging also are important. Professional communities already exist on platforms like LinkedIn, Twitter, Facebook, and Reddit, to name a few, that talk and regularly share resources regarding the use of social media in emergency management. Every Friday at 12:30 EST, for example,

#smemchat takes place on Twitter where professionals from across the country discuss popular topics in social media and disasters. There are countless blogs, websites, and professional social groups networked directly around creative engagement in emergency management as well.

After harnessing the power of social media, emergency managers can use that power to engage community members in ways that were not possible even a decade ago. Although changes in social media use have been uncertain in the emergency management field, the need to include social media in planning efforts is obvious. Social media trends are transitioning from informing the public during disasters to connecting directly with people to prepare the community before an incident occurs. By stepping outside current comfort zones, the emergency management field has a greater chance of directly influencing personal and community preparedness.

Tanya Ferraro is the Medical Reserve Corps coordinator for the Roanoke/Alleghany and Central Virginia health districts. She serves on the staff of the Regional Healthcare Coordination Center for the Near Southwest Preparedness Alliance, a regional healthcare coalition. She also is the co-host of the biweekly podcast EMtalk. With experience in volunteer management, incident command, public information, and the use of social media in disaster, she has worked in emergency management since 2007. She studied public safety, emergency management, and homeland security at Bluefield College and is a certified hospital emergency coordinator. Connect with her at about.me/tjlasagna.

Exercise Extent-of-Play Agreements

By Ken Lerner & George Yantosik, Exercises

Preparedness for large-scale disasters involves the ability of many organizations – local, regional, national, and sometimes international – to coordinate actions. Large-scale exercises can serve a useful function in practicing this coordination, identifying organizational disconnects, and promoting a shared sense of community among response organizations. However, emergency response exercises involving multiple organizations are challenging to plan and conduct because of organizations' priorities, agendas, levels of capability, and resource constraints. Different organizations have varying levels of resources available to commit to an exercise, and may have conflicting goals in terms of what they would like to take away from the exercise.

For a successful exercise, it is necessary to find points of agreement among the participant organizations: scope of exercise, degree of participation by each organization, coordination of exercise activities, and evaluation process for lessons learned from the exercise. One U.S. emergency preparedness program addressed these difficulties through the mechanism of a formal, written agreement among the parties, referred to as an "extent-of-play agreement" (XPA).

The Chemical Stockpile Emergency Preparedness Program

The U.S. Army and the Federal Emergency Management Agency (FEMA) administer the Chemical Emergency Stockpile Emergency Preparedness Program (CSEPP). The "chemical stockpile" in CSEPP refers to the Army's stockpile of lethal chemical weapons, including nerve and blister agents. The U.S. Army Chemical Materials Activity reported in 2013 that, of the eight continental-U.S. facilities housing the stockpile in the 1980s, the stored weapons have been successfully destroyed – under Congressional mandate and international treaty obligation – at six. The two remaining facilities are near Pueblo, Colo. (Pueblo Chemical Depot), and Richmond, Ky. (Blue Grass Chemical Activity, located on Blue Grass Army Depot).

In the Department of Defense Authorization Act (1986, Public Law 99-145, U.S. Code Title 50, Sec. 1521), Congress mandated that the destruction process be conducted with, "maximum protection for the environment, the general public, and the personnel who are involved in the destruction of the lethal chemical agents and munitions." This led to the formation of a program to enhance emergency preparedness at the Army installations, where the weapons are stored, and in the surrounding civilian communities. With technical assistance from the Army and FEMA, the states, counties, and local communities near these Army installations have built impressive plans and capabilities for response. CSEPP has operated at a mature level for more than 20 years and has conducted well over a hundred full-scale exercises involving Army, federal, state, local, and private agencies and organizations. Each CSEPP exercise takes months of planning and involves hundreds of participants at the federal, state, and local level, plus dozens to hundreds of control and evaluation staff. The scale of CSEPP exercises makes exercise planning both complicated and essential.

Challenges to CSEPP Exercise Planning

Because of the scale and the interjurisdictional nature of CSEPP exercises, the level of commitment by each organization is an important variable. In the early years of CSEPP, some exercises fell short of expectations because exercise planning and scenario design occurred before confirming the participating organizations and their extent of participation. It was necessary to continually revise exercise plans and scenario details, sometimes until the day before the exercise, as participant organizations vacillated on the scope of their involvement. In some instances, despite repeated planning meetings, these differences were never resolved. Exercises were plagued by disconnects in player actions and suffered disruptions in the flow of interaction among participants. In addition, they were often heavy with simulations in lieu of actual demonstrations of capability.

When multiple organizations are involved, exercise planners need to know in advance the extent of play for each involved organization: what functions the organization will demonstrate and what resources (personnel, facilities, response assets) it will commit

to the exercise. These are important for planning because of: (a) interdependencies among organizations; and (b) planning for exercise control and evaluation.

Interdependencies between response organizations are an issue for any exercise – especially when multiple organizations operate a joint facility. For example, a Joint Information Center, where spokespersons from multiple organizations gather to provide information to the media, works best with participation by all key response organizations. Another example is demonstration of an evacuee shelter in a school. Operation of the shelter requires much more than the cooperation of the school district. A thorough demonstration of this function will include participation by: the local Red Cross chapter to register the evacuees and arrange for supplies; local law enforcement agencies to provide security; and emergency medical services to provide medical care. The absence of any one of these organizations from the exercise will affect the other organizations to some degree because of their inability to interact with the absent organization. Similarly, if an emergency operations center (EOC) in a core jurisdiction does not staff the exercise to demonstrate all functions, it will affect any other playing organization that would feed information to or take direction from that EOC.

Exercise control and evaluation also require a stable basis for planning. It is challenging to field a team of controllers and evaluators appropriate for the scope of an exercise when there are uncertainties about the level of play. A mismatch can mean some controllers and evaluators are not properly prepared for their assignments, some activities are not adequately covered, and/or some controllers and evaluators are not used to the best advantage.

Agreeing on the Extent of Play

CSEPP addresses the challenges described above by negotiating formal, detailed XPAs to define the commitment of each jurisdiction in advance. In an XPA, each participant organization outlines its commitments to demonstrate particular functions, facilities, and levels of play. Reaching the point of commitment may involve considerable negotiation. However, once completed and approved at the appropriate level, exercise planners can rely on those commitments in developing the exercise scenario and planning for exercise control and evaluation. CSEPP exercises began to reach their full potential only when they became standard practice to negotiate formal, definitive XPAs with all jurisdictions before commencement of detailed planning. Key elements of CSEPP XPAs and associated negotiations include: organizational objectives; exercise parameters and "ground rules"; executive approval; and advance planning.

1. *Organizational Objectives* – Organized by jurisdiction, CSEPP XPAs outline each jurisdiction's commitment to demonstrate certain broad functions or objectives. Within each function, the XPA includes specific tasks. For example, a jurisdiction may commit to demonstrating public warning, and agree to the following actions: (a) prepare warning messages to be broadcast to the public, including specific instructions; and (b) promptly activate systems to disseminate the messages – for example, radio broadcasts, sirens, text messaging – in a timely fashion. The XPA may go into considerable detail on demonstrating these tasks – for example, activating broadcast systems at the appropriate time, but only broadcasting a test message. The agreement also may address deliberate inaction – for example, in an actual emergency, dispatched vehicles will verbally warn people in remote areas, but not in the exercise.

The objectives and tasks used in CSEPP XPAs come from a standard set whose use is prescribed in CSEPP-specific guidance and is tailored specifically for CSEPP. For non-CSEPP exercises, exercise planners need to determine the desired objectives and levels of demonstration. In general, any set of emergency response functions may be used and the tasks tailored to fit the specific objectives of the exercise. One place to start would be the core capabilities and mission areas outlined in the U.S. Department and Homeland Security's (DHS) September 2011 National Preparedness Goal.

An XPA must include sufficient detail about the expected play by every organization so that exercise managers can design scenario inputs to meet expectations, and recruit and prepare controllers and evaluators. This means negotiations within and among jurisdictions are necessary to ensure a balance in time, space, activities, and numbers of participants so that each organization can fulfill its individual objectives as well as the overall objectives of the exercise.

2. *Exercise Parameters & "Ground Rules"* – The core of an XPA is the description of objectives and how exercise participants will demonstrate them. In addition, an XPA can be used to specify various exercise parameters including pre-exercise preparations, agreed simulations, exercise ground rules, evaluation standards, and the roles of controllers and evaluators. Examples include:

- Date and time frame for exercise;
- Participation in exercise design teams, pre-exercise training, and exercise planning activities – including responsibility for developing part of the scenario, delegation of a trusted agent, and deadlines for scenario components to be completed;
- Pre-positioning and set-up – to save time or minimize disruption of normal work, certain responders and other response resources might be pre-positioned before exercise start-up;
- Out-of-sequence demonstrations – for example, setting up a shelter after school hours to avoid interfering with the school day;
- Allowable corrections or "do-overs" – allowing evaluators to correct player errors on the spot, especially for technical functions such as how to operate a piece of monitoring equipment;
- Allowable simulations – for example, whether to activate, simulate, or discreetly test sirens and other public-warning systems;
- Demonstration of functions by talking through a procedure or demonstrating a sample of activities that would be performed (or equipment that would be used) in an actual response – for example, one personnel-decontamination station (rather than the several that would be required by the scenario);
- Evaluator access to particular areas;
- Saving and copying exercise records – the CSEPP general practice is to ensure that exercise-generated records such as emails and news releases are printed or copied specifically for evaluator use; and
- Rules and procedures for adjusting or terminating the exercise if necessary due to hazardous conditions or real-world, emergency response needs.

3. *Executive Approval* – An XPA must have the unqualified support of the appropriate authorities in each jurisdiction before using the XPA for exercise planning. Most likely, emergency managers will handle the details of drafting and negotiating participation levels and, at the appropriate point, elevate the XPA to the executive level for approval. All participants should be able to depend on the approved and signed document. Generally, each major participating agency should have an executive level approval. For example, if a public health, law enforcement, or environmental agency will have a significant role in the exercise (along with the emergency management agency) an executive of that agency should sign the XPA.

4. *Advance Planning* – XPAs should be completed well before the planned exercise. Current CSEPP guidance calls for confirmation of exercise dates at least one year in advance, and for negotiations on the XPAs of participating jurisdictions to begin 310 days before the exercise date, be completed 270 days before the exercise date, and be signed no later than 150 days before the exercise date. This schedule ensures commitment to certain demonstration levels before exercise planners invest too much time in developing exercise inputs, logistics, and other planning details. The long period allowed for XPA negotiation reflects program experience and often proves to be worthwhile in the end.

The negotiation of the XPA does not merely serve those who are "running" the exercise; rather, every participant organization benefits. The added certainty means that each organization can be confident of a robust opportunity to test its capabilities.

Applications Beyond CSEPP

Pre-exercise agreements on the scope-of-exercise participation and demonstration of particular objectives have long been standard in the Radiological Emergency Preparedness (REP) Program administered by FEMA and the Nuclear Regulatory Commission for communities near nuclear power plants.

Like CSEPP, REP Program XPAs draw from a standard set of exercise objectives developed specifically for the REP Program, based on criteria in FEMA's REP Program Manual and a federal guidance document from U.S. Nuclear Regulatory Commission and FEMA,

NUREG-0654/FEMA-REP-1, Rev. 1. The REP Program objectives include items specific to radiological emergency response, such as radiological assessment and protective action decisions, dosimetry and exposure control for emergency workers, and administration of potassium iodide tablets, which protect against thyroid exposure. REP Program XPAs address methods of demonstration, which may include discussion, coordination between organizations, decision-making, and physical demonstration of field activities such as radiological monitoring and decontamination.

DHS's February 2007 Homeland Security Exercise and Evaluation Program guidance recommends the use of XPAs and a variety of exercises for various types of hazards also have adopted XPAs. Two recent examples are the Alaska Shield Exercise Series 2012 and the Evergreen Quake exercise series in the State of Washington. Based on a cold-weather scenario leading to infrastructure and heating problems, the Alaska Shield Exercise Series 2012 employed an XPA form to be signed by each jurisdiction or agency participating, which obligated the organization to designate a point of contact for exercise planning. Participating jurisdictions and agencies also were responsible for local aspects of exercise control and evaluation, described in the Alaska Shield Exercise Series 2012's scope-of-play agreement:

> Participating communities and agencies are responsible for local exercise design and coordination to include: local inject development, arranging for controllers and evaluators, coordinating exercise design with neighboring communities and agencies as needed, attending exercise planning meetings as required, and completing all required exercise documents (i.e., local exercise plan, local Master Scenario Events List and other documents as needed).

The Evergreen Quake exercise series included a functional exercise in June 2012 based on an earthquake scenario in the Seattle area. Participants included FEMA and 14 other federal agencies or departments, 11 State of Washington agencies, 6 Native American Tribes, 6 counties, and 23 municipalities. The XPA addressed the exercise date and time frame, listed the five overarching objectives, described the operation of the supervisory exercise design group ("Core Group") and the functional exercise design team, and assigned responsibility for local exercise design to the local communities (similar to the Alaska Shield XPA). It also requested each participating organization to use a limited-access website for coordination regarding the exercise event calendar, exercise templates, general instructions, and other exercise documents. Each participating community and agency was asked to develop, among other things, a local exercise plan and local Master Scenario Events List. The functional design team was tasked with the overall exercise planning, coordination, and reporting.

As with CSEPP exercises, a commitment to the exercise was required long in advance. The Evergreen Quake XPA set a deadline of 15 February 2011 for sign-up to participate in the June 2012 exercise. In a personal conversation on 11 February 2013, Brittany Ginn, exercise program manager at the Washington Military Department Emergency Management Division, reported that the Evergreen Quake XPA was very useful for organizing the exercise and highlighted the importance of pre-exercise commitments by participating agencies.

Investment & Dividends

Using formal XPAs to drive planning for any multijurisdiction exercise will pay dividends in the end. The time and effort expended on this process is a worthwhile investment. The larger the scope of the exercise and the more parties that are involved, the more valuable this tool will be. In general, exercises planned well in advance that involve multiple jurisdictions or organizations can likely benefit by the formalization and level of commitment that an XPA provides.

Ken Lerner (pictured) manages the National Response and Health Preparedness section of Argonne National Laboratory's Center for Integrated Emergency Preparedness. He has supported programs in emergency management, homeland security, critical infrastructure, and environmental compliance. He draws on 30 years of experience in exercise design and evaluation for radiological, chemical, and infectious disease hazards. Information on Argonne's Center for Integrated Emergency Preparedness is available at www.dis.anl.gov/groups/ciep.html.

George Yantosik is an emergency systems analyst at Argonne National Laboratory. Since 1995, he has assisted the U.S. Army and the Federal Emergency Management Agency (FEMA) with chemical stockpile emergency preparedness strategic planning, program management and evaluation, plans integration, research and development of technical policies and procedures, and training. Before joining Argonne, he held a number of positions within the Army Materiel Command (AMC) involving nuclear, chemical, and biological weapons and nuclear reactor logistics and operations for more than 30 years. As director of the AMC Surety Field Activity from 1988 through 1993, he was responsible for ensuring the safety, security, and reliability of Army nuclear and chemical weapons throughout the continental United States, as well as nuclear reactors operated by the AMC.

2014 Preparedness, Emergency Response and Recovery Consortium and Expo

PERRC

April 14 - 16 * Orlando, Florida

The latest in disaster preparedness, response and recovery all hazards training & continuing education for healthcare, medical, public health & volunteer emergency management personnel!

TOPICS INCLUDE

Evacuation Preparedness Modeling
Safe Food Handling in Disasters
Catastrophic Incident Search and Rescue: The CO Floods
Regional Mass Fatality Management Planning
Bomb Threat Readiness
Sheltering Operations
Volunteer & Donations Management
Continuity of Operations Plan
...AND MANY MORE!

*Panel discussions with some of the most knowledgeable **subject matter experts** in the country, **hands-on workshops**, in-depth lectures, and networking opportunities to **connect with peers & stakeholders** in the disaster preparedness, response and recovery community.*

Interested in EXHIBITING?
Networking events, meals, message boards and the internet cafe are located **ON THE SHOW FLOOR** to bring your company maximum exposure to all attendees! Develop new relationships with potential clients & increase your lead generation while providing awareness and access to your products!

Attendees use code **DOMPREP14** to receive $25 off & Exhibitors use code **EXPO14** to receive $50 off!

PERRC is sponsored by the Chesapeake Health Education Program, Inc.
Ph: 410-642-1857 or 843-285-8241
conferences@chepinc.org
www.chepinc.org

www.perrc.org