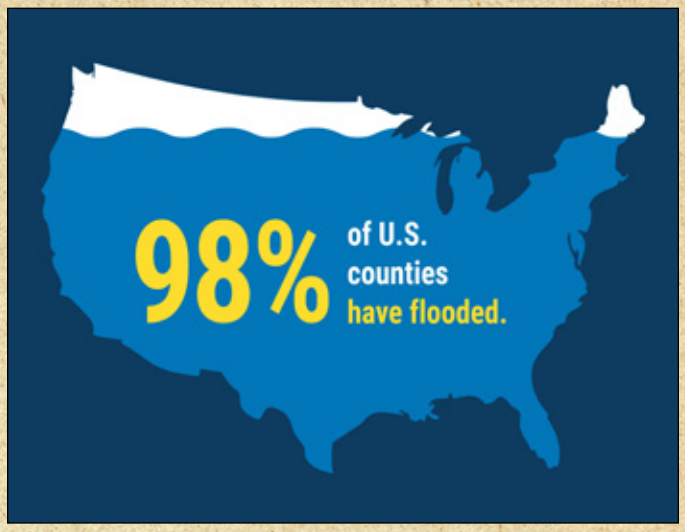
domestic preparedness .com

DomPrep Journal

Subscribe

Volume 15, Issue 5, May 2019

Meeting Healthcare Supply Chain Needs at All Times
By James M. Rush Sr.



More Floods, More Effective Flood-Fighting Technology
By John Dames

Advancing Resilience – Building Codes & Benchmarking
By Ryan Colker

School Active Shooter Drills – From Anxiety to Apathy
By Robert C. Hutchinson

Also inside...

Hybrid Warfare – Impact on Preparedness & Resilience,
By Martin (Marty) D. Masiuk;
Emerging Homeland Security Issues – A 2018 Panel Review,
By Joseph J. Leonard Jr.

IS YOUR DEPARTMENT PREPARED FOR

THE UNEXPECTED?

Hazardous materials have become a part of everyday life. When mishandled or when accidents occur, hazardous materials can present a deadly threat to public health and safety.

For over 30 years the **International Hazmat Response Team Conference** has offered informative sessions and unique hands-on training designed to tackle the most pressing hazmat issues at all levels of experience.

WHAT TO EXPECT

This four-day event offers attendees hands-on training across a range of essential topics, including:

- Biothreat response & sample collection
- Incident management best practices
- Chemical & physical properties of hazardous materials
- Recognizing & responding to commercial explosive incidents

EXHIBITORS

Bring back the newest hazmat gear for your department, with more than 100 exhibitors showcasing the latest innovations in the hazmat industry.

CONNECT WITH US: @IAFC @firechiefs @IAFC #Hazmat2019

POWERED BY:

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

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

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

Carole Parker
Manager, Integrated Media
cparker@domprep.com

Advertisers in This Issue:

BioFire Defense

FLIR Systems Inc.

International Hazmat Response Team Conference

PROENGIN Inc.

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.

IMR GROUP

Featured in This Issue

Pictured on the Cover: (top row) Rush, Source: ©iStock.com/petrovv; Dames, Source: FEMA, 2018 (second row) Colker, Source: ANCR, 2019; Hutchinson, Source: ©iStock.com/Susan Vineyard

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!

BIOFIRE®

DEFENSE

Learn more at www.BioFireDefense.com

Strengthening Threat-Mitigation Efforts in Changing Times

By Catherine L. Feinman

Threats come in many forms. Some occur naturally from weather events. Some occur maliciously through technological manipulations. Some occur violently with traditional weaponry or weaponized materials. Some threats combine two or more of these and other threats. The preparedness community is tasked with identifying potential threats in order to mitigate or thwart the devastating consequences should a threat manifest in disaster.

The 21st century is proving to be a period of rapid change, with technological advances being both beneficial and detrimental to disaster mitigation efforts. For example, social media disseminates valuable real-time information for disaster response as well as false information to change public opinion or hinder response. Social media has even become a tool to support hybrid warfare. The only way to effectively combat hybrid threats is through interagency relationships and collaboration.

The 21st century is proving to be a period of rapid change, with technological advances being both beneficial and detrimental to disaster mitigation efforts.

Such relationships ensure development of procedures and processes that promote dialogue and problem-solve for threats and concerns that affect disparate communities. Healthcare supply chain management is one example where interjurisdictional collaboration is critical. Building codes and benchmarks facilitate the development of strategies and materials to fortify structures and minimize risk to persons and property. Technology provides tools to enhance crisis management through surveillance, connectivity, and situational awareness technologies.

Of course, the community's part in threat detection and mitigation cannot be understated. Threat management involves engaging the community with effective messaging, providing stakeholders with the right tools, and ensuring an appropriate level of engagement from the public. Avoiding the societal response extremes of anxiety and apathy can help to build a strong threat detection, mitigation, and response base upon which planning, communication, technology, and crisis management can thrive.

Hybrid Warfare – Impact on Preparedness & Resilience

By Martin (Marty) D. Masiuk

During the first two decades of the 21st century, the nation's security and defense focus was primarily on terrorism by non-state actors and lone wolves. During that same period, advances in digital and information technology were rapidly adopted by government and industry. Often technology's implementation was quick and cheap with little regard to being secure, which created security gaps and vulnerabilities. Today, China, Russia, Iran, and North Korea are asserting themselves on the geopolitical stage. Each country has recognized that there is a strategic advantage to using cyber warfare to "threaten both minds and machines in an expanding number of ways – to steal information, to influence our citizens, or to disrupt critical infrastructure." Threats include the weaponization of information by utilizing social media and sponsorship of "news-media" programs.

Industry along with emergency managers and public safety officials are now challenged with a sobering question: "Is your organization ready to defend, respond to and recover from a well-planned and funded hybrid act on your local, critical assets by state and non-state actors?"

In 2019, the Preparedness Leadership Council (PLC) will host four roundtables across the country to better define the hybrid warfare problem, understand its consequences, discuss interdependencies, and provide solutions and actionable items for operational executives and policy makers. A typical roundtable will host approximately 30 invited guests representing industry, emergency management, public safety, medical response, law enforcement, the United States Coast Guard and National Guard, along with nongovernmental organizations. Senior operational managers will convene in San Francisco (July), Chicago (September), New Orleans (October), and New York City (December) with facilitated conversations.

Topics of discussion will include:

- What is hybrid warfare and its consequences to local preparedness and resilience professionals?
- What are some of the weapons used in a hybrid attack?
- How can social media and other nontraditional "media outlets" complicate a local response and recovery plan?

- How do "weapons of mass distraction" affect public trust while providing deniability and anonymity to the covert attacker?
- What are feasible solutions, actionable items, and other next steps that need to be understood?

After the roundtables, the PLC will host an executive briefing at The National Press Club, Washington, DC, in January 2020, to present a report gathered from those roundtables. That report will also be presented to members of both legislative and executive branches of the federal government. Additionally, DomesticPreparedness.com will distribute copies nationwide.

The PLC and DomesticPreparedness.com invite emergency preparedness, response, and resilience professionals to share their knowledge and experiences on the critical topic of cyber warfare throughout the year. There are three urgent calls to action:

- Would you like to participate in a roundtable at one of the venues in 2019?
- May we send you information about submitting an article to share information on one of the above topics of discussion?
- Are you a subject matter expert who would like to participate in a call-in podcast recording?

Contact me at masiuk@plcouncil.org if you are interested in participating in an upcoming roundtable or podcast; and contact the editor-in-chief at cfeinmand@domprep.com to submit an article for consideration in the *DomPrep Journal*.


DomPrep, 2018

Meeting Healthcare Supply Chain Needs at All Times

By James M. Rush Sr.

The healthcare industry has numerous supply chain challenges as it strives to meet patient and facility needs during routine operations as well as during small- and large-surge events. The current process has gaps that need to be filled. However, there is a possible solution.

Federal agencies have promulgated publications regarding supply chains and how they work. The Centers for Disease Control and Prevention (CDC) published a "Supply Chain Disaster Preparedness Manual" aimed at advising healthcare organizations (and other enterprises) on how to prepare for disasters. U.S. Department of Homeland Security's Federal Emergency Management Agency published a booklet entitled, "Supply Chain Resilience Guide." However, neither publication adequately discusses "The Industrial Base" for the supply chain, and how industry and the supply chain are affected by large spikes in demand for products, such as those that occur during a disaster.

Stockpiling Concerns

Surges in product demand (orders) affect the entire supply chain. In 2014, the United States had three cases of Ebola in North Texas and one case in Nebraska, which required 21 days of monitoring for Ebola symptoms and was later cleared. It was difficult to obtain personal protective equipment (PPE) during that scare – all for just three cases of Ebola. This raises the question, "How is it possible that the supply chain ran short of PPE with only three cases of Ebola?" The answer is that many hospitals across the country checked their stocks of PPE and other items and "stocked up" on PPE plus a lot more. Whenever there is a rush to purchase the same products at the same time, shelves empty very quickly – "the empty shelves syndrome." These runs on the supply chain can upset "just in time" (JIT) inventory for months at a time.

In addition, hospital stockpiling causes a "yoyo effect" with periods of plenty, followed by long-term backorders at the local, regional, and national levels. In order for JIT to work, it has to correlate with regular usage, not cache (stockpile) levels. Hospitals that replenish their caches do so based on their own storage objectives rather than their product usage. When enough healthcare organizations order based on their individual stockpile, the relationship between weekly use and weekly orders break down. There will be a tipping point where medical manufacturers and distributors product demand forecasts become meaningless. It may take many years for America's medical supply chain to recover.

Manufacturing & Distribution Concerns

Offshore single-source manufacturing of medical products is problematic during large-scale, long-term disasters. Considering the problems in 2017 with intravenous (IV) fluids after hurricane Maria in Puerto Rico, multiple sources of medical products are needed – including in the United States. During a large-scale epidemic – or worse, a pandemic –

nations will likely take care of their domestic needs, before shipping products to other countries. Once again, JIT may fail in the face of a surge event. The industrial base cannot instantaneously gear up for a surge event. For this reason, federal agencies should pay civilian medical supply chain vendors to build large federal inventories for use by federal agencies during large-scale disasters.

Federal agencies would do well to use national distributors' inventory management subject matter experts before advising healthcare or other enterprises on disaster supply chain issues. The supply chain is complicated and has many tentacles in a global economy. Civilian enterprise inventory management/supply chain experts are invaluable sources for advice on critical supply chain issues for use before, during, and after disasters. Federal planners must use private industries for building supply systems robust enough to remain operational during and after large-scale, long-term disasters.

Solution: Build a Public-Private Sector National Medical Materials Management System

The following outline of the process supports the idea of building an enhanced, resilient supply chain that is lean and economical during normal times, yet resilient enough to support the medical community during large surges in medical material demand.

- The JIT operational construct will continue to work well for day-to-day medical material demands. There has been some guidance for healthcare facilities to build caches/stockpiles to improve medical inventories at the health facility level. This is a bad decision because hoarding weakens the accuracy of computer demand forecasts. Unreliable computerized demand forecasts eventually may result in persistent backorders and product shortages. Distributors need to stress to their healthcare customers the negative aspects of cache building on the overall supply chain enterprise.
- Once a federal agency (most likely the U.S. Department of Health and Human Services) develops medical material requirements listings based on a national hazard vulnerability assessment (HVA), the product of the national HVA would be a *list of federal planning scenarios*. These planning scenarios would describe the most likely disasters, the numbers and types of casualties and fatalities of each scenario, and the types and quantities of medical products needed to support each planning scenario. The finished product would constitute a *national medical materials requirements listing*. The federal government would then provide the funds for civilian distributors to purchase, store, manage,

release (as directed), and recover federal medical material as appropriate. This would be a separate government-owned inventory of materials along side of the distributor's inventory, which is ready to use in a disaster.

- The federal agency would convene a group of private sector senior level Inventory management subject matter experts (distributors inventory management team), to use the *national medical materials requirements listing* to build a national materials management system, representing both medical/surgical and pharmaceutical product distributors. There would be a senior-level government expert with deep knowledge of the various inventory accountability models attached to the private sector subject matter team. Federal financial subject matter experts are proficient in setting up government financial obligation systems, like a medical/dental stock fund in use in armed forces medical materials management systems. The final product will be a robust, resilient national medical materials management system that will ensure availability of the right materials in the right quantities at the right place in good times and in bad. The goal is to maximize the number of lives saved and minimize suffering during and after future disasters.
- This program would enable medical distributors to manage both "private sector-owned" material (JIT for normal times) and government-owned/ contractor managed just in case material (JIC for emergencies) that can flow into the private sector supply chain when the federal government orders the release of government-owned material during disasters or contingencies.

A plan for building a resilient supply chain that is equally beneficial during normal operations and during high-demand surges involves three key steps. First, the government requirements team produces the *national medical materials requirements listing* for the top federal planning scenarios and hands those listings off to the private sector inventory management team, along with a federal fund citation needed to purchase the federal requirements. Second, using the provided federal fund citation, the private sector inventory management team procures government-owned materials and develops a stock rotation, warehousing site plans and inventory location plans. Third, a federal oversight agency reviews and approves all plans, processes, and procedures and approves the national medical materials management system for adoption.

James M. Rush Sr. has over 45 years of healthcare administration and community emergency management experience in the U.S. armed forces, the U.S. public-health community, and the nation's civilian healthcare industry. He served as the Region III project officer for the National Bioterrorism Hospital Preparedness Program, and the CDC's National Pharmaceutical Stockpile, always dedicated to assisting healthcare and public health organizations prepare for "all hazards" events and incidents. He is author of, among other published works, the "Disaster Preparedness Manual for Healthcare Materials Management Professionals," and a self-published book "Unprepared."

Emerging Homeland Security Issues – A 2018 Panel Review

By Joseph J. Leonard Jr.

DomPrep hosted the 2018 Emerging Homeland Security Issues Panel in conjunction with the Clean Gulf Conference in New Orleans, Louisiana, on 13 November 2018. The active discussion among panel members and more than 50 attendees focused on hybrid warfare and the current threat environment, strategic and operational preparedness, emerging technology to meet these threats, and sustainment of interagency relationships.

As of May 2019, there was still doubt whether either major political party was actively involved in efforts to undermine the 2016 elections. What seems to be certain is that Russia was actively involved in undermining confidence in the election process. How effective this endeavor was will remain open to debate for years:

- Was this a form of "hybrid warfare" implemented by a nation-state as a low-cost means of manipulating a message to advance its own agenda?
- Was this an example of the so-called "Gerasimov Doctrine," whose existence has been debated over the last few years?

Former Secretary of Defense James Mattis stated in the 2018 National Defense Strategy that, "Inter-state strategic competition, not terrorism, is now the primary concern in U.S. national security." Although a peer-competitor, Russia's $42 billion 2017 defense budget is only 6% of the U.S. defense budget; and Russia has shown a willingness to use low-cost, innovative means to influence the political and strategic landscape, as shown in the Crimea and Eastern Ukraine. These facts raise questions about: whether Russia is using similar means and achieving a level of success in the United States; whether much smaller nations could manipulate information and perceptions of that information to advance their goals at the United States' expense; whether a multi-national corporation could do the same thing to a commercial competitor; and whether an individual could influence a community's attitude against a neighbor.

A North Atlantic Treaty Organization (NATO) military working group defined hybrid threats in 2010 as "those posed by adversaries, with the ability to simultaneously employ conventional and nonconventional means adaptively in pursuit of their objectives." U.S. Marine Corps (USMC) Major Valerie McGuire expanded on this in a 2018 article for U.S. Naval Institute's *Proceedings* stating, "Hybrid warfare, often employed in the gray area between traditional peace and war, is the synergetic fusion of asymmetric tactics, unconventional methods, and traditional instruments of power and influence applied across and within every warfighting domain – air, land, sea, space, cyberspace, and information – to pursue national and strategic interests."

These and other topics were addressed by the November 2018 panel of homeland security professionals, which included:

1. Captain Kristi Luttrell, U.S. Coast Guard (USCG), Commander, USCG Sector New Orleans
2. Justin Thomas Russell, Executive Director, Spill Cleanup Association of America
3. Commander Sharon Russell, USCG Reserve, CEM, PMP, Emergency Management Director, Pasco County Sheriff's Office
4. John Temperilli, Senior Manager with Garner-KSolve-OMI
5. Dr. Michael Wallace, EdD, Professor of Practice and Director, Emergency and Security Studies at Tulane University (and Commander, U.S. Navy, retired)
6. Forrest Zolczer, Emergency Response Project Manager with U.S. Environmental Services

Panel participants were in unanimous agreement that hybrid warfare is being used by peer and non-peer competitors of the United States as a means of fostering division through confusing messages that degrade confidence in political and economic systems. All agreed that information acquisition by itself is insufficient to enhance security. The information must be analyzed and vetted to ensure accuracy and reliability. Only then can this information be transformed into actionable intelligence to support the decision-making process.

Sharon Russell put this in terms everyone could understand, saying:

> *We are now very much a divided community. That's important, regardless of the cause, because it means we cannot unify behind anything. It's akin to a family dinner where everyone is arguing over who will carve the turkey, not realizing the dog has already stolen the turkey.*

As Luttrell so succinctly stated, "Hybrid warfare diverts attention from what is important." This diversion, if successfully exploited, can be an opening to even more significant vulnerabilities with catastrophic consequences. And it could be accomplished with a minimal budget.

Wallace looked at this more holistically, "The rise of social media has contributed to a rise in information operations. You can reach and influence a lot more people with today's internet. If it's written on the internet, it must be true." As Russia has shown, this can be accomplished on a minimal budget. If that is the case, other nations or entities might be employing hybrid warfare to advance their agendas as well.

Zolczer echoed Wallace's comments, saying:

> *Every one of us has probably had to face "false data" in the course of our recent personal and professional lives. We know and recognize that some things being portrayed in the news, in social media, and from some elected leaders and other prominent people are false. How do we combat the enemy from within?*

These actions are exemplified in data manipulation. If people cannot trust the data in front of them – and they have unlimited time – they might seek more information elsewhere. However, with limited time, the options are also limited. Imagine a broker needing financial data to process a short-fuse acquisition, a surgeon needing critical information on a patient, or a pilot or ship's master needing navigational information to transit a busy commercial waterway. The information consumer must determine which data to trust and which to ignore. The impact of using some or all of the wrong data, though, is unknown.

Many entities, such as emergency operations centers, elected leadership, public health organizations, and the news media rely on standardized procedures to ensure the information that they are using or presenting is as accurate as possible. Planning section chiefs in an incident command post typically rely on a "rumor board" within the situation unit, where information not yet vetted would be listed. A person or small staff would have the unenviable task of sifting through this information to discern what is accurate and what is noise that may or may not impact the task. This takes time, resources, and a dedicated effort by knowledgeable individuals who often go unrecognized. Overwhelming an incident response with this kind of "noise" and other distractions provided via the telephone or social media could drastically impact the overall response, putting lives in jeopardy, lead to the loss of property and critical infrastructure, and significantly damage the environment.

The diversion of hybrid warfare, if successfully exploited, can be an opening to even more significant vulnerabilities with catastrophic consequences.

As another example, the U.S. Coast Guard vets every ship coming into U.S. ports. The follow-on activities (e.g., additional inspections offshore, detention or removal of persons, escorting of the vessel as it enters port) of Coast Guard, Customs and Border Protection, Federal Bureau of Investigation, and other entities are then based on the findings of this vetting. If a state or non-state actor or a lone wolf manipulated this information, it could significantly affect the flow of commerce through the Marine Transportation System. This could limit the movement of goods and raw materials that can affect additional critical infrastructure systems, and run up the costs of consumer goods. It may also provide an opportunity for those with nefarious purposes to smuggle weapons or persons with the intent of harming the general public or critical infrastructure.

Cellphones provide direct ties to reality during and after incidents and events, with Facebook, Twitter, and other forms of social media becoming the primary means to exchange real-time information. Foreign and homegrown actors have used social media to sow false

information to unsuspecting persons. For example, something as simple as "the water supply is contaminated" can easily impact a significant population. Such information must be handled and stopped. The U.S. Department of Homeland Security and Federal Emergency Management Agency deal with this on a regular basis. As Justin Russell said, "We need to avoid going down rabbit holes…. Instead, we have to block the rabbit holes from being created … that's the challenge."

Sharon Russell stated the need to refocus with pre-9/11 attitudes:

> *Our best course of action is still to prevent an incident from happening. We are not doing a good job rallying behind common goals. This could well be because others are sowing seeds of doubt. We as a nation have to come together against common enemies. Differences were set aside and we were able to focus as a nation. We need to recreate that unification without the need for a catalyst like 9-11 to do so.*

Agencies and organizations need to be wary of those fostering division, recognize the warning signs, and act accordingly in the best interests of the nation. Those in the private sector also need to consider threats against their industries or organizations. Everyone must be vigilant. The insidious nature of hybrid warfare knows no bounds and can range from nation-states acting in their own self-interests, to industrial sabotage that lessens confidence in consumer products, to cyberbullying that can affect a single individual.

Whether or not hybrid warfare is referred to as something conceived by Marshal Gerasimov (i.e., "Gerasimov Doctrine") is immaterial. Hybrid warfare is not only real, its impacts occur to varing degrees every day.

Cybersecurity Challenges

This is an issue that seems to be on the news almost daily and is becoming a growing issue in daily life. To highlight current cybersecurity challenges, a quick survey of those assembled at the panel discussion revealed that *everyone* in the audience was a victim of either some form of hacking or had portions of personally identifying information compromised within the past two years.

Wallace stated:

> *We are currently engaged in a cyber cold war where nations are stealing information and data. This has been going on for decades. Digital insurgency – used by extremist groups to reach recruits, give them a sense of belonging and provide tactics, techniques, and procedures for participation in a global effort.*

The Islamic State Group is the pioneer in the effort and al-Qaida is catching up, as are others. Wallace went on to state, "The internet of things will only make things worse. The interconnection of systems (such as critical infrastructure sectors) will be exploited – not if, but when. Given enough time, money, and effort, terrorists and criminals will find a way."

Sixty percent of the world's grain is transported via inland river systems to locations all over the world. The annual value of the U.S. Marine Transportation System is $4.6 trillion and it employs 23 million people. A maritime cyberthreat is real. Cybersecurity specialists and preparedness specialists must consider potential vulnerabilities and determine security measures to safeguard the flow of people and commerce. Justin Russell noted the potential for a direct tie between hybrid warfare and cybersecurity issues in the maritime community, pointing out that a state or non-state actor could:

- Manipulate data to cause every intermodal container on a ship to be sent to the wrong location. The economic impact could be millions of dollars.
- Intentionally update navigation systems with false or inaccurate information – for example, when a complacent officer on watch does not confirm a person's identity before allowing him or her access to a cruise ship's navigation system. Although the economic impact would be considerable, the potential loss of life could be catastrophic.
- Hack into the computer system of an oil rig and provide a false reading on computer stabilization or pressure readings. This could lead to an environmental disaster and potential loss of life.

All of these scenarios are realistic. Documented cyberattacks have already occurred in the maritime community. Justin Russell recalled:

> *One East Coast port had the opportunity to be a participant with the Director of National Intelligence, the Coast Guard, and industry on an effort to enhance cyber preparedness but declined because the port authority did not envision this as a real threat. Within a month, they were attacked.*

The Maersk attack in June 2017 triggered an internal assessment by numerous multinational corporations to discern if they have the capacity to purchase cryptocurrency to pay a ransom to facilitate continued operations. That is not much different than the tribute paid by nation states to the Barbary pirates to ensure the safe transit of their goods in the Mediterranean Sea in the late 1700s and early 1800s. Ransom should not be the long-term answer, but that does not mean going "to the shores of Tripoli" is the answer either. Governments and multinational corporations will have to determine if their responses will be proportional or if they will escalate events.

The 2014 Sony hack was alarming to many people, especially in business, regarding the impact of a cyberattack, which involved the financial sector and was politically driven. For a multinational company like Sony, many questions arise regarding: who will respond (e.g., the company, the United States, Japan); if and how they would work together; what the response will be; and whether the response will invite another, potentially more damaging, attack.

Temperilli discussed a recent effort in the Houston-Galveston area called Operation SWORDFISH. Captain (now REAR Admiral) Brian Penoyer, then-Commander at Sector Houston-Galveston, with assistance of USCG headquarters, attempted to discern the number

of open-source platforms they could find along the river systems within the sector area of responsibility. "Of the 20,000 platforms detected, over 1,000 were open source, 10-12 of which were major petrochemical facilities that were wide open and susceptible to hacking," said Temperilli. Operation SWORDFISH excluded vessels and focused only on fixed facilities. Those facilities were informed of their vulnerabilities and requested to enhance protection. This highlights some potential vulnerabilities that need to be safeguarded.

Even with these examples, though, there are no easy answers to the following: how to get stakeholders to understand this is real; how to balance constitutional rights with protecting the country, the infrastructure, and the economy. Like much of the emerging technology associated with it, the U.S. cybersecurity and response strategy is evolving at a rapid pace. It also costs money, often a lot of money. Sometimes it is difficult for those controlling the budgets to realize the tangible benefits of these costly security measures. This is not surprising. Technology is constantly evolving, sometimes faster than procurements systems can keep up with the progress. As such, cybersecurity specialists need to work with technology developers to ensure that the appropriate capabilities are being developed or enhanced.

As those with nefarious purposes seek to subvert these systems, those protecting them must react in a timely and effective manner to minimize damage. Although it is still debatable whether the United States is as proactive as it needs to be, it is obvious that the need to safeguard cyber systems is at an all-time high and continues to grow. One audience member voiced concerns that industry will only make the needed investments in security if they themselves are directly impacted or if it can be made clear how the costs of enhanced security will be offset in resilience and long-term profitability.

Interagency Relationships

The panelists concurred that, with today's whole of government approach to homeland safety and security, it is vital for leaders at all levels to foster active and sustained relationships with response partners at the federal, state, tribal, local, and private sector levels. Future generations need to be strongly encouraged to develop and build on these relationships to enhance interagency interoperability over the long term. Do not wait until a 3 a.m. incident to meet one another for the first time. It is equally critical to continue improving the process for sharing and communicating critical information and creating a shared common operational picture to enhance preparedness and resilience.

Recommendations

As Sharon Russell said, "Most of society will look for the good. Many of us in this room are the doom and gloom minority. Society wants to find something happy to rally around. They don't want to think of people doing nefarious things." Nevertheless, DomPrep readers are comprised of preparedness, safety, or security specialists who live in the world of "doom and gloom" and plan for Black Swan events. They have to look at these complex issues and offer reasonable recommendations to elected leaders and/or corporate or

organizational leadership. Hybrid warfare, cybersecurity, emerging technologies, and interagency interoperability are four areas to consider for improving and enhancing homeland security capabilities.

Hybrid Warfare – Take a look at one or more of the articles on hybrid warfare and the Gerasimov Doctrine (e.g., "Hybrid Warfare Helps Russia Level the Playing Field" by USMC Major McGuire). Decide on the validity of the Gerasimov Doctrine and how it might apply to an organization and its personnel. Then go a step further. Seek out means to implement a hybrid attack on the organization during the next security exercise. Note if and how people respond, how an attack of this nature can divide staff members or impede decision making, or how it might cause unanticipated delays when time is of the essence. Assess the organization's ability to respond in a timely and effective manner. Most importantly, share any lessons learned and best practices.

Cybersecurity – Take the time to review and, if necessary, update the organization's cybersecurity, continuity of operations, and business continuity plans. Odds are they are protective in nature, at least as far as the cyber realm goes, but may not be as response oriented as they potentially need to be. Ask the IT specialists what their response plans are if the organization's systems are compromised or unusable. If the plans do not effectively address response, then short- and long-term resilience is in question. Consider which activities would enhance capabilities, before it is too late. For a blueprint for response to an IT incident, consider starting with, "Incident Management for Operations" by Rob Schnepp, Ron Vidal, and Chris Hawley.

Emerging Technologies – Whether it is systems to display a common operational picture, air monitoring devices, communications capabilities, or drones, it is difficult to stay current with all aspects of emerging technology without becoming so bogged down that other tasks become neglected. Look at not only technological capabilities but usability in the field. Commercial off-the-shelf technology is great *if* it meets current and anticipated needs. Before looking elsewhere, recognize that manufacturers are often quite willing to work with organizations in helping them meet specific capability needs. Be willing to reach out to these manufacturers and engage them with ideas, probing questions, and concerns. It may be necessary to become equal partners in the design and development of technology to ensure it meets the organization's needs – both now and in the foreseeable future. Take the time to meet manufacturers' representatives at the organization, at their facility, or at suitable events such as conferences and expositions. Ensure the developers have a comprehensive understanding of the organization's needs, procurement methods, and budgets to find effective solutions to technology needs. This is one of the most effective ways to put scarce budget dollars to desired use.

Interagency Interoperability – No effort to enhance security is less costly than taking the time and effort to improve relationships with actual and potential partners and stakeholders. The Houston Ship Channel Security District and the Houston-Galveston Port Coordination

Team are robust platforms designed and developed by stakeholders to support comprehensive marine transportation initiatives. These are models that should be emulated elsewhere in the United States. In addition, a cup of coffee, lunch, a challenge coin, a t-shirt, a business card, or LinkedIn request are often all that is needed to open the door to an improved relationship. This relationship needs to focus on mutual trust and confidence; on an understanding of organizational jurisdictional authorities, plans, capabilities, and limitations; and on ways to mutually support one another in the conduct of duties. Planning scenarios need to reach a level that effectively challenges plans, training, resources, capabilities, and facilities – not simply planning for the last event. Use these relationships to challenge "what if" scenarios and Black Swan events.

Conclusion

Threats are emerging from a variety of state, non-state, and corporate entities as well as from lone wolves. Agility is the key to a dynamic defense in depth that will help safeguard the nation's infrastructure, economic engines, and political systems as well as foster long-term resilience.

Addressing the ability to recognize and respond to new and innovative means of hybrid warfare will minimize the likelihood of being surprised by an adversary who seeks to undermine capabilities and systems. Personal and organizational protection from cybersecurity threats is critical, but having an effective capability to respond to a cyberattack is the next logical step to ensure resilience. Organizations need to actively work with the developers of emerging technology to ensure advancements meet anticipated organizational needs. This requires input from the field as well as from management to address design, procurement, and budgeting. Lastly, organizations must continue to build active and sustainable relationships with partner agencies and stakeholders to ensure mutual support and effective information sharing in today's all-threats/all-hazard environment.

Homeland security is a long-term process involving a whole of government and whole of community approach to be effective. It involves the public sector, private sector, and individuals throughout the nation. Effective homeland security ensures resilience, but only if all stakeholders are part of it. *DomPrep challenge to all of its readers*: Be a part of "our" homeland security process. Temperilli recalled what retired Navy Captain Steve Nerheim, Director of the Houston-Galveston Vessel Traffic Service, often says, "Success is not earned. It is the rent that comes due every single day."

CDR Joseph J. Leonard Jr., USCG (ret.), MEP, MCP, CEM, CHPP, CPE, is a 30-year veteran of the Coast Guard and is a principal with the Penta Consortium LLC. He serves as the chair of the Greater Harris County Local Emergency Planning Committee and actively serves in the U.S. Coast Guard Auxiliary. He holds designations as a Master Exercise Practitioner, Master Continuity Practitioner, Certified Emergency Manager, Certified in Homeland Protection Professional, and Certified Port Executive. He has a BA in history from the Virginia Military Institute and an MS in engineering technology from Murray State University.

UNLABELED LEAKING BARREL

FLIR Griffin G510

The FLIR Griffin G510 GC-MS enables responders to confidently identify unknown chemical threats. It is the ultimate chemical detection toolbox, with guided controls and simple threat alarms. Completely self-contained and mission-ready, the G510 is built for everyone and everywhere.

Download FLIR's Chem Guidebook to learn more about ID tools like the G510: flir.com/chemguidebook

FLIR®

More Floods, More Effective Flood-Fighting Technology

By John Dames

As floods become more severe and more frequent, government authorities must invest in advanced technology platforms that take the guesswork out of crisis management. Since the consequences of flood events vary dramatically, the tools used to fight them – such as surveillance, connectivity, and situational awareness technologies – must be able to adapt to each unique situation.

In 2018 alone, there were 14 weather-related natural disasters across the United States that caused total damage exceeding $65 billion. From hurricanes and wildfires to droughts and floods, natural disasters have had devastating effects in recent years, with increasing frequency. Although all of these threats deserve renewed attention from government authorities and first responders, floods have been especially destructive, from the deadly 2005 flooding in the wake of Hurricane Katrina to the recent flooding in the Midwest.

As floods take a greater toll on the nation's aging national infrastructure system and put communities across the country at risk, it is incumbent on government authorities to develop flood preparedness and response plans equal to the magnitude of the challenge. To do so, local, state, and federal authorities must surmount historical obstacles that have (perhaps until recently) largely stymied governmental agencies and first responders alike. Many of these lessons have been learned the hard way, but they underscore the importance of "getting it right" in the immediate aftermath of major flooding events.

Flooding: A Rising Threat

Natural disasters of all kinds pose challenges for communities across the country. However, flooding – the end result of events such as hurricanes and late winter storms – carries significant consequences in both the short- and long-term. In addition to the 2019 flooding in the Dakotas, Nebraska, and Montana (events that have already pushed local governments to the breaking point), the past decade has witnessed floods that have left indelible marks on communities and resulted in the loss of human life. Many of these events have also posed serious threats to national security and defense apparatus.

The floods that accompanied Hurricane Harvey paralyzed one of the nation's largest metropolitan areas and contributed to the deaths of nearly 100 people. Superstorm Sandy, which struck New York and New Jersey in 2012 and resulted in more than $60 billion worth of damage, resulted in floods so severe that nearly half of all deaths caused by the disaster were related to flooding.

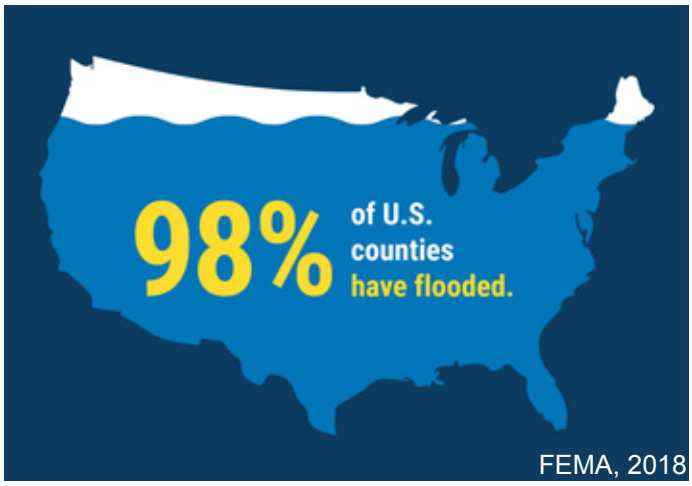
For government authorities, which marshal disaster relief resources and organize crisis management, flooding poses unique challenges. Often simultaneously affecting broad geographic areas ranging from urban zones to rural communities, floods demand synchronized action on multiple fronts. Additionally, the essential components of orderly

and unified disaster relief (e.g., effective information sharing and community outreach) may become even more strained during floods, which can cause power outages, interfere with internet and cellular connectivity, and disable phone lines.

The Role of Technology in Disaster Management

Although the short- and long-term consequences of increasingly frequent flooding vary from one community to the next, what is clear is that authorities across multiple levels of government need to invest in smart, strategic flood-response technology to prepare disaster response teams for the immediate aftermath of these events. The most effective flood response technologies range from drones for surveillance to situational awareness platforms that ensure valuable data reaches the right people. These tools allow decision-makers to build a comprehensive plan of action and respond to flooding events in real-time.

Although natural disasters have always presented considerable challenges to authorities – especially at the local level where resources and personnel can be limited – flood responses in particular demand a significant degree of coordination and collaboration. By incorporating surveillance, connectivity, and situational awareness technologies, it should be possible to launch emergency responses that are faster, better organized, and ultimately more effective in mitigating the damage of flood events.



It is essential that emergency response teams deployed to flooded areas operate from a shared common operational picture (COP) – one that provides reliable, real-time information as to the whereabouts of citizens, response crews, and infrastructural assets. In other words, the COP should enable high-fidelity situational awareness across all relevant personnel. By working from sound intelligence, disaster management efforts can be organized from the top down, rather than by way of the traditional "every crew for itself" mentality. At the same time, flood-response technology can enable and encourage personnel in the field to share important information with other deployed personnel and with a central headquarters.

Emerging Flood-Response Technologies

Recent floods have underscored the importance of communication and coordination in developing real-time responses. Fortunately, the technologies that are emerging are imminently capable of adding tremendous value on a number of fronts.

Pivotal flood-response technologies include:

- *Surveillance Technology* – Drones or unmanned aerial vehicles (UAVs) provide ground crews with an "eye in the sky" that allows them to gain a full picture

of the flooding, including which areas are most affected and where emergency responses may be required next. Underwater drones can also help responders examine infrastructure and coordinate rescue efforts in heavily flooded areas.

- *Flood Mapping Technology* – Flood forecast maps use remote sensors to determine which areas are most at risk of flooding based on elevation, proximity to bodies of water, and other topographical data. They can also be helpful in evaluating if and when to rebuild infrastructure after a natural disaster, as some areas may have become too dangerous to accommodate homes and businesses.
- *Connectivity Technology* – The most powerful tool available during a natural disaster is one that nearly everyone has access to: a smartphone. Quickly deployable cellular data communication platforms can help people stay in contact with their loved ones during floods. These networks can also help authorities communicate more easily with one another and with imperiled communities over social media.
- *Situational Awareness Technology* – Situational awareness platforms integrate discrete technologies, synthesize information streams, and activate data from UAVs, intelligent infrastructure, meteorological data, and more. Such integration helps responders build a COP, enabling crews on the ground to execute their critical responsibilities with far greater effectiveness.

A new generation of digital technologies is helping governments take decisive control over major flooding events. Perhaps the most important development in flood-response technology is the rise of situational awareness platforms. This technology enables decision-makers to effectively coordinate response efforts at a moment's notice, rather than executing strategies designed for dynamic situations that will almost certainly have changed by the time first responders arrive on the scene.

Integrating flood-response technologies and disaster response personnel into a situational awareness platform can make real-time coordination a reality, and help prioritize and distribute mission-critical information to the right people at the right time. It is even possible to leverage the power of crowdsourcing to pull citizen-generated data from social media and purpose-built public applications into a COP. Through the use of mobile data communication platforms, citizens are able to support the COP and receive vital information from government responders.

Ultimately, surveillance, connectivity, and situational awareness technologies have the potential to revolutionize how governments respond to major flooding events. By leveraging information in a more coordinated fashion and pulling from a wide array of assets across disaster-stricken areas, it is possible to develop responses that are better organized in turn – and save lives in the process.

John Dames is chief technology officer for Coolfire Solutions, a software company specializing in platform development and technology to deliver actionable intelligence. He has spent the past 8 years helping conceive and develop solutions for customers such as Enterprise Rent-A-Car, U.S. Military Special Forces, and municipal public safety and security teams.

Advancing Resilience – Building Codes & Benchmarking

By Ryan Colker

Communities are facing a wide variety of shocks and stresses. Whether it is a natural disaster threat (hurricane, earthquake, flood, wildfire), socioeconomic stressor (homelessness, poverty), or loss of a major employer, communities are looking for strategies to protect their citizens, tax base, and infrastructure (including buildings) from disaster. New tools and benchmarks provide the basis for developing these strategies.

Multiple community functions, including utilities, healthcare, and education, all contribute to a resilient community (see Figure 1). That is why the Alliance for National and Community Resilience (ANCR), a member of the International Code Council's family of companies, is developing tools and benchmarks that help communities understand how resilient they are and giving them tools to determine how to become more resilient. ANCR's approach focuses on 19 community functions identified by subject matter experts representing all aspects of a community.

A resilient community is one that can quickly and efficiently withstand, respond to, and recover from both shocks and stresses. Buildings are a fundamental community function that supports the resilience of almost all the other community functions. A community's key elements – whether its education, healthcare, culture, or commerce – ultimately require buildings to support their specific functions. For instance, resilient education systems demand resilient school buildings, just as resilient healthcare systems require resilient hospitals, and resilient water systems require resilient treatment plants and plumbing infrastructure. A community cannot be resilient without a strong focus on its buildings.

Fig. 1. Community functions identified by ANCR, 2019.

The Buildings Benchmark

Given the important role that buildings play, in January 2019, ANCR made buildings the focus of its first benchmark release. The

Buildings Benchmark is especially important, in part, because it is the foundation upon which subsequent benchmarks are constructed. The Buildings Benchmark is primarily grounded in building codes as the foundational strategy for achieving a resilient building stock. The benchmark includes nine criteria that go into making the benchmark a useful, well-rounded resource for lawmakers and policy makers. Those criteria are:

1. The adoption of current building codes;
2. Effective enforcement strategies, including human and financial resources;
3. Licensure and continuing education of contractors;
4. Identification and investment in vulnerable buildings;
5. Identification and mitigation of critical facilities such as fire stations, hospitals, etc.;
6. Encouragement of resilient design practices through programs that exceed minimum code requirements;
7. Engagement of the building industry and relevant departments in the community-wide Continuity of Operations Plan (COOP) development;
8. Assurance that emergency shelters meet or exceed relevant requirements and are regularly inspected; and
9. Availability and affordability of insurance.

Building codes have existed in some form or fashion since roughly 1754 B.C., when the Code of Hammurabi made constructing unsafe buildings punishable by death throughout the Babylonian Empire. Although some might argue that King Hammurabi was ahead of his time in terms of his commitment to safe buildings, his leadership around the issue was a bit extreme.

The penalties for violating building codes are much more reasonable these days, but the codes themselves are more important than ever. May 2019 marks the 39th anniversary of Building Safety Month, an annual international campaign started in 1980 by the International Code Council to promote and raise awareness about the importance of building safety. In the centuries since Hammurabi's reign, advances in building safety have been made across the board, and 2019 focuses on recognizing the importance of taking a community approach to building safety and the need for metrics that support that mission.

Despite being easily overlooked, building codes play a vital role in society. In addition to the obvious benefits, such as saving lives and keeping people safe, a 2019 study released by the National Institute of Building Sciences (NIBS) demonstrated that adoption of the most recent building codes can save $11 for every $1 invested. That accounts for hurricane, earthquake, flood, and wind damage mitigation, and increases community resilience.

Together, the nine criteria in the ANCR's Buildings Benchmark comprise the key requirements and regulations that support a resilient building stock, the foundation of a resilient community. Each of these nine requirements is then graded on a three-point scale, from "essential" to "enhanced" to "exceptional." The goal of this system is to help communities pinpoint exactly what their next steps should be. In other words, if a community is graded as having an "enhanced" level of enforcement strategies, it will be able to look at the benchmark to determine exactly what steps it needs to take to upgrade to "exceptional."

The benchmark includes nine criteria that go into making the benchmark a useful, well-rounded resource for lawmakers and policy makers.

Housing & Other Benchmarks

In the coming months, ANCR will be rolling out the rest of its benchmarks, with the Housing Benchmark centered around access and affordability set to be released this summer. Similar to the Building Benchmark, the Housing Benchmark recognizes the interconnectedness of community functions and its intersection with subsequent benchmarks. For instance, a lack of affordable and accessible housing stock for people to live in will lead to increased homelessness, which will negatively affect a community's healthcare resilience.

The goal of the Buildings Benchmark is to provide states, cities, and towns with the tools and information they need to evaluate their current resilience efforts and be able to strengthen their infrastructure, building stock, and community as a whole. Therefore, ANCR is celebrating 2019's Building Safety Month by encouraging communities to pilot the Building Benchmark and use these tools to improve the safety of everyone before a disaster inevitably strikes.

ANCR's goal is to create benchmarks across each of the 19 community functions to allow community leaders to have a complete picture of how to build a resilient community and enable them to evaluate the performance of various local government departments.

Ryan Colker is the vice president of innovation at the International Code Council, where he identifies emerging issues in the building industry, including how new technologies can be leveraged by codes and standards, methods to modernize the application of building regulations, and the development of new business strategies that support members and building safety professionals. He also serves as executive director of the Alliance for National and Community Resilience. Most recently, he was the vice president of the National Institute of Building Sciences, where he led the Institute's efforts to improve the built environment through collaboration of public and private sectors. Previously, he was the manager of Government Affairs at ASHRAE.

School Active Shooter Drills – From Anxiety to Apathy

By Robert C. Hutchinson

The Marjory Stoneman Douglas High School Public Safety Act (MSDHSPSA) was approved by the Florida governor on 9 March 2018. The act implemented numerous new, and at times controversial, laws and requirements for schools, law enforcement, mental health officials, and others. Included in the law was the new requirement for schools to conduct active shooter drills as often as other emergency drills. Since fire drills are usually conducted once a month, the new requirement greatly expanded the number of active shooter (or code red) drills from approximately one to approximately ten per school year in Florida schools.

This increase in active shooter drill training was likely overdue, but the extent of the expansion could be counterproductive. Anecdotal observations and discussions have raised great concerns that the expansion of these drills in such a short time period has created anxiety among many students and staff. It is feared that this initial anxiety shall transition into apathy over time with a possible 900% increase in active killer drills. A review of the frequently lackadaisical response of students to repeated fire drills demonstrates their fluctuating level of appreciation of the seriousness in the evacuations over time.

The National Association of School Psychologists (NASP) and National Association of School Resource Officers (NASRO) created guidance in December 2014 regarding the *Best Practice Considerations for School in Active Shooter and Other Armed Assailant Drills*. The guidance addressed numerous concerns and considerations to include that drills are critical but they can risk causing harm to students and staff. The appropriate number and design of active shooter or code red drills require additional research and analysis to best balance preparedness and impact on the participants.

Emergency Drills

The identification and classification of emergency drills can vary from state to state and school district to school district. The definition of a code red lockdown/drill and an active shooter/assailant lockdown/drill has created confusion at times for schools, first responders, and parents. In many locations, a code red lockdown/drill may include many immediate threats to include an active shooter. A code red lockdown may include an array of possible threats including a fleeing suspect or trespasser on campus to a noncompliant person on campus posing an immediate threat or possibility to evolve into one. Not all code reds/lockdowns involve an active shooter, but all active shooters would involve a code red lockdown or related response.

Beyond a code red, schools may utilize other emergency codes for various threats from an incident near the school campus to a threat on the campus that requires an evacuation in addition to fire drills. A code yellow lockdown may involve law enforcement activity near a school campus that could affect school operations and transition to the campus requiring a code red. The implementation of code yellow procedures also permits the school campus to better prepare for a code red if necessary by restricting movement and securing the campus.

Additional emergency codes can be utilized for evacuations, shelter-in-place, or other instructions for threats inside or outside school buildings or campuses to address a myriad of concerns. There continues to be discussions if emergency codes or plain language communications are more efficient and effective for an incident. Staff and students could confuse codes, but they could also misinterpret instructions that may differ in a time of evolving chaos.

NASP developed a brief guide for schools to mitigate the psychological effects of lockdowns. In this guide, NASP identified that "differentiating lockdowns can help to mitigate potentially traumatic experiences when situations are occurring in the community and are not an immediate threat to the school." The importance of working with first responders and outside partners is vital to ensure a common understanding of definitions, policies, and response plans to avoid confusion with different emergency codes or incidents.

Expansion of Drills

The MSDHSPSA amended Florida Statute 1006.07 regarding student discipline and school safety to include:

> *EMERGENCY DRILLS; EMERGENCY PROCEDURES – (a) Formulate and prescribe policies and procedures, in consultation with the appropriate public safety agencies, for emergency drills and for actual emergencies, including, but not limited to, fires, natural disasters, active shooter and hostage situations, and bomb threats, for all students and faculty at all the public schools of the district comprised of grades K-12. Drills for active shooter and hostage situations shall be conducted at least as often as other emergency drills. District school board policies shall include commonly used alarm system responses for specific types of emergencies and verification by each school that drills have been provided as required by law and fire protection codes. The emergency response policy shall identify the individuals responsible for contacting the primary emergency response agency and the emergency response agency that is responsible for notifying the school district for each type of emergency.*

The preparedness and psychological impact of the expansion of active shooter drills at the same frequency as fire drills in Florida is unknown this early in the MSDHSPSA implementation. Conducting an active shooter/emergency code drill and a fire drill each month in every school, no matter the grade level, shall likely have unintended consequences beyond the intentions of the new law for the pendulum has apparently swung from one extreme to the other. There is a need for additional information and guidance.

Federal Guidance

In 2007, the Government Accountability Office (GAO) issued a report entitled *Most School Districts Have Developed Emergency Management Plans, but Would Benefit From Additional Federal Guidance* (GAO-07-609). The report found that "most school districts have taken federally recommended steps to plan and prepare for emergencies, including the development of emergency management plans, but many plans do not include recommended practices."

Although the GAO report did not focus directly on drills, it estimated that 70% of all school districts struggled to balance their primary duties of education and emergency management

©iStock.com/Susan Vineyard

activities with the limited training time, opportunities, and resources. GAO stated that 73% of the surveyed schools conducted some type of drill or exercise to include evacuations, lockdowns, and shelter-in-place.

The report found that the federal government had a recommended practice to "conduct regular drills" to prepare for emergencies. The 2007 report repeatedly identified pandemic flu as a serious threat rather than an active shooter, an indicator of the greatest perceived threats at the time.

In 2016, a GAO report, entitled *Improved Federal Coordination Could Better Assist K-12 Schools Prepare for Emergencies* (GAO-16-144), found that an estimated 67% of surveyed districts conducted active shooter exercises. Officials from two districts interviewed by GAO believed that exercises can create anxiety with the school community, especially with younger children. The report, focusing on federal coordination, did not discuss the frequency of exercises and any possible impact. The GAO report concluded that "an existing federal interagency group on active shooters was not created to address the range of threats and hazards schools face, nor to be specific to schools' needs, which, given the presence of young children, can differ significantly from those of other institutions."

The Final Report of the Federal Commission on School Safety, issued in December 2018, found that "a robust training and exercise program is essen¬tial to successfully addressing the complex active shooter threat." The report stated that active shooter training should be age appropriate for the students and designed to not unduly traumatize the students and staff. The commission identified the following recommendation for the federal government:

> *In order to assist schools in deciding the optimal approach to preparing students for active shooter situations, federal agencies should work with school security stakeholders to identify and develop recommended, age-specific best practices or options for consideration for active shooter training and exercises for students spanning the K–12 spectrum.*

The commission identified the following recommendation for state and local communities:

> *All schools should conduct active shooter training and exercises for staff on a recurring basis as well as age-appropriate active shooter training for students. Exercises might include evaluations that assess the participant's ability to meet exercise objectives and capabilities, and document strengths, areas for improvement, core capability performance, and corrective actions in an After-*

Action Report or Improvement Plan. Following the exercise, organizations should develop a plan to implement the corrective actions identified during the exercise to improve plans, build and sustain capabilities, and maintain readiness.

The commission report identified the importance of training and exercise/drill design, but did not address the more specific topics of frequency and duration considerations.

NASP/NASRO Guidance

The NASP/NASRO document provides information and guidance for consideration when developing and conducting armed assailant drills at schools. As an overview, the document found:

- Response to armed assailants has focused on implementing a school lockdown. Recently, discussion has emphasized options-based approaches, which sometimes include the "Run, Hide, Fight" model.
- Armed assailant drills have both benefits and concerns associated with their implementation.
    - Armed assailants in schools account for only 1% of homicides among school-age youth; schools must balance costs and benefits when allocating crisis preparedness resources.
    - Such drills have the potential to empower staff and save lives, but without proper caution, they can risk causing harm to participants.
    - Available research supports the effectiveness of lockdown drills carried out according to best practices, but research is still needed on the effectiveness of armed assailant drills.

The NASP/NASRO document addresses numerous issues such as drill planning and keeping simulation techniques appropriate to the developmental maturity of the participants, a critical subject with the wide-range of students and staff throughout a school district.

The document finds that "regular practice helps participants develop readiness and quickly access and apply knowledge." However, the guidance does not mandate student participation in drills and permits staff to opt out for less intense instruction such as a tabletop exercise. The failure to train students and staff to a unified and common standard could create considerable confusion during an actual event. Regrettably, the cost of confusion and delay has been well documented during many critical events.

The document stresses that drills that include all students and staff have the potential for causing harm to them. According to the findings, "an individual's cognitive and developmental levels, personality, history of adverse or traumatic experiences, and psychological makeup are among the many factors that influence the potential for harm." Accepting the position regarding the potential for harm from NASP/NASRO, the question arises would a higher frequency of drills lessen or expand this possible harm. One of the most important findings of the document was that "at present there is no empirical research regarding school-based armed assailant drills."

Mitigating Psychological Effects

Active shooter training for staff that simulates an actual attack with blank gunfire, simulated bullets, and other tactics can provide a realistic environment to better prepare them to react, but may exacerbate psychological trauma. Understanding what gunshots would sound like echoing through a school building is a tremendously valuable lesson to reduce future reaction time, but there can be a real psychological cost for this training. However, stories of teachers being shot execution style with plastic pellets during active shooter training may require additional research and analysis to validate the benefits as compared to the costs.

The NASP brief guide for schools to mitigate psychological effects of lockdowns explains how schools have been involved in preparing for and responding to safety threats for decades, to include lockdown drills to secure schools from an immediate threat. The guide declares "however, depending on circumstances, some lockdowns may produce anxiety, stress, and traumatic symptoms in some students or staff, as well as loss of instructional time."

The NASP guidance provides enormously valuable information to better plan, prepare, and execute a drill or lockdown without discussion regarding frequency of execution. NASP believes that "armed assailant drills that are not conducted appropriately may cause physical and psychological harm to students and staff, not to mention disruption to the overall learning environment." Consequently, further research and consideration are required to determine if excessively conducted drills, appropriate in nature or not, could cause physical and psychological harm to students, staff, parents, and the general community.

Evidence-Based Guidance

Safety consultants can disagree on the value and design of active shooter training and drills that are not supported by evidence. The drill disagreements include the frequency of active shooter incidents as compared to other incidents on school campuses for the development of training and drills. The proponents of active shooter training and drills consistently stress the fact that required fire drills are regularly conducted and a life has not been lost in a school fire for many decades – something that cannot be said for active shooter attacks.

The popular ALICE (Alert-Lockdown-Inform-Counter-Evacuate) training program is utilized by numerous school districts and law enforcement agencies around the country. The program addresses many of the critical elements for active shooting training and lockdowns. However, the "counter" component to attack the armed assailant with objects as a last resort has not been a proven tactic. There is a concern by some school safety consultants that this training could also cause staff or students to leave a shelter location to confront an active shooter when they should not.

According to Steve Brock, a professor of school psychology at California State University, in a September 2017 *Education Week* article stated, "there's not enough research to support ALICE and similar training in schools." Brock supports lockdown drills without unnecessarily frightening students and staff with more elaborate training scenarios.

If the efficacy of active shooter training has not been adequately researched and could be harmful, it raises the question of why states across the nation have increased their mandatory drill requirements since the attacks at Sandy Hook Elementary School and Marjory Stoneman Douglas High School. According to Professor James Fox at Northeastern University in a September 2018 *Medium* article:

> *"Schools are in a difficult position," Fox says. "They feel that they should do something." Active shooter drills are a quick, understandable way to prepare for a school shooting, and law enforcement can conduct them in a couple hours on a Tuesday morning. The drills make people, particularly the lawmakers, administrators, and parents who don't have to endure them, feel safe, even if they're not making children much safer at all.*

Michael Dorn, executive director of Safe Havens International, has questioned the value of active shooter and other emergency training and drills without specific research and information to support their validity. In a 2014 *Emergency Management* article, Dorn said one of the reasons for his concern "is the heavy emphasis on the active shooter scenario, which ignores other threats, and that some of the training is not evidence-based and not proven to work, such as the *Run, Hide, Fight* video."

In addition to safety consultants and academics, some practitioners also question the harm created by active shooter drills. A number of educational professionals promote not conducting the active killer drills at all, even after so many school attacks. For example, Michael J. Maguire, a vice president of the American Federation of Teachers Massachusetts, advocates putting an end to the practice. Maguire believes that:

> *Halting active shooter drills does not mean we do nothing to protect students from the worst. Training teachers for emergency situations is prudent and inflicts no trauma upon children.*

Need for Further Research

Beyond the lack of abundant evidence-based research documenting the effectiveness of active shooter training and drills, the appropriate frequency and duration of these drills is even more unconfirmed by sufficient evidence-based research. The impact of the change in the frequency of active shooter drills requires additional research and discussion to assess the costs and benefits of a massive swing of the pendulum. Without this analysis, the actions of lawmakers and others may be causing more harm than good and not better preparing the nation's schools.

These good intentions need additional research and information to ensure that any massive increase in active shooter drills is truly beneficial for the participants and overall educational environment. No school or community shall benefit from their students and staff transitioning from anxiety to apathy on their campus due to a possibly excessive mandate of monthly active shooter drills. An evidence-based balance must be identified to properly prepare for an active shooter attack without creating additional harm along the way.

Robert C. Hutchinson was the chief of police for the Broward County Public Schools, Special Investigative Unit from 2016 to 2019. He was the former deputy special agent in charge and acting special agent in charge with the U.S. Department of Homeland Security (DHS), Homeland Security Investigations in Miami, Florida. He retired in 2016 after more than 28 years as a special agent with DHS and the legacy U.S. Customs Service. He was previously the deputy director and acting director for the agency's national emergency preparedness division and assistant director for its national firearms and tactical training division. His writings and presentations often address the important need for cooperation, coordination and collaboration between the fields of public health, emergency management and law enforcement. He received his graduate degrees at the University of Delaware in public administration and Naval Postgraduate School in homeland security studies.

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

PROENGIN

Chemical and Biological Detection Systems