



DomPrep Journal

Subscribe

Volume 12, Issue 9, September 2016

CBRNE Threats

identiFINDER® R200

PAGER-SIZED, IDENTIFICATION-CAPABLE



NEW PRODUCT!

Meeting the mission: preventative radiological detection

FLIR identiFINDER® R200: Rugged and belt-wearable, this tool delivers immediate threat alarms and radioisotope identification to front-line responders during a radiological event.

www.flir.com/domprep



The World's **Sixth Sense**®

Business Office

P.O. Box 810
Severna Park, MD 21146 USA
www.DomesticPreparedness.com
(410) 518-6900

Staff

Martin Masiuk
Founder & Publisher
mmasuk@domprep.com

Catherine Feinman
Editor-in-Chief
cfeinman@domprep.com

Kerri Kline
Project Manager
kkline@domprep.com

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

4th Annual EOD/IED & Countermine
Symposium

64th Annual IAEM Conference &
EMEX

American Military University

BioFire Defense

Critical Infrastructure Protection &
Resilience Asia

FLIR Systems Inc.

PROENGIN Inc.

© Copyright 2016, by IMR Group Inc.; reproduction
of any part of this publication without express
written permission is strictly prohibited.

DomPrep Journal is electronically delivered by
the IMR Group Inc., P.O. Box 810, 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previously unpublished, and not simultaneously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.



Featured in This Issue

Addressing Threats – From Concept to Field
By Catherine L. Feinman5

The Danger of Not Keeping Up With Technological Advances
By Melissa Moses11

Technology for Improved Public Health Preparedness &
Response
By Greg Burel16

Hazard Detection: “Bring Your Own Protection”
By Kathryn Laskey20

A Conversation That Should Have Happened
By William H. Austin22

Major Themes From the 2016 Aspen Security Forum
By Erik Gaull25

About the Cover: The ever-changing chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) threat environment requires special attention on detection technology and personal protective equipment. Protecting those who protect others from existing and emerging CBRNE threats needs to be at the top of an agency’s priority list. (Source: ©iStockphoto/Amacistock)

Our commitment to **BioDefense**
has allowed us to be ready
for the **Ebola outbreak**
in West Africa.

Now, with the **FilmArray system**
and our reliable **BioThreat Panel**,
we are able to test for 16
of the worlds deadly
biothreat pathogens
all in an hour.

Now That's Innovation!



Learn more at www.BioFireDefense.com



Addressing Threats – From Concept to Field

By Catherine L. Feinman

To address various national threats and the U.S. Department of Defense's (DOD) role in military and civilian defense technology, DomPrep hosted a roundtable discussion on 21 July 2016 at the Edgewood Chemical Biological Center (ECBC). That discussion, which was moderated by ECBC's BioScience Division Chief Peter Emanuel, brought together professionals from various disciplines and is summarized in this article.



Located in Aberdeen, Maryland, the U.S. Army Research Development and Engineering Command Headquarters houses 76 tenants, with the Edgewood Chemical Biological Center ([ECBC](#)) being the third largest tenant, employing approximately 1,500 people. As a civilian-run research, development, and engineering center, ECBC is a critical resource for research and development of technologies related to chemical and biological weapon defense and strives to solve problems and reduce lead times of equipment from concept to the field.

Technology Development

Responses to chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) incidents require equipping response personnel with the most effective equipment and technology available to protect their lives and safety. However, developing that equipment can be a challenge. “It’s not the science that kills us, it’s usually the contracts, policies, rules, or other things that you don’t expect that makes the process that much harder,” said Emanuel. Advance technology development (ATD) is one way to cut the delivery from survey to soldier/responder by one-third. From the government perspective, specific problems need material solutions, so there needs to be an analysis of alternatives (what already exists and is working).

ECBC is a chemical-biological solutions center and has served as a test bed for market surveys, laboratory testing, field testing, technology development, and so on. To better serve first responders, warfighters, combat health support systems, homeland security personnel, as well as military and civilian research laboratories, ECBC created a book entitled “Global CBRN Detector Market Survey” to enable users to better compare available technologies. That book contained over 400 technologies based on the following four scenarios to create product data sheets: man portable and field use; mobile laboratory/field laboratory; diagnostic laboratory or point of care use; and high-sensitivity, high-throughput analytical. With frequently changing technologies, though, that printed book was later converted to a freely accessible [website](#) resource in order to expand it and keep it up to date. The goal is to educate communities while remaining unbiased.

Emanuel warned that waiting until a technology is perfect could leave communities more vulnerable, “Stop making ‘perfect’ the enemy of the good.” In order to find a viable solution, all stakeholders need to be involved in the design process to ensure that all expectations and needs are addressed. There are different perceptions from local, state, and federal field responders. So, without presumptive diagnostics, the pressure falls on these responders to balance response actions with public expectations.

According to Emanuel, the DOD has 30-year plans for technology, but that is not always the case at the local level. ECBC's efforts ensure that the lessons learned across the organization are shared. To meet the technological requirements of agencies and organizations, a combination of bottom up and top down approaches are needed. BioDefense Branch Chief Nicole Rosenzweig agreed, "There are things you can change and things you cannot change. We have to figure out ways to address the pieces that we can, so we can do a better job with the pieces that we can't."

Deploying the same technologies and capabilities at all levels is neither practical nor affordable. Emanuel questioned why there is not a greater civilian effort to position affordable and sustainable technology in smaller jurisdictions versus putting specialized equipment in every police vehicle that may not be as accurate or reliable (with higher false positives). Responders need to have technology that they can use to defend their decisions after a response. Although the DOD has an understanding of "acceptable loss," Anthony Mangeri, director of strategic relations for fire services and emergency management and faculty member of the American Public University System, pointed out that, "in the civilian world, there is a very low tolerance for any losses," especially under the microscopes of modern media and public perception.

These perceptions become even more pressing when public health issues are involved. However, Emanuel warned that a public health overlay for a clinical environment does not mesh evenly with the operational field paradigm, leaving a low or no tolerance for mistakes. However, in the operational world, he said, "the job is not to avoid risk but to manage it." Such timelines and willingness to accept a tiered elevation of confidence has been at the center of tension between the military and the domestic homeland defense culture. The learning process does not end, of course, but reducing any percentage of risk is a move in the right direction. To avoid being separated by expectations, federal developers need to work closer with the user community.

Measuring Technology Performance

As a bio-identifier test bed, ECBC acquires optimal detectors for a particular use, tests the equipment in the field, and then provides feedback valuable to the manufacturers. This dynamic interplay improves technology through cooperative research and development agreements, thus determining whether the equipment meets the expectations of the buyers and assertions of the manufacturers. In some cases, equipment may work perfectly in a laboratory environment, but not as well in real-life scenarios – confounders include: effects of atmosphere, moisture, user interface, and sensitivity.

During the testing process of 16 bio-identification devices, which cost about \$3 million, ECBC learned that interfacing with companies as well as equipment being geared toward the wrong enterprises are both gaps that need to be bridged. Since small industry cannot support the high cost of extensive testing as performed by ECBC, Emanuel suggested that the government provide an incubator site that could be shared throughout the technology industry as a possible solution. The military creates a more efficient use of its resources by incorporating them into dismounted reconnaissance sets, kits, and outfits ([DRSKOs](#)), but there are still disconnects. Large acquisitions like DRSKOs can be cumbersome and slow. However, by weeding out technologies at each step of the assessment, testing, and feedback process, the best technologies for their specified purposes can be identified.

Chemical Threats: A Test for Technology

Dr. Fred Berg, chemistry division chief of ECBC, briefed on chemical threats and how technology is used to detect them. Nerve agents like VX and GB (sarin) may be desirable by terrorists because of their toxicity and lethality per weight, with a rapid onset that receives more attention from the public and attribution for those deploying the agents. Although mustard is not designed to kill, such agents still pose a significant threat. In Syria, for example, 550 tons of methylphosphonyl difluoride (DF) and distilled mustard (HD, which is 100-percent pure) were reportedly destroyed, but the Islamic State Group is using a relatively simple procedure of mixing sulfur and chlorine to create mustard (H), which is 20- to 40-percent pure. Unfortunately, not all instruments are tuned for such impure creations. Chemical library datasets are optimized to pure forms for better results, but also include impure variations. Berg described the Next-Generation Chemical Detector ([NGCD](#)) that ECBC is currently working on to solve this problem.

ECBC is one of about 30 Office for the Prohibition of Chemical Weapons ([OPCW](#)) laboratories located around the world that analyzes agents. Twice a year, the OPCW conducts a “round robin” exercise to have specific agents tested by all the OPCW laboratories. The laboratory results are then graded to determine how well they were able to detect and identify specific agents. Detecting an agent that is not in the compound is an automatic failure, so it is critical that laboratories are able to accurately identify the ingredients of chemical compounds, while minimizing false negatives and eliminating false positives.

In the field, some scientific knowledge and a few thousand dollars are needed to create chemical weapons, but Berg noted that it only takes one person with such knowledge who could then train others. On the responder side, ensuring that the right people are trained to address these “home” laboratory threats is challenging. To address these threats, realistic training scenarios and coordination from the federal to local levels are needed. Other topics such as vaccination, crowd control, and quarantine need to be addressed as well, but can be controversial. In such cases, it is important to explain and weigh the good of the individual versus the good of the population – a concept that is more widely understandable and acceptable in the military than the civilian environment.

However, according to Melissa Moses, who is a senior analyst at SC&A Inc., even when exercises are conducted, involvement from all key stakeholders may decrease because of redundant or incomplete (not addressing the full range from left to right of “boom”) training, which is not effective for challenging people to keep their skills sharp. Understanding roles and bridging the gap between military and civilian response is also a challenge. She stated that there are sometimes uncertainties about when to notify authorities such as Civil Support Teams ([CSTs](#)) and gaps in local, state, and federal involvement (compartmentalization), which make response efforts less effective.

Biothreats: A Threat Like No Other

Dr. Calvin Chue, BioSciences Division deputy chief of ECBC, described how biological threats are different from other weapons of mass destruction threats. There are four types of biothreats, which change over time: traditional (naturally changing pathogens), enhanced (naturally or human-modifiable pathogens), emerging (new, but naturally occurring pathogens), and advanced (human-created pathogens). He explained how biothreats are the opposite of nuclear and chemical threats. In the case of chemical, nuclear, and other threats,

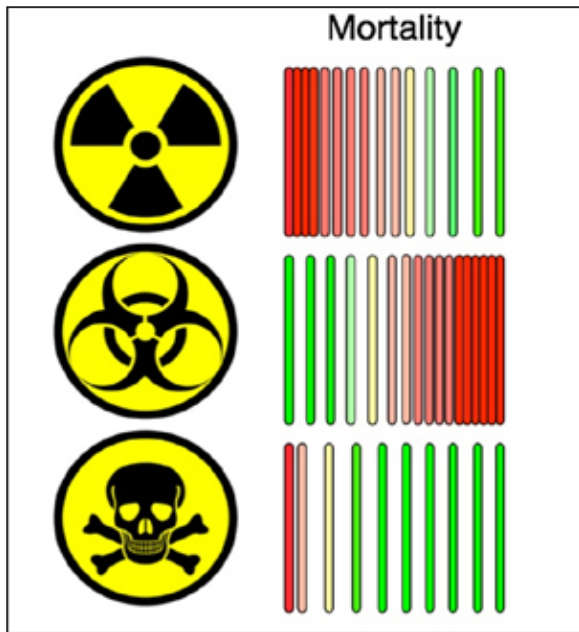


Fig. 1. Comparison of the long-term mortality rates resulting from a radiological, biological, or chemical attack. (Source: Dr. Calvin Chue, 2016)

hundreds to tens of thousands are affected in the early stages of the attack, with deaths and injuries decreasing over time. Conversely, bioattacks may not be visible initially, but the fatalities and injuries could exponentially increase over time – to as many as tens of millions after one year (see Figure 1). Such attacks could potentially be more devastating as they undermine society and create potential scenarios of public panic and marshal law.

The differences between detection, financial investment, and technical skills needed for biological versus chemical agents are significant as well. For less than \$1,000, Chue said that someone with limited technical skill could begin growing bacterial spores with equipment easily available on the internet – for example, fogging devices for dispersal of agents. Bioagents come from

nature and, because they are living, distribute themselves naturally. Even small pathogen quantities can amplify in a vulnerable population. As they do not exist in the natural environment, chemical and radiological dangers can be identified almost instantaneously. Since pathogens are found in the environment, biological detectors could take 15 minutes to several days to detect and identify specific agents higher than normal background. Further, biological detectors are highly specific and tuned for dangerous levels of pathogens, possibly reducing utility for operational personnel.

Biologicals also do not have to be lethal to pose significant problems such as lowering combat effectiveness. Even a specific DNA blueprint cannot determine whether an agent is pathogenic or benign. Unfortunately, Chue said that contagiousness versus deadliness is not emphasized enough, despite being a critical decision factor. Sampling knowledge and capability are essential. For example, response to a deliberate, contagious smallpox release should not be the same as for a noncontagious anthrax release.

The Future of CBRNE Threats

Perpetrators of bioattacks include: cults, terrorists, disgruntled insiders, independent researchers, bad state actors, as well as scientists who tinker and create agents they did not expect. As convergence with nature (pigs, birds, horses, bats, seals, and humans) increases, the threat also will increase. The good news is that it does not require sophisticated personal protective equipment to create a barrier to infection, but protection may not be used until it is too late. For example, at security checkpoints, a simple pat down could be the mechanism for human-to-human transfer.

Enhancement in biochemical research enables researchers to interfere with and create vulnerabilities in critical cell pathways to: manipulate genes, recreate polio, create synthetic botoxins, enhance physical features, or cross breed organisms. Although the vast majority of such scientific efforts are for beneficial use, a nefarious actor with advanced scientific

knowledge and facilities could target a bioagent to critical genes. Human genome sequencing once took years and cost millions of dollars, but now takes weeks and a few thousand dollars. Such rapid advancements herald an age of unprecedented medical technology, but the same tools can be used for evil. This is the classic “dual-use” conundrum that resulted in the formation of the National Science Advisory Board for Biosecurity in 2005.

As genetic databanks grow with ever-faster genome-sequencing ability, it raises questions about how that information will be used. The digital world made things faster, but at the same time more vulnerable. A new wave of genetic threats could be devastating, or “existence ending,” said Chue, and the researchers, “don’t have to be mad, just tinkering.” Despite all the above, highly contagious diseases like measles are Chue’s greatest concern because natural pathogen emergence and evolution are more likely and would affect far more people.

Developing technology and measuring its performance are essential for protecting emergency responders and the public when a CBRNE event occurs. ECBC provides valuable resources to help decision makers compare these technologies, make knowledgeable purchases, and equip responders in the field.

In This Issue

Melissa Moses leads this edition of the *DomPrep Journal* on “CBRNE Threats” with a warning for the intelligence community to remain current on rapidly developing technological advancements, which could have dual-use implications. Technology and equipment that once was only available in scientific and research environments may now be accessible on the internet.

Some technological advances increase levels of preparedness against CBRNE threats. For example, Greg Burel shares how government and public health agencies at all levels can leverage predictive technology resources provided by the Strategic National Stockpile to address potential failure points and build community resilience. Kathryn Laskey then describes an emerging affordable public safety smart system that could reduce deployment times during an emergency.

Rounding out the issue, two articles emphasize that knowledge is key for addressing the ever-changing threat environment: knowledge about federalism, politics, and disaster logistics described by William Austin; and knowledge about violent extremism, cybersecurity, and other international security issues addressed by Erik Gaull. Through discussion and research, preparedness professionals are better equipped to understand threats and vulnerabilities, develop actionable plans, and ultimately improve preparedness on the frontline.

Special thanks to the following writers, sponsors, panel participants, and ECBC staff who made this issue possible:

William Austin, Homeland Security Coordinator, Connecticut Capitol Region Council of Governments

Fred Berg, Chemistry Division Chief, ECBC

Greg Burel, Director of the Division of Strategic National Stockpile, Office of Public Health Preparedness and Response, Centers for Disease Control and Prevention

Sean Carey, Government Regional Sales Manager, Dräger

Julie Carrera, Section Manager & Principal Chemist, Chem/Bio Analysis Section, Argonne National Laboratory's Global Security Sciences Division

Calvin Chue, BioSciences Division Deputy Chief, ECBC

Barbara Dill, ECBC

Robert Dorsey, BioSensors Branch Chief, BioSciences Division, ECBC

Peter Emanuel, BioSciences Division Chief, ECBC

Erik Gaull, Director of Public Safety and Emergency Management Programs, Applied Research Associates Inc.

R. Ralston Hough IV, Research Intern, Homeland Security Studies and Analysis Institute, Department of Homeland Security, ANSER Inc.

Donald Kennedy Jr., Public Affairs and Communications Officer, ECBC

Kathryn Laskey, Professor of Systems Engineering & Associate Director, Center of Excellence in Command, Control Communications, Computing, Intelligence and Cyber (C4I & Cyber Center), George Mason University

Matt Lesho, Luminex Corp.

Anthony Mangeri, Director, Fire & Emergency SVS Strategic Relationships, American Military University, American Public University System

Melissa Moses, Senior Analyst, SC&A Inc.

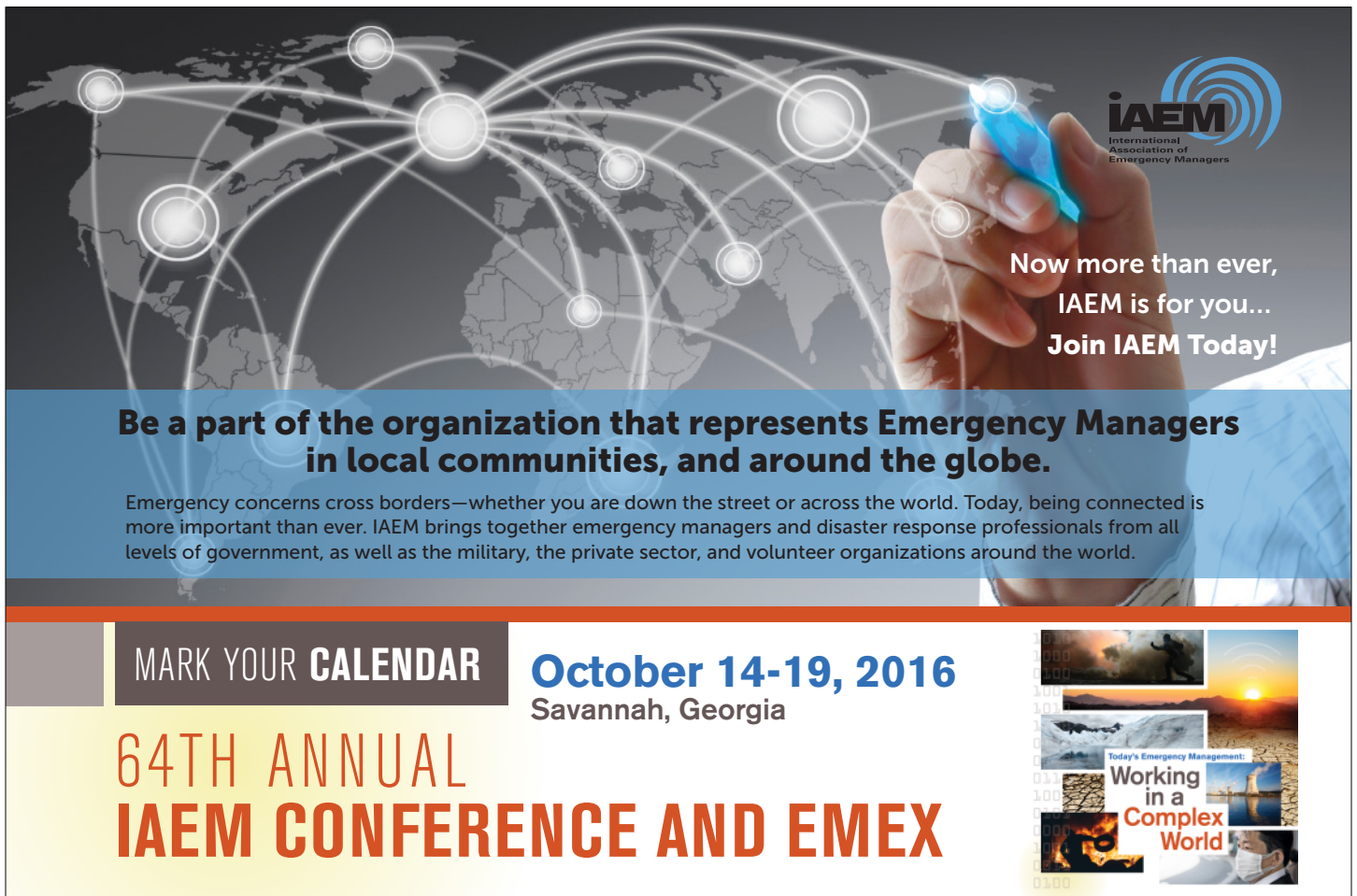
Aaron Poynton, Executive, Federal Resources Supply Company

Mark Reuther, Vice President & General Manager, PROENGIN Inc. North America

Nicole Rosenzweig, ECBC

Eric Schaffer, ECBC

Catherine Feinman joined Team DomPrep in January 2010. As the editor-in-chief, she works with subject matter experts, advisors, and other contributors to build and create relevant content. With more than 25 years of experience in publishing, she heads the DomPrep Advisory Committee to facilitate new and unique content for today's emergency preparedness and resilience professionals. She also holds various volunteer positions, including emergency medical technician, firefighter, and member of the Media Advisory Panel of EMP SIG (InfraGard National Members Alliance).



The banner features a background of a world map with glowing nodes and connecting lines, symbolizing global connectivity. A hand in the foreground holds a blue pen, pointing towards the map. The IAEM logo is in the top right corner. The text is arranged in several sections: a headline, a sub-headline, a paragraph, and a call to action. The bottom section contains event details and a collage of emergency-related images.

IAEM
International
Association of
Emergency Managers

Now more than ever,
IAEM is for you...
Join IAEM Today!

**Be a part of the organization that represents Emergency Managers
in local communities, and around the globe.**

Emergency concerns cross borders—whether you are down the street or across the world. Today, being connected is more important than ever. IAEM brings together emergency managers and disaster response professionals from all levels of government, as well as the military, the private sector, and volunteer organizations around the world.

MARK YOUR CALENDAR **October 14-19, 2016**
Savannah, Georgia

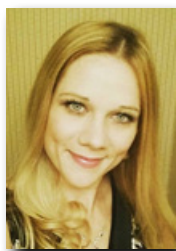
**64TH ANNUAL
IAEM CONFERENCE AND EMEX**

Today's Emergency Management:
**Working
in a
Complex
World**

The Danger of Not Keeping Up With Technological Advances

By Melissa Moses

The internet has revolutionized the way modern populations live their lives. From communication to commerce, the internet has changed the way people fundamentally operate. This extends to the life sciences as well. Technology and equipment once only found in research laboratories or universities can now be ordered online and shipped direct to the purchaser's doorstep.



Although there are benefits to be gained by opening the scientific world to the masses, there are also serious security concerns to which current treaties and protocols have not been able to address. Potential bioterrorists or states with biological ambitions can utilize online marketplaces to acquire the equipment, technology, genetic blueprints, and even the actual pathogens all while avoiding detection by export control regimes such as the Australia Group ([AG](#)).

Online Access to Deadly Threats

E-Markets such as Ebay or Alibaba pose an even greater challenge as the vendors sell directly to the customer and there is no third party involved. Some of the vendors on these websites are considered “[low-profile actors](#)” as they are often either individuals or small companies, which seek profits and may not ask pertinent questions regarding the sale of a particular piece of equipment. These low-profile actors are of particular concern due to the difficulty in tracing the financial transactions. Confounding factors include the minor amounts of money involved and a faster rate of completion of transactions. These [transactions are able to be completed](#):

- At a faster rate as a result of increased competition, ease of money transfers, and access to new international courier services;
- With greater potential for anonymizing financial transactions as low-profile actors are more likely to have a greater willingness and flexibility for the use of alternative, less secure methods of payment such as [Bitcoin](#) or [Dash](#); and
- With far greater access to vendors operating in countries with weak national export control laws.

The AG and the United Nations’ Biological and Toxin Weapons Convention ([BTWC](#)) – although only 30 and 40 years old, respectively – are rapidly becoming irrelevant in regards to biotechnology and the implications for bioterrorism. Technology associated with the life sciences, which can be purchased online and shipped all over the world, is developing rapidly and creating newer technologies not addressed by either entity. [Six of the newer technologies of concern](#) are: algae photobioreactors; freeze-dryer gas sterilization upgrade kits; hand-held aerosol generators; DNA kits; synthetic biology kits; and 3-D bioprinters.

Emerging Technologies

Although algae photobioreactors have a legitimate use in many industries, they can also be used to create pathogens or species of algae that produce toxins. Freeze-dryer gas sterilization upgrade kits can be used to retrofit freeze dryers – the [AG Biological List](#) lists only freeze-dryers employing steam sterilization. The upgrade kits claim to possess equivalent sterilization performance to that of a freeze dryer equipped with a traditional steam-sterilization system. This is an example of a loophole within the AG since the upgrade kit is not listed.

Hand-held aerosol generators are another example of a loophole within the AG because the AG only lists aerosol generators that can be easily fitted onto an airborne platform. The new

Threats may be just a click away! However, is the intelligence community keeping up with emerging technologies and biological threats?

handheld aerosol generators are capable of dispersing 1- to 10-micron-size particles and can fit inside a backpack or other nondiscrete carry case.

DNA kits and synthetic biology kits both reduce the technological barriers for genetic

engineering and are available online, relatively inexpensively. The [3-D bioprinters](#) can be used to print tissues on which to test compounds or agents and evaluate their effects. The printers can be used to accelerate the discovery of new compounds and improve toxicity models to predict the compounds or agents' effects on humans.

Emerging Biological Threats

The explosion in the popularity of synthetic biology, “do-it-yourself” biology, and biohacking are ushering in a new era of biological weapons. Although the biological threats of the past still pose real threats, the new age of bioterrorism presents even greater challenges as pathogens are genetically modified and engineered beyond what they were originally capable of. The JASON Group, a scientific advisory group that advises the U.S. government on sensitive scientific and technological issues, conducted a 1997 study (described in [Biotechnology: Genetically Engineered Pathogens](#) [The Counterproliferation Papers, Future Warfare Series No. 53]) predicting the future of biological threats. They generated six categories of biologically engineered pathogens that could pose a serious threat to society. The six categories of potential threats are binary biological weapons, designer genes, gene therapy as a weapon, host-swapping diseases, stealth viruses, and designer viruses.

A binary biological weapon is comprised of two segments, or parts, that individually can be handled safely. However, once combined, this weapon becomes lethal or increases in virulence. This type of research and development was undertaken by the Russians to create a more virulent and antibiotic-resistant form of plague. They were able to create a less virulent strain that was safer to handle and store. However, upon deployment, it was converted into a more lethal, antibiotic-resistant strain. Due to the intentionally benign nature of the two separate components, binary weapons can be easily and discretely transported, decreasing their signature footprint and making detecting and tracking more difficult.

The breakthrough in biotechnology and synthetic biology has made the creation of “designer genes” a reality. Utilizing gene splicing, genes can be inserted into another organism altering its original genetic properties. This can create organisms that are more virulent or are resistant to medical countermeasures. Given the ease in which genes and genomes can be acquired, this particular bioweapon could pose the greatest threat based on the ability to choose genes to combine and attributes to enhance. Although not done for nefarious purposes, researchers at the State University of New York at Stony Brook were able to download a genetic map of polio from the internet, purchase strands of DNA that corresponded to the polio virus, and artificially [synthesize a “live” polio virus](#). The virus that they created was able to paralyze and kill the mice injected with the synthesized virus.



Gene therapy is used to treat genetic diseases by identifying bad genes and replacing them with good genes as a means of restoring health and function to the afflicted individual. Scientists use vectors – commonly genetically modified viruses – to deliver these healthy genes in the body. Although gene therapy has had success in animal trials, it also highlighted how it could be hijacked for nefarious purposes. Researchers utilized gene therapy in an experiment while working with the [mousepox virus](#). Instead of the intended outcome, they inadvertently engineered a mousepox virus that was 100 percent lethal in unvaccinated mice and 60 percent lethal in mice that had been vaccinated. The genetically modified virus attacked the immune system of the mice and killed them. This has serious implications for the human smallpox virus as the same modification could create the same lethality rate in humans as was seen in the mice.

Host-swapping diseases are those that jump from a natural host to a new host where it mutates or picks up other genes. This is already seen in diseases such as bats with Ebola and rodents with hantavirus. Many of these diseases are classified by the Centers for Disease Control and Prevention as [Category A agents](#) and are known to be highly lethal to humans. “Do-it-yourself” biotechnology, dual-use equipment, and the fact that these pathogens can be found in nature can potentially make these pathogens easier for acquisition and manipulation.

Stealth & Designer Viruses

Two more futuristic and technologically challenging, albeit still possible, weapons are stealth and designer viruses. A stealth virus is similar to gene therapy as it uses a vector to enter and infect the body. However, instead of causing an immediate reaction in the body, it lies dormant until triggered by an internal or external stimulus. An example would be a virus that is engineered to cause apoptosis upon activation by a specific trigger such as a routine medication. A person could unknowingly set off the virus merely by taking his or her daily medication.

The designer gene concept starts by determining the desired result and builds a pathogen around the desired outcome. A designer gene differs from a designer virus in that it irrevocably alters a person's DNA. A designer virus is introduced via a vector and actions can be taken to mitigate the damage or, in some instances, to cure. To utilize a designer gene as a weapon, scientists would determine the symptoms or effects they want to induce and utilize synthetic biology and technology such as clustered regularly interspaced short palindromic repeats (CRISPR) to manipulate an organism's DNA to design a pathogen that would have that intended effect on the body. Advances in gene editing and sequencing have used CRISPR technology to more easily target and edit specific genes. Traditional gene sequencing was used on a limited number of animals such as mice and rats; however, CRISPR can be used on any organism to include humans. CRISPR is touted as the potential cure to genetic diseases via genetic engineering and the ability to modify abnormal genes, but it could also be used for much more nefarious purposes. Creating designer genes and viruses and stealth viruses would be more difficult, although not impossible, in the near future and would be much more difficult to detect.

One of the challenges facing the intelligence and law enforcement community with regard to the ability to collect, analyze, and accurately assess biological weapons programs conducted by states and/or terrorist groups is a fundamental lack of scientific understanding about these programs. Analysts are trained to detect anomalies or other indicators and warnings surrounding a particular threat. However, biological weapons programs are much more difficult to detect based on the nature of the programs, which are usually folded into legitimate research or are conducted on a smaller scale with a less noticeable footprint.

In August 2015, the University of Pittsburgh Medical Center for Health Security conducted [a survey](#) of 59 experts in the field of biosecurity. Of those surveyed, most believed that the intelligence agencies would be unlikely to provide actionable information or warnings prior to a biological attack. Of the 59 experts polled, 53 thought there would be a 50-percent or lower probability that such a warning would occur prior to an attack. Only a few participants felt that there had been improvements in the detection capabilities against biological weapons programs. Major hurdles identified in the survey were: "the difficulties inherent in detecting and tracking biological weapons capabilities due to: the intrinsic dual-use nature of biology; the ease of concealing preparations for a biological attack; limitations in expertise and investment in biological threats by the IC [intelligence community]; and past experiences of the challenges associated with intelligence collection against biological threats."

Much to the nation's detriment, the intelligence community – like most other entities designed to monitor and prevent biological weapons proliferation – is not keeping pace with rapidly developing technological advances.

Melissa Moses spent five years enlisted in the Air Force as an emergency manager and was part of the 141st CE CERF-P (Chemical, Biological, Radiological, Nuclear and high-yield Explosive [CBRNE] Enhanced Response Force Package) team. She received her B.S. and commissioned into the Marine Corps where she was stationed in Yuma, Arizona, as the intelligence officer for VMA-214 harrier squadron. She has deployed to Afghanistan, Kyrgyzstan, and Israel, and was onboard the USS ESSEX as part of the 31st MEU. She received her M.S. in biosecurity and disaster preparedness with a concentration in medical and public health intelligence from Saint Louis University. She also received graduate certificates in applied intelligence from Mercyhurst University and biosecurity/biodefense from University of Maryland, University College. She has spent over a decade pursuing her two passions – intelligence and biosecurity.

EMERGENCY MANAGEMENT & LEADERSHIP

UNDERGRADUATE AND GRADUATE CERTIFICATES

Developed in partnership with key professional training organizations,
American Military University offers public safety leaders:

- Support through scholarship programs
- Cohort class registration options
- Financial incentives available for select partnerships

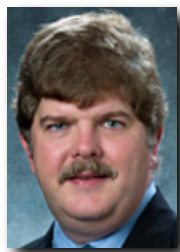
TAKE THE NEXT STEP TOWARD YOUR LEADERSHIP GOALS.
LEARN MORE TODAY AT PUBLICSAFETYATAMU.COM/DPJ



Technology for Improved Public Health Preparedness & Response

By Greg Burel

Planning the response to a public health emergency can be a daunting endeavor. Many factors in multiple complex systems contribute to the potential for success in executing these plans at every level of the response. Preparedness planners have to consider these many factors to ensure that their plans can work despite potential failure points.



Potential failure points exist all along the route of identifying, for example, a medication that can save life or reduce illness to the point that someone who needs it can take a pill. At the Centers for Disease Control and Prevention's Strategic National Stockpile (SNS), many of these failure points are addressed in the work that SNS and its federal, state, and local partners do to prepare for an emergency. SNS uses predictive technology and software tools to improve its capabilities around three main failure points: having the right medications available; distributing those medications across the nation to the specific communities in need; and, finally, dispensing those medications to individuals.

Health Security Within Complex Systems

CDC's SNS is a repository of large quantities of medicines, vaccines, and other critical medical supplies that can be rapidly mobilized to intervene in a life-threatening situation. The SNS is one part of a web of resources that must be successfully employed to respond to and recover from national public health emergencies. CDC has worked with state and local public health emergency planners for years to create plans to respond to various threat scenarios. If those plans fail to work when a threat becomes reality, they represent no gain in preparedness. To make sure the plans work, they must be tested and refined.

Success is not achieved in a vacuum. There are many actors in the complex system of responding to public health threats and emergencies. A threat to public health may be discovered when multiple people get sick and astute clinicians recognize their illness as an unusual case or cluster of cases. The first response community may identify a threat as it assists those who are suddenly and visibly affected by things like accidental release of harmful material or who are physically injured in an accidental or intentional disaster. Law enforcement personnel may see a threat or a need to assure persons who are affected by or responding to a disaster are protected.

When a threat that may have implications for national health security is identified, various computer models can be applied to identify potential numbers of people who need help. These numbers are based on scenarios used to drive computer projections of required interventions. Understanding these factors, SNS can begin to apply other models to decide

what the cost will be to hold various material to affect positive interventions. This leads to many of the tradeoff decisions that must be made in order to protect the most people for the highest likely threat scenarios while providing a good return on investment and value to the public.

Resource Positioning & Distribution

As material is identified and incorporated into the SNS, SNS personnel must ensure that the material can actually be used in a clinically relevant time, place, and method to return the desired positive

outcomes. The first step in this process is to position the material throughout the storage network to enable rapid delivery to any location in the United States. Once material is placed in storage, SNS projects timelines to move the material to the locations where it might be needed and regularly updates its projections for delivery.



It is commonly understood in the emergency management community that preparedness plans must be exercised regularly to identify and correct gaps and ensure that actors in a response system know and can accomplish their roles effectively. A well-planned exercise that involves the public, who may someday be at risk, can inform and educate all levels of the nation in what to expect and how to act in the event of an emergency. The fact is that, if plan improvements are made without testing them to ensure they work, gaps will continue to exist. Although exercises on a large scale need to be conducted routinely to test and evaluate public health emergency response plans, doing so can be costly. In addition, repeating these drills and exercises to test variables and proposed alternatives is prohibitive to even the best-funded jurisdictions. Fortunately, there are alternatives that can more efficiently identify gaps and help refine plans.

Complex systems, such as those SNS relies on to quickly and efficiently deliver a countermeasure to an area of need during a response, are inherently difficult to test and evaluate. The high number of inter-relationships in multiple systems during an event can be quickly overwhelming. The cost to actively conduct tests with large numbers of participants and other resources can be daunting. This is especially true considering the limited funds that are available to pilot and evaluate proposed new response strategies to possible events or scenarios. The answers to many of these questions lie in application of technology to public health interventions. SNS has invested in tools that specifically help its state and local partners better prepare to respond in their jurisdictions, while easing possible resource burdens that they face. Two prominent tools SNS provides free of charge to its state and local partners are SNS TourSolver™ and the RealOpt Suite© of Preparedness and Response Optimization Tools.

Technology for Medical Supply Dispensing

SNS TourSolver™ – a system with over 1,200 users – is a web-based software optimization program that assists state and regional planners in routing their vehicle fleets to optimize the speed with which medical countermeasures (MCMs) are distributed to points of dispensing (PODs) and other medical facilities. This product, developed and maintained by c2Logix-Route Optimization Solutions, is offered at no cost to state, local, tribal, and territorial partners to help maximize countermeasure distribution. SNS TourSolver™ gives emergency preparedness personnel abilities to quickly generate optimized distribution routes for delivery of PODs and simulate multiple scenarios that might affect those routes.

A user can easily adjust the number and size of trucks that are available to move products, the quantity of product that should be delivered to each POD, and the ways in which factors such as time windows and multiple deliveries might influence the dispensing of medicines. This takes planning far ahead of the days when routes were planned by putting pushpins in

Building public health security within complex systems requires careful positioning, distribution, and management of medical resources.

maps or using software that could only route individual vehicles. The software allows users to save scenarios for later access and revision, and model the effect of traffic and other route disruptions on their existing plans.

To address the challenges faced at the local level once product is delivered to each POD, the RealOpt Suite of tools is available. Since 2006, CDC's National Center for Environmental Health (NCEH) and SNS have funded the development of a suite of tools by the Center for Operations Research in Medicine and HealthCare, School of Industrial and Systems Engineering, Georgia Institute of Technology. Taken together, this is called the RealOpt Suite© of Preparedness and Response Optimization Tools. The current RealOpt modules have nearly 10,000 registered users in total.

The RealOpt Suite is comprised of several modeling and optimization software tools designed for planning and simulating flow of persons through PODs, apportioning and dispensing medicines, and even planning for response to radiological events. Using RealOpt, a jurisdiction may design a POD and then see how quickly they can achieve movement of individuals through that POD. Applying this tool will allow a planner to test various assumptions about how many people can be served and how quickly through a given POD. This can lead to a better understanding of how many PODs are required and how many individuals are needed to staff each of those PODs in order to provide medicine to their population in a defined timeline. RealOpt-POD can help optimize the location of PODs so that they reach the optimal number of people. Using computer models such as this is a much cheaper way to determine if a plan works than iterative testing of various scenarios through real-time, resource-intensive exercises and drills.

As the state of public health preparedness continues to advance, preparedness planners must continue to consider how to leverage today's technology and look ahead to emerging capabilities. Application of technological innovation, particularly computational modeling and simulation, will allow the public health sector to better identify resource limitations and overcome those to improve preparedness efforts.

To learn more about SNS, visit <http://www.cdc.gov/phpr/stockpile/stockpile.htm>.

Greg Burel is the director of the Division of Strategic National Stockpile, Office of Public Health Preparedness and Response, at the Centers for Disease Control and Prevention. As head of the nation's largest stockpile of medicines and supplies available for emergency use, he is a leading expert on supply chain management and medical countermeasure distribution and dispensing in the United States. With more than 30 years of civil service, he has risen through the ranks of the federal government, beginning his career at the Internal Revenue Service and serving in leadership roles in the General Services Administration and the Federal Emergency Management Agency. In 2007, he assumed the helm of Strategic National Stockpile operations.

4th
EOD/IED & Countermine Summit

November 7-8, 2016
Mary M. Gates Learning Center, Alexandria, VA

DEFENSE STRATEGIES INSTITUTE
ADVANCING THE MISSION · SUPPORTING THE FORCE

FREE for Military & Government

To register & for More Information visit countermine.dsigroup.org/

Hazard Detection: “Bring Your Own Protection”

By Kathryn Laskey

Current approaches for ensuring public safety rely on expensive and obtrusive equipment and procedures having limited availability and inadequate performance. Newly emerging wearable sensors have the potential to spark a fundamental change in this equation. Researchers at George Mason University are investigating a new concept called “Bring Your Own Protection” (BYOP).



Chemical and radiological hazards pose major safety challenges at venues such as airports, sporting arenas, concert halls, city parks, and college campuses. The increase in threats aimed at soft targets coupled with the relative accessibility of chemical and radiological materials creates the potential for serious destruction perpetrated by malevolent actors.

The BYOP concept leverages the combination of ubiquitous, specialized sensors and state-of-the-art atmospheric dispersion modeling to provide effective protection at lower cost than the current state of practice. A BYOP system can be unobtrusively and affordably deployed at communal occasions such as sporting events, concerts, rallies, and other public gatherings. BYOP promises to provide an agile, affordable, smart system for public safety and protection based on a virtual, quickly deployable wireless sensor network of mobile and/or wearable devices capable of detecting and localizing hazardous sources within an urban environment.

A BYOP system will feature a ubiquitous wireless sensor network that anyone, anywhere, at any time can join. Newly emerging wearable radiation and chemical detectors will alert users when the measured intensity exceeds a threshold. A network formed from such devices can continuously monitor for chemical, biological, radiological, nuclear, and high-yield explosive materials. Sensor outputs can be fused to provide an updated picture of the situation and give timely warning of potential incidents, enabling rapid prevention and/or response.

BYOP provides an affordable smart system for public safety & protection based on a quickly deployable wireless network of devices to detect & localize hazards.

BYOP will bring changes at the national, enterprise, individual, and policy levels. From a *national* perspective, as the number of threats

aimed at soft targets such as public gatherings increases, BYOP can dramatically change the dynamics at the core of the vulnerability of soft targets. From an *enterprise* perspective, the public safety paradigm will change from expensive, centralized control devices to distributed, networked sensors coupled with advanced data fusion and decision-support systems. From an *individual* perspective, the system will bring transformational change in people’s perceptions and their personal responsibility in preparing for and preempting incidents

of public disorder as they shift from information consumers to information providers and from passive targets to actively participating in homeland security. Finally, the BYOP concept requires *policy* initiatives to adapt to the new safety environment of citizens as active participants in ensuring the homeland's safety.

Research on wearable sensors has now progressed to the point at which products are reaching market. However, architectures for information fusion, risk analysis, and decision support have received much less research attention. Further, a multitude of policy challenges ranging from interoperability standards to privacy protection to liability determination need to be addressed to bring the BYOP concept to fruition.

Kathryn Laskey is professor of Systems Engineering and Operations Research (SEOR) at George Mason University and associate director of the Center of Excellence in Command, Control, Communications Computing, Intelligence, and Cyber (C4I & Cyber) at George Mason University. Her primary research area is multi-source information fusion for situation awareness and decision support. She has developed technology and systems to support situation awareness and decision-making across a variety of domains, including military situation awareness and decision support, managing uncertainty in geospatial data, and delay mitigation in the National Airspace System. She is currently examining modeling of inference enterprises devoted to detecting insider threats. She serves on the board of directors of the International Society of Information Fusion, the Association for Uncertainty in Artificial Intelligence, and the Washington Metropolitan Area chapter of the International Council on Systems Engineering (INCOSE). She has served on committees and boards of the National Academy of Sciences.

Don't Miss Last Month's Issue!

Chemical, biological, radiological, nuclear, and high-yield explosive (CBRNE) incidents require many considerations, which include public and mental health, safety and security, training and education, among other critical issues. By asking the experts what keeps them up at night, communities will be better informed as they prepare for a variety of emerging threats.



**Click to
download now**

A Conversation That Should Have Happened

By William H. Austin

Appointment to an emergency management position is a proud moment as well as a moment that creates doubt, anxiety, and internal questioning of one's own ability to handle a major catastrophe. Questions arise about the community's hazards awareness, the status of the local emergency operations plan, and the proverbial, "What keeps you up at night?" scenario.



The appointing authority (mayor or city manager) has confidence in the appointment and everything seems in place for a competent response to disaster, or so it is thought. However, real success in a catastrophic disaster goes far beyond operational expertise. In fact, at least three other areas are so important that a conversation centering on these subjects should be considered immediately between the appointing authority and new emergency manager.

Any overwhelming disaster provides obvious answers to the operational questions surrounding saving lives, stabilizing the incident, and protecting life and property. However, a quick check of disaster history usually shows that it is “downhill” from this point on. The more severe the problem, the quicker these three critical influences begin to surface. The influencers, or “stumbling blocks,” are the concepts of federalism, politics, and disaster logistics.

Knowledge, Skills & Experience

Emergency managers (including fire, emergency medical, and law enforcement officials) are trained for the high-probability, low-consequence events that occur every day. These events have a definable outcome in time, damage, and loss of life. However, the seldom-occurring low-probability, high-consequence events bring a different challenge not practiced on a daily or even monthly basis. High-consequence events cause the need for additional experiential and knowledge requirements. Requirements such as intergovernmental relationship skills, knowledge of citizen and first responder behavioral health concerns, sheltering and feeding procedures for large numbers of citizens, a citizen evacuation plan, and expert knowledge in handling the rescue of disabled citizens.

Intergovernmental skills are required for managing local situations (mutual aid agreements), coordinating with the state (home rule and emergency management assistance compacts), and working with the federal government (Stafford Act). The attitudes, knowledge, and cultures of various players at every level can either contribute to a positive outcome or magnify the weaknesses of the emergency manager. Likewise, background research and training in citizen and first responder behavioral health needs during the pre-disaster period pay off remarkably once the disaster occurs.

Experienced and exercised knowledge of sheltering and feeding operations is an absolute must for every emergency manager. Then, it is important to gain every bit of knowledge one can about evacuation procedures, including the successful handling of disabled citizens in the municipality. These critical knowledge areas are heavily dependent on and run head on into the three influencers or “stumbling blocks.”

Federalism

The first critical influence every emergency manager should understand is the concept of federalism. Federalism has an exciting history of development in the United States and has evolved into a huge shadow of power driven by the control of funding through disaster relief and various other grant programs. The concern about “who is in charge” gets more confusing and complicated when merged with the “who is paying for this” concept.

Although federalism can be called by a number of identifiers, coercive and cooperative federalism, especially in the preparedness grants area, requires a high level of understanding on the emergency manager’s part. More information on federalism can be obtained from Roger Pilon’s article “[Federalism – Then and Now](#),” which was published in the *inFocus Quarterly* on 13 January 2015. From federalism, the transition shows the need for an advanced understanding of a second influencer that is commonly known as politics.

Politics

Emergency managers may be naively thinking that, since “all politics are local” and all the players are known, politics are not a problem. For example, Hurricane Katrina brought out every ugly event and mistake to illustrate the incompetence of emergency managers, mayors, and even a governor, including: numerous agency investigations, congressional hearings, and a presidential review; national media coverage of questionable emergency preparedness and response actions; chaos; and the death of over 1,800 citizens.

Knowledge, skills, and experience give emerging managers the right tools to overcome the influencers of federalism, politics, and disaster logistics.

Elected officials as a rule do not like to explain mistakes. When this happens, blame flows downhill, the public screams, and officials are fired or quietly replaced. Anxiety and anger reach the tipping point when citizens begin to realize that government officials charged with their protection are not prepared, lack a functional emergency operations plan, cannot support shelter and feeding operations, and appear confused about what to do next. Failure, or just the perception of failure, in the emergency operations plan or recognition of citizens’ needs drive politics. For an example, in a [9-minute video](#), Mayor Ray Nagin talks politics as it relates to Hurricane Katrina.

Disaster Logistics

The third influencer in this dilemma now begins to show. This would be a working knowledge of and skill in disaster logistics. A lack of knowledge in disaster logistics – or more directly the lack of understanding required in how to implement the components of disaster logistics – is a major shortcoming. These components include: the procurement, transport, storage, staffing, and training in logistical operations; the handling of safety issues related to logistics; the establishment of site control; distribution of materials and supplies; and demobilization requirements. The logistical components must be embedded into every successful emergency operations plan at every level of response. Logistics are a critical function in pre-disaster as well as post-disaster operational periods.

Disaster logistics is such a relatively new area for emergency managers at the local level that a specific textbook does not exist yet on the subject. However, the University of New Haven,

Connecticut, has developed a graduate-level course on disaster operations and management that is a logistics-based study on implementing the logistical components described in major disaster operations. Further information on the logistics course is available from Wayne E. Sanford, coordinator of the Emergency Management Program at 203-479-4891.

There is a great deal of additional research, training, and understanding required to master these three key influencers. Understanding federalism, politics, and disaster logistics make or break a successful disaster operation. They may appear to be strange subjects to talk to appointing officials about. However, after a disaster, it is too late to say that it was “a conversation that should have happened.”

William H. Austin, DABCHS, CFO, CHS-V, MIFirE, served as the fire chief of West Hartford, Connecticut, from December 1996 until his retirement on 30 July 2011. He has since formed his own consulting practice, The Austin Group LLC, assisting both government and corporate clients in leadership, emergency management, and homeland security issues. He holds a master's degree in security studies (defense and homeland security) from the School of International Studies, United States Naval Postgraduate School, in Monterey, California, and a master's degree in public administration from Troy State University. He served as the chairman of the Connecticut Statewide Citizen Corps Council Advisory Committee from its formation in 2005 to 2014 and served as an appointed member of the Connecticut Emergency Management and Homeland Security Advisory Committee for nine years. He currently serves as an adjunct faculty instructor in the master's degree program in emergency management at the University of New Haven.



critical infrastructure
PROTECTION & RESILIENCE ASIA
including Critical Information Infrastructure Protection



PLUS:
ONE-DAY CERTIFIED TRAINING COURSE
brought to you by:



further details at www.cip-asia.com

5th-6th October 2016
Bangkok, Thailand
www.cip-asia.com

Register Today and Save with the Early Bird
at www.cip-asia.com

Developing resilient infrastructure for a secure future

Today's modern economies and improving living standards rely more and more on the development and security of a country's critical infrastructure. How would a country stand should there be an attack, from natural or man-made disasters, on its key infrastructure?

Discover the latest challenges, strategies and solutions for protecting ASEANs critical national infrastructure

Critical Infrastructure Protection and Resilience Asia will bring together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Asia. Book your delegate place today and save with the Early Bird delegate rate - book your place online at www.cip-asia.com/onlineereg

Co-Hosted By:





Supporting Organisations:












Major Themes From the 2016 Aspen Security Forum

By Erik Gaull

The 2016 Aspen Security Forum was held from July 27 to July 30 in Aspen, Colorado. Over the past seven years, the forum, hosted by the Aspen Institute, has earned a well-deserved reputation as the most important venue for thought leadership in the homeland and national security arenas, attracting distinguished speakers and high-level attendees from around the world. This year's forum was no exception.



Over the course of three days, the secretary of homeland security, the director of the Central Intelligence Agency (CIA), the assistant to the president for homeland security and counterterrorism, the director of national intelligence, two four-star generals, the former chief of the British Secret Intelligence Service (MI-6), the European Union counterterrorism coordinator, the German and Afghanistan ambassadors to the United States, current and former members of Congress, leading academics, and internationally renowned journalists – among others – presented their views, carried on frank dialogues, and answered pointed audience questions on the global issues and trends affecting U.S. and international security. A total of 22 panels covered a wide range of topics, but several issues emerged repeatedly and should be of interest to domestic preparedness professionals. The three persistent themes included the:

- Evolving tactics, techniques, and practices of the Islamic State of Iraq and Syria (ISIS) and what they imply for countering violent extremism and homegrown radicalism;
- Impact of cyber intrusions and cyber warfare on governments, companies, and individuals; and
- Implications of actions and events in Russia, China, North Korea, Iran, and Syria for security in Europe, Asia, and the United States.

Countering Violent Extremism and Homegrown Radicalization

By far, the dominant theme of the conference was the need to counter violent extremism (CVE) and stop homegrown radicalization. Secretary of Homeland Security Jeh Johnson's main comments concerned the rise of the terrorist-*inspired* attack and homegrown radicalization. The homeland security secretary noted that ISIS has changed from trying to position its operatives to carry out terror operations themselves to getting people to "stay home" and execute attacks on behalf of ISIS. Such attacks, the secretary observed, are *significantly* more difficult to interdict than ones that use ISIS personnel, which requires considerable planning, logistics, and funding.

Johnson views "building bridges" to Muslim communities as crucial to preventing ISIS-inspired attacks because law enforcement is not in a position to detect the vast majority of people who are undergoing radicalization – a clear message that law enforcement CVE tactics

need to change. He also stated unequivocally, “Rhetoric that vilifies Muslims is counter to our efforts to build bridges to Muslim communities. Irresponsible rhetoric has consequences.” His clear warning was that Islamophobic demagoguery enables ISIS to recruit new followers by creating an “us-versus-them” motivation in people who are subject to becoming radicalized.

Johnson’s view of the rising threat of homegrown extremism and the need for serious CVE programs was echoed by numerous panelists that followed. Assistant to the President for Homeland Security and Counterterrorism Lisa Monaco stressed that U.S. enemies are recruiting based on the message that Western civilization is at war with Islam. She echoed Johnson’s comments that the nation needs greater connectivity with communities throughout the United States to counter violent extremism, and she went on to say that the governments will have to give communities the tools to identify and react to radicalization. Director of

Understanding and countering violent extremism, homegrown radicalization, and cyberattacks are a priority for international security leaders.

National Intelligence James Clapper indicated that the United States and its allies have made progress against ISIS in areas that can be measured (e.g., terrorists killed, land captured, funds seized), but went on to say, “where we haven’t made progress is in the areas we can’t [measure] ... countering their ideology, proselytizing, and skillful use of the internet and social media.”

Director of the National Counterterrorism Center Nick Rasmussen pointed out that even though ISIS has a significantly reduced geographic area from which to operate, it will still have the ability to launch external attacks because of its ability to inspire people to engage in violence in their home countries – far remote from ISIS strongholds in the Middle East. Bill Bratton (who had not yet announced his resignation as New York Police Department commissioner) drew a distinction between ISIS-inspired, ISIS-enabled, and ISIS-directed terrorism, and he indicated that he is more concerned about ISIS-inspired terrorism than the other two forms because it is so much harder to detect.

Director of the DHS Office of Community Partnerships George Selim, and Secretary Johnson noted that the ability to prevent ISIS-inspired terrorism is largely dependent on people in the community coming forward with information (i.e., “see something, say something”). Selim, who heads a CVE task force, said that local jurisdictions want to develop community-led CVE intervention models. Harvard School of Public Health researcher Jessica Stern pointed to a report from the British think tank, Demos, which points out that successful CVE programs are “localized” (i.e., customized to a given area) and that “tone matters” (i.e., people tend to interact with positive messages, not negative ones). She also indicated that in the West, time on the internet is a major risk factor for the radicalization of young people.

The resounding message was that CVE programs must be made a priority by law enforcement, community leaders, and religious institutions – that countering violent extremism and homegrown radicalization must be a “whole-of-community” effort.

Absent concerted CVE efforts, the United States is likely to see a long period of homegrown, self-radicalized individuals using any tools at their disposal to carry out acts of terrorism on behalf of ISIS.

Cyberattacks and Hacking

Another major theme that should be of interest to state and local government officials as well as to private sector leaders is the vulnerability of critical infrastructure and data systems to cyber attacks and hacking. Speakers focused on the ability of state-sponsored hackers to penetrate seemingly any computer network. The recent hack of the Democratic National Committee e-mail system provided fodder for many questions about who was culpable and whether one could safely say that the hack was the work of the Russians. Although this has been suggested by the Clinton campaign and some information technology security professionals, none of the presenters were willing to go on the record and attribute the intrusion to anyone or speak about how the matter was being investigated.



Cyber vulnerabilities have clear implications for public safety entities. Terrorists have demonstrated their willingness and intent to use the internet as well as guns and explosives to carry out attacks. Presenters pointed out that cyber penetrations have led to physical damage to computers, loss of valuable data and sensitive information, and the compromising of physical systems that are controlled by SCADA (supervisory control and data acquisition) systems. They also noted that many hackers, especially those associated with foreign governments and terrorist organizations, can employ extremely sophisticated methods.

The central message of the experts was that cybersecurity is currently – and will continue to be for the foreseeable future – a major problem. The primary admonition for public safety agencies was that, given their dependence on computing solutions (e.g., computer-assisted dispatching systems, mobile telecommunications systems, and investigative databases), jurisdictions of all types would be well-advised to re-evaluate their cybersecurity programs, policies, and equipment, and to take the necessary actions to prevent and mitigate the effects of a cybersecurity breach.

Understanding International Security Issues in a Domestic Context

The third major theme of the conference was the international security environment. This could be broken down into two primary sub-themes – first, the intentions and recent actions of Russia, China, North Korea, and Iran, and second, the impact of the Syrian Civil War on security in Central Europe.

Panelists and attendees alike seemed to gravitate to the understanding that Russia, China, North Korea, and Iran all display a clear intent to counter Western interests and possess (or are building) the capability to carry out both kinetic and cyber attacks to realize this intent. Russia and China appear to be concentrating largely on the development of offensive cyber capabilities, whereas North Korea and Iran are focused primarily on kinetic weapons.

Panelists were concerned that Kim Jong-un is relatively unknown and unpredictable. Therefore, he could pose a serious threat should North Korea achieve its long-held dream of developing a long-range missile able to reach the Continental United States. Although the chances and timing of success in this respect are hard to assess, realization of this capability could portend a need for domestic preparedness agencies to revive Cold War-like capabilities, doctrines, and practices. Such a return would also be probable should Iran not honor its obligations under Iran Arms Treaty–The Joint Comprehensive Plan of Action and surreptitiously develop a nuclear capability.

There was a lot of discussion of the impact of the Syrian Civil War on the security situation in Europe and the United States. CIA Director John Brennan suggested that there is no end in sight for the Syrian conflict as long as Bashar Al-Assad is in power. The war has produced a steady flood of refugees into Europe, which has proven very difficult to control because of the relative proximity of Syria to Central Europe. Panelists seemed to concur that the war in Syria poses only an indirect threat to the United States in the form of increased terrorism in Europe. In addition, Syrian refugees in the United States are both low in number and risk because of the rigorous vetting process to which they are subject (it takes nearly two years for a refugee to get cleared to enter the United States) and the relative distance and expense of making the trip here. The unstable situation in Syria, however, makes it difficult to root out Nusra Front (al-Qaida’s affiliate in Syria) and provides fertile ground for ISIS to continue its operations. Lisa Monaco warned that the United States should be careful that any success in defeating ISIS does not create a power vacuum that would allow a resurgence of al-Qaida.

Conclusion

The three major themes evident at the 2016 Aspen Security Forum – countering violent extremism and homegrown radicalization, cyber vulnerabilities, and the international security landscape – offer domestic preparedness professionals much in terms of developing actionable plans, understanding threats and vulnerabilities, and improving the awareness and training of frontline personnel. The forum provides an excellent and broad venue for homeland and national security professionals to exchange ideas and build new professional relationships. Attendance at next year’s [Aspen Security Forum](#) (19-22 July 2017) ought to be on every domestic preparedness professional’s agenda.

Erik S. Gaull is the director of Public Safety and Emergency Management Programs for Applied Research Associates Inc. He is a Certified Emergency Manager®, Certified Protection Professional®, and Certified Business Continuity Professional®. In addition, he has earned FEMA’s Master Exercise Practitioner, Professional Continuity Practitioner, Advanced Professional Series, and Professional Development Series recognitions. He is currently an officer in the D.C. Police Department Reserve Division and a firefighter/paramedic III in the Montgomery, Maryland, County Fire-Rescue Service. He has a Master of Public Policy and an MBA from Georgetown

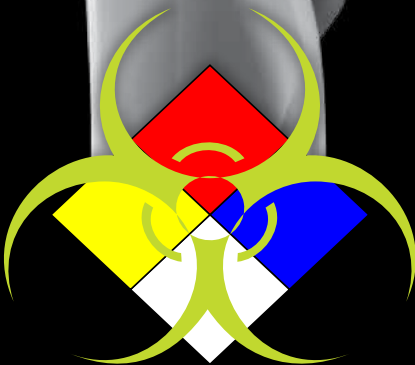
Invisible Threats Exposed



AP4C

**Portable Chemical Detection System
Protects First Responders, Military & Infrastructure**

- Fast, Reliable Analysis of Invisible Hazards Saves Time & Lives
- Unlimited Simultaneous Detection Exposes Unknown Agents
- Low Maintenance & Operation Costs Save Money
- Rugged Handheld Design is Easy-To-Use With Minimal Training
- Complete System Includes Accessories & Case for Easy Transport



[Learn More Online](#)

PROENGINE

Chemical and Biological Detection Systems