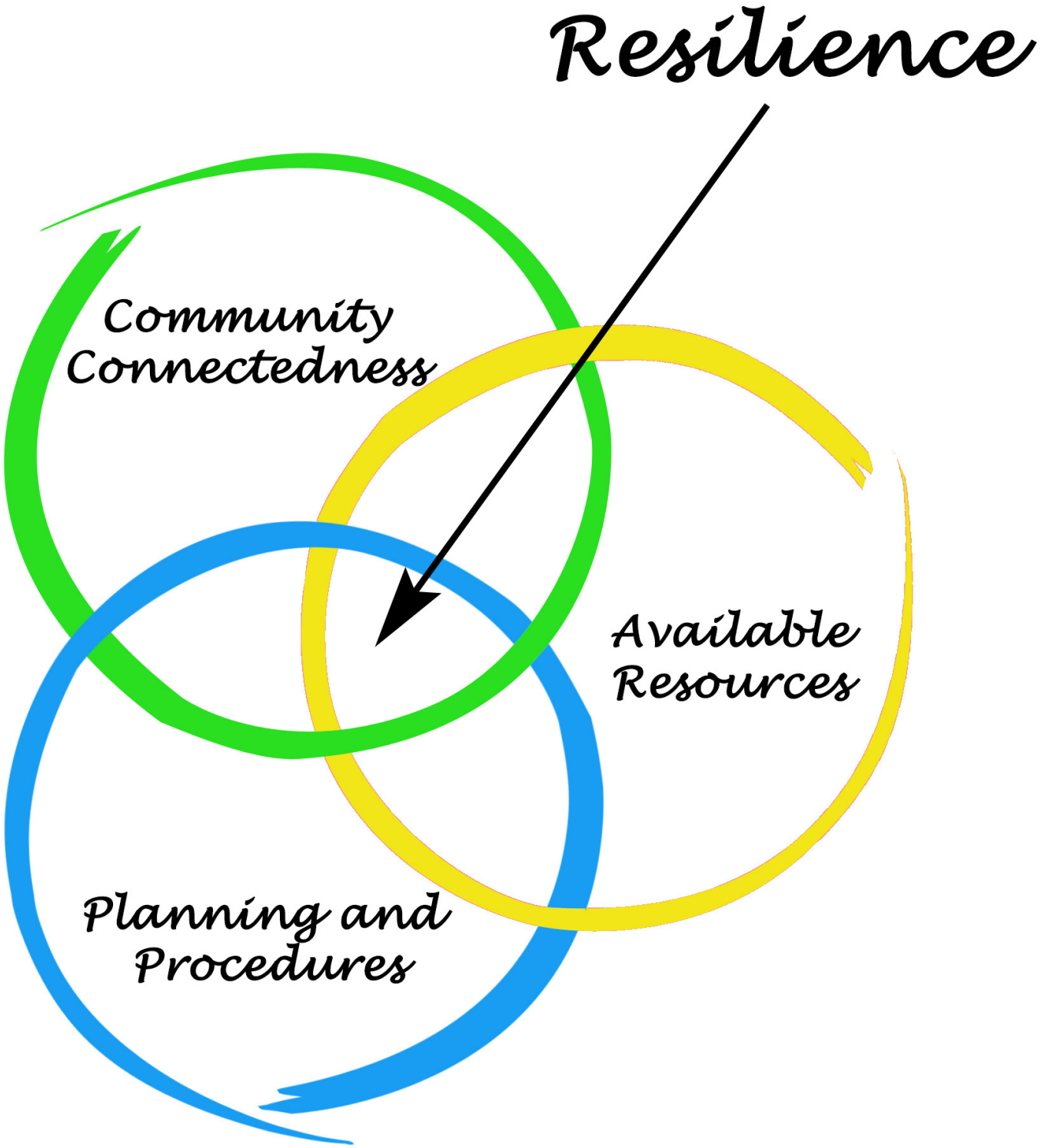
DomPrep Journal



Volume 17, Issue 12, December 2021

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

Business Office
1033 La Posada Drive
Suite 135
Austin, Texas 78752
www.DomesticPreparedness.com

Staff
Texas Division of Emergency Management
Publisher

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

Martin Masiuk
Founder & Publisher-Emeritus
mmasiuk@domprep.com

Advertisers in This Issue:

BioFire Defense

Dräger

Teledyne FLIR

PROENGIN Inc.

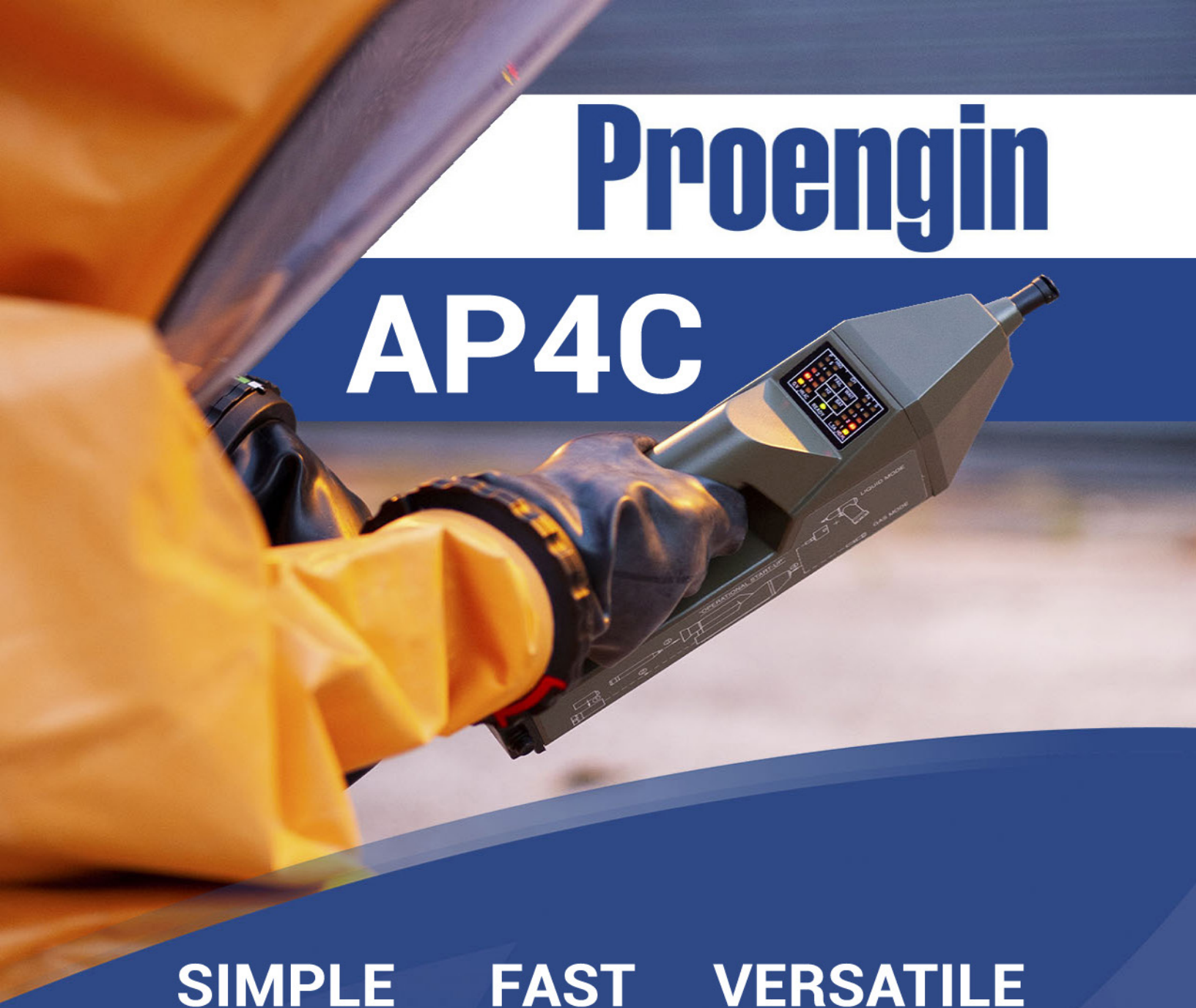
DomPrep Journal is electronically delivered by the Texas Division of Emergency Management, 1033 La Posada Drive, Suite 135, Austin, TX 78752, USA; email: subscriber@domprep.com.

Featured in This Issue

Pictured on the Cover: Source: ©iStock.com/vaeenma

Proengin

AP4C



SIMPLE FAST VERSATILE

Chemical weapons & NTAs

HAZMAT & Homemade agents

Quick response

Accurate & Precise

www.proengin.com

Resilience in 2022 – Planning, Resource & Connections

By Catherine L. Feinman

A quick search through articles on DomesticPreparedness.com for the word "resilience" reveals a possible shift in focus for preparedness professionals over the years. In 2005, the Domestic Preparedness Journal published many resilience articles that focused on creating standards and plans in order to more rapidly return to normalcy. By 2010, there seemed to be a greater focus on funding, grants, and other resources needed to be able to sustain operations when disasters occur. By 2015, education, communication, and collaboration were key buzz words in articles on resilience. Then 2020 arrived along with much reflection on what could have been done better to be resilient in the face of an unprecedented event and how to endure the consequences of past decisions.

The authors in this edition of the Domestic Preparedness Journal review past events while looking toward the future. Numerous disasters over the past two decades were book-ended with terrorist attacks on three U.S. cities that caused a nationwide shutdown and a worldwide pandemic with widespread shutdowns in most if not all countries. The 9/11 attacks in 2001 demonstrated a strong unity of effort, with many selfless heroes running into danger rather than away from it. That and other mega-disasters since then – for example, Hurricane Katrina in 2005, the 2010 Haiti earthquake, the Fukushima Daiichi nuclear disaster in 2011, and the 2021 Dixie fire, just to name a few – have tested the resiliency of communities around the world. By 2021, the unity of effort observed in the wake of 9/11 has waned as the world continues to recover from a worldwide pandemic.

However, with regard to resilience, it is necessary to address unfinished business and the future agenda. The first step is to review and update current plans or create new ones to address risks and threats in an everchanging environment. Then, identify critical resource needs and availability of those resources under adverse conditions. For example, recognize essential assets like global positioning system satelites and signals as high-priority targets for bad actors, and create a plan to protect them from interference or destruction. Transportation is another critical infrastructure that requires a greater awareness of threats and risks that could hinder operations and how to manage them to enhance resilience.

Over the years, the focus when preparing for disasters may have shifted at times between planning and procedures, available resources, and community connectedness. However, the nexus of all three of these is still resilience. In a post-9/11 and post-COVID-19 world, the goal of resilience needs to remain at the center of disaster preparedness efforts. As 2021 ends, the focus should be on the future – plan for the next mega-disaster, assess available resources, and build connections within and between key stakeholder groups. Simultaneously fortifying all three components will make communities much more resilient in 2022.

Resilience After 2021: Unfinished Business & Future Agenda

By Robert McCreight

In 2021, many questions have been raised about resilience. Is more known about resilience and have more leverage tools been retained to establish resilience at will than a decade ago? What ideas and notions were expected 10 years ago in energizing resilience tasks, activities, and operations? Has the leverage needed been acquired to apply proven strategies and operational systems for implementing post-disaster resilience with skill and confidence? Did a collective experience with mega-disasters since 2011 equip communities with new and innovative pathways to achieve resilience? The answers to these questions are far less than clear.

Often, a decade of hard-boiled experience with disasters elicits insights and ideas useful in confronting another head-on bout with a similar future catastrophe. However, that is not always true. More than 15 years after the colossal Hurricane Katrina event and 20 years after the 9/11 attacks, there is a need for serious reckoning with a complex operational challenge in emergency management – whether the next decade will require a fundamental rethinking, redefining, and reshaping of what resilience means. It is questionable whether communities can firmly retain, enshrine, or deftly abandon notions of resilience as understood during the past decade. Instead, they may be forced by the complex forces of explosive modernity, widespread cutting-edge technology, and the growing uncertainties of genuine vulnerability and risk to start all over again and redefine resilience anew. It may not be that simple. There are obvious and hidden manifestations to assess.

Looking at Four Basic Questions

An article published 10 years ago in the *Domestic Preparedness Journal*, "Attaining Resilience: Getting From Here to There," asked four questions:

1. What defines resilience?
2. What could the public and private sectors do to collaboratively attain resilience?
3. What metrics make sense to measure resilience?
4. What social technologies and interdisciplinary strategies would better capture resilience?

In many ways, after 10 years of experience and reflection, a mixed picture on those four points emerges. Looking back, it seems there was significant lip service to the ideals of resilience, but there is limited evidence it became an operational priority as other issues pushed it further back in the public agenda. One way of assessing the command of resilience activities as a counterweight to disaster is to gauge how well communities have done since 2011 in coping with calamity.

It is important to consider whether the United States has become more resilient since 2011, however it may be defined. There were numerous climate-related disasters, several major earthquakes, the Fukishima nuclear-tsunami mega disaster, Super Storm Sandy, the Ebola outbreak, Hurricane Maria shutting down Puerto Rico's economy, and recurrent California wildfires – just to name a few. As a proxy indicator of resilience, these disasters revealed a lack of resilience in terms of lengthy post-disaster returns to quiescent conditions and the underestimated and woeful recovery curve following a mega-disaster. In terms of a definitional lexicon flush with 2021 insight, there is still a need to look for the persuasive and impressive instances of being *robust*, to possess the ability both to *absorb disasters* and *bounce back*, and to determine whether it is possible to *restore order* and reactivate *key systems* as mentioned 10 years ago. In many cases, it seems the nation is far from where it should be.

The obvious conclusion derived from the past 10 years of disasters is that resilience may be different than originally imagined. It may entail other aspects, conditional factors, and contributing technologies than first anticipated. The hidden issues are still there, which too often entails creative formulas for defining and establishing infrastructure and community resilience in ways not readily grasped or supported. In some ways, the obvious and hidden remain a bit opaque when still struggling to discover and test methods, systems, and innovations that have not yet been proven or tested. There are a few obvious issues to explore that may offer a starting point.

Resilience Continues to Be What It Was Thought to Have Been

What is far less clear is whether traditional or classical notions of resilience still make sense given the way society will likely operate and function after 2021. Of course, with ongoing commercial and industrial activities as well as many aspects of the community infrastructure, the same package of risks, hazards, and vulnerabilities still exist. However, it is fair to ask whether the global pandemic experience, the onset of new and unique technologies, the steady expansion of urban areas proximate to coastlines, the involvement of greater cyber and artificial intelligence (AI)-enabled systems along with the inherent limitations of risk analysis and mitigation measures will be enough. Complex interconnected systems today where AI governs infrastructure, or where genomics and nanoscience steer medicine and public health in different ways, implies that the ability to engage in sophisticated risk management and mitigation analysis is less than ideal. Clearly the evidence is ambiguous at best:

- Is there an expectation that the core elements and definition of resilience will change?
- Does the last decade provide comfort that notions of resilience have been validated and confirmed?

Basic expectations about resilience – snapping back from crisis, adapting to disruptive change, absorbing the worst aspects of disaster, streamlining effective recovery, and rapidly restoring normal life – are all still there to haunt and motivate a better way forward. The advent of more advanced technology engrafted into government operations and

Flooding caused by Hurricane Katrina in the New Orleans area is visible from Air Force One as President Bush returned to Washington from Crawford Texas (*Source:* White House photo by Paul Morse, 31 August 2005).

infrastructure falls short of being transparent and understood. The question of whether communities got better at resilience in the last 10 years seems to be a simple yes-no question. However, the answer is not entirely clear. The approaches, strategies, tools, and technology applied in 2011 to create, build, and reinforce resilience were tested against calamity during the past decade. It is difficult to find a convincing answer about whether resilience efforts were adequate or lacking.

Public and Private Sectors – Two Sides of the Same Coin

Here the issue is somewhat simplified in terms of verifiable collaborative activity. There are solid indications many worthwhile efforts were undertaken during the past decade to forge practical partnerships in anticipation of disasters. Aside from any persuasive instances that reflect cooperative harmony on the impressive side of the ledger and looking at the 2011 National Academy of Sciences (NAS) report on public-private collaboration to achieve resilience, the NAS notes a few salient issues that became a key set of conclusions. NAS leadership noted several barriers to greater collaboration found in 2011 included private-public sector cultural differences, concerns about information sharing, and wariness of government mandates and regulations. Business and government executives lacked a common definition and approach to resilience. There were also several serious misunderstandings and mismatched expectations about what the business sector can do and what government has the capacity to do post-disaster. The NAS mentioned that, in addition to the economic and cultural limits among the population that inhibit regularized cooperation with business, there was a tendency to see the public as *customers* rather than partners. The NAS also found respective *turf* issues and sensitivities between business and government along with the absence of an agreed-upon set of vulnerability and resilience indicators that would make it possible to measure and assess them in communities and over time.

This does not mean there is little prospect for collaborative progress, but the mechanisms and strategies needed to establish a working relationship and trusted dialogue focused on solutions for the community seems to be elusive. In effect, it takes hard sustained work. Some communities have found a formula, but the overall architecture for sustained, uniform, nationwide, systematic public-private cooperation on mitigation, response, readiness, and recovery is far from where it should be as 2021 ends. The following questions remain:

- What is the stress-tested template for public-private collaboration in all phases of emergency management?

- What have effective public-private partnerships demonstrated thus far in terms of collaborative readiness, mitigation, response, recovery, and the pursuit of greater resilience?
- What lessons and insights have crossed the boundaries of both sectors and to what extent have the nongovernmental and faith-based organizations contributed to attaining better resilience?
- What lessons about resilience have been adopted by government since 2011?

The Task of Measuring Resilience – Determining How Much Is Enough

When academic and serious research materials are surveyed to discern resilience, there is a mixed picture with some common themes. Social scientists said resilience was the ability of a community to recover by means of its own energy and devotion. Others claimed community resilience was a process linking a myriad of adaptive capacities (such as social capital and economic development) to responses and changes after adverse events. It was seen as gradual capacity building. Engineers saw resilience in terms of restoring the essential parts of damaged critical infrastructure with focus on structural mitigation along with engineered robustness, redundancy, and resourcefulness. The front end of resilience was aggressive mitigation planning to harden vulnerable sites against a range of expected threats.

Expecting communities and critical infrastructure to remain unscathed and untouched by a Category 5 hurricane or an F4 tornado is unrealistic. However, the absolute level of material commercial and human damage could be reduced significantly by the application of innovative resilience measures, with systematic metrics providing a measuring scale. A bottom-line perspective can be applied using the case of Hurricane Katrina and Super Storm Sandy. Resilience can be seen as the explicit engineering of robust mitigation and risk-reduction measures that would significantly reduce the net damage and make post-disaster recovery much easier. However, it begs the question of what seeking "a significant reduction in damage" means: an amount like 25%; the post-disaster recovery curve for communities and businesses to shorten its length by 50%; or something else. This remains unclear and offers a solid opportunity for academic engineering departments to work with city planners and emergency management officials, together with commercial business continuity experts, to devise a resilience plan tied explicitly to a variety of high-probability disaster scenarios. In effect, this is collaborative anticipatory risk management in its simplest form. There is uncertainty whether this is already happening today but raises the question of how much better community and commercial resilience should be after 2021.

So, the challenge regarding resilience is in determining exactly how much is enough:

- If seeking a level of resilience 25-30% better than the last decade, can that be defined and measured?
- Can specific steps be identified that would cause the reduction in damages and injuries?
- If defaulting to a position of stopping a disaster's worst effects from getting even more destructive, is that a valid resilience goal?

- What about ambitious resilience goals and objectives devised by public-private partners that aim to build resilience to measurable levels of robust community and commercial resistance to disasters at levels never seen before?

Finding Social Technologies and Interdisciplinary Strategies That Make Sense

In many cases, this aspect of resilience is the toughest challenge because one size does not fit all. In other words, urban versus rural resilience contains important differences. Seaside and frontier plains environments are different enough to suggest a resilience strategy must be adjusted accordingly. Then there is the question of shifting variables. Some communities are resource rich or have ready access to innovative technologies not available to all communities nationwide. Some communities have orchestrated effective public-private partnerships to tackle resilience issues while others are miles away from that kind of arrangement. Then there is the opaque variable of state and federal support, which targets investments to further deepen avenues and ideas promising greater resilience. Questions to ask include:

- Have investments been sustained, well-funded, omnipresent, or even offered to communities willing to engage in unique resilience ventures?
- How has robust well-funded external investment in resilience by states and federal government helped or hurt resilience plans and ideas?
- Can it be determined where prototype resilience projects have been effective or ineffective?

Apart from these considerations is the sheer breadth of targeted infrastructural resilience itself – including resilience research, funding, and incubation of ideas involving the energy, emergency health, agriculture, or communications sectors:

- Is there evidence this has been systematically nurtured or funded since 2011?
- What innovative resilience projects drafted by public-private partners have been launched and sustained since 2011?
- What new projects are proving to be effective in 2021?
- Has government derived metrics to determine when true community and commercial resilience is established and sustained?
- Is the landscape of post-disaster damage continually be looked over and the losses and injuries tabulated?

There is a palpable need to do much better at resilience than the past 10 years have shown. More must be identified and discerned about the specific strategies and formulations of genuine resilience where – at a minimum – losses and injuries are reduced in measurable ways. A 25% reduction in losses and injuries given the same disaster situation may not be a realistic metric. Those who subscribe to the notion that all disasters are essentially the same get one answer. However, those who believe all subsequent disasters are inherently different get another outcome.

Undoubtedly, communities will confront disasters similar to those encountered during the past decade. However, from 2021 onward, there must be a capacity to discern what resilience looks like, including:

- During crises that far exceed anything seen before (e.g., for maximum-of-maximum disasters);

- When calibrated operationally for disasters of lesser magnitude and effect; or
- When answers are in hand vs. needing to obtain further research.

Over a decade ago, I wrote about this perplexing issue in an academic journal:

> *One sterling revelation from these disasters, and any like them, is that existing mitigation is never enough and major disasters tend to leave the victims feeling defeated. Worse, we recognize that emergency response is one thing, and post-disaster recovery is another. In the midst of clearing rubble, removing bodies, bulldozing collapsed buildings, establishing expedient shelters, and restoring elements of power and communications we discover that recovery is a lot tougher than is ever expected.*

Back then, I claimed that resilience must be understood to embrace far more than smart mitigation practices, robust emergency response, and effective recovery operations. It must be understood in terms of the actual post-disaster situation which a city, state, or region wants to achieve within one week (or a few weeks) after the crisis is over. It means painting a realistic picture of what is required for much more than mere community survival. It must also depict what a fully restored community with essential minimums looks like.

After a decade of disasters, it is less clear whether traditional notions of resilience still make sense given the way society will likely operate and function post-2021.

In addition, recovery must be studied more intently to learn from it what is required and expected. Only then will it be possible to grasp the real difference between resilience and recovery. Firmly, there must be a reckoning with the prospect that searching for concrete elements of resilience will go far beyond the conventional four-part paradigm that has shaped emergency and disaster management. In grasping what recovery means in operational terms, there is automatically a compulsion to tackle what resilience requires: redundancy in key systems; devising coherent and measurable resilience factors and indicators; and building and validating the art of the possible with public-private partnerships.

The final question is whether communities have learned enough about resilience from the past decade to have viable strategies for greater resilience in the next. If that appears to be true, it is inspiring. If not, it is sobering indeed.

Dr. Robert McCreight has over 35 years of experience in the U.S. State Department working in such major fields as global security, arms control, intelligence operations, biowarfare, nuclear weaponry, counterterrorism, emergency humanitarian missions, and political-military affairs. He served concurrently for 27 years in the U.S. military – primarily in intelligence, psychological operations, civil affairs, and logistics. His teaching areas of expertise include counterterrorism analysis, homeland security, regional security, and treaty verification. He has written a number of articles for the Journal of Homeland Security and Emergency Management, the Strategic Studies Quarterly and the International Journal of Homeland Security on homeland security, emergency management, and national defense subjects and is an adjunct professor in the graduate programs of both the University of Nevada and The George Washington University.

Domestic Preparedness in a Post-COVID-19 World

By Nathan DiPillo

Traditional definitions of domestic preparedness have been influenced by the Cold War and international terrorism. As the 20-year milestone of the 9/11 attack on the United States passed, domestic terrorism also has made its mark on the interpretation of domestic preparedness. It is time for a fresh look, considering pandemics, local human-caused and natural catastrophes, reoccurring threats (like wildfires, earthquakes, and cyberattacks), and crumbling domestic infrastructure. The landscape of emergency response actions and readiness of public and private agencies in a globally interconnected world has left a deep scar on domestic preparedness and how risk is evaluated both nationally and internationally.

Preparedness theater verses true preparedness is difficult to define and plan for. With emerging cyberattacks and the barrage of social media appetites, there are many threat vectors seeking to delay response actions, disrupt communications, and confuse agency priorities. Federal, state, and local emergency operation centers are scrambling to prioritize funds and resources and react to incidents. Local, regional, and state agencies must determine how to prioritize multiple emergencies simultaneously while dealing with internal emergencies – like employee shortages, slow or delayed supplies, power outages, and a remote staff.

Prioritizing Preparedness

In the New vision for the Environment and Surface Transportation in American Act or the INVEST in America Act, "The purpose of the prioritization process pilot program shall be to support data-driven approaches to planning that, on completion, can be evaluated for public benefit." The global pandemic has highlighted how important preparedness is in supply chain management, data sharing, infrastructure, and effective management of regional lifeline systems, which is why the federal government has decided to spend almost $555 billion dollars on it. The prioritization process or risk matrix of incident management in this post-pandemic culture has been impacted for the better. Lessons learned and best practices will be reviewed for years by emergency mangers and academia. Government agencies and nongovernmental organizations will have to adapt to the changing landscape of preparedness, when addressing multi-vectored threats. It is time to refresh standards and training in domestic preparedness strategies and policies and review risk as a connected and interconnected matrix blended with public- and private-driven agendas.

One of the most important lessons learned during this pandemic is how connected public and private partnerships have become, domestically and globally. Pandemic preparedness is not a new concept, but many new realities have emerged influencing preparedness actions across all public and private sectors. The 35th president, John F. Kennedy stated in 1961, "And so, my fellow Americans: ask not what your country can do for you – ask what you can do for your country." Although this is one of the most famous

political speeches in U.S. history, there is another quote in the same speech that better defines the role of the public private partnership, "In your hands, my fellow citizens, more than in mine, will rest the final success or failure of our course." Ingenuity of private enterprise balanced with consistency in response of government is the backbone of the emergency management industry's ability to be resilient when preparing and responding to catastrophes.

Domestic preparedness is a mindset that equates to transferring ability into capability with consistent measures of success and failure. Now more than ever, the impact and importance the private industry has on domestic preparedness and the cascading impacts on supply chain disruptions, critical infrastructure, staffing, and resources along with other factions of response and preparedness activities are even more paramount. Initial planning and response stems from the micro community levels. Cooperation between profit-driven and policy-driven enterprises before an incident is paramount when identifying and sustaining lifeline systems. Impacts from this pandemic have emphasized many realities never seen in U.S. history. Rob Schnepp said it well in the Domestic Preparedness Journal:

©iStock.com/Jennifer_Miranda

> *This leads to the question about what exactly the nation should prepare for. Preparedness is a complex proposition because it is an exercise in forecasting and trying to predict the future and what to do about it.*

This can be defined as the "IF/SO then WHAT" statement to identify the cascading effects or impacts if critical infrastructure were to fail.

Asking the Right Questions

These "what if" questions are driving local and global preparedness inequities and stressing emergency management agencies across the nation, which pushes risk boundaries. Viewing preparedness as a relevant consistent holistic network of local, regional, and national partnership is now the reality. With the implementation of 5th generation mobile network (5G) and, with it, the ability to quickly transfer terabits of data across vast distances, how lifeline systems are managed will be radically impacted. Business analytics will take on new importance and relevance in continued observation of workflow process.

One example is how California manages energy loads. Senate Bill 49 was introduced to combat the stress on California's electrical system. The bill states:

> *[T]he Energy Commission to adopt, by regulation, and periodically update, standards for appliances to facilitate the deployment of flexible demand*

technologies, as specified, and would require that those standards be cost effective and prioritize appliances with specified attributes.

Preparing for a statewide energy shortage is no small feat. This bill is intended to connect thousands of personal use appliances to a secure cloud environment, and then monitor usage to avoid possible energy blackouts. All this must be done while protecting privacy or other critical infrastructure information. The next step defined in the bill will be to connect larger more energy-thirsty infrastructure to the cloud, which can have drastic impacts if not protected properly. This is just one piece of the holistic approach to preparedness and risk management that is pushing the boundaries of domestic preparedness definition.

Emergency managers across the nation ought to re-examine limitations of the preparedness industry and risk resilience. Although some concepts are not new, dependency on the public and private sectors both national and internationally will be paramount as industries experience new vulnerabilities and impacts from additional catastrophic events, highlighting months to possible years of delays in domestic supply chain(s). These events include aging and crumbling infrastructure, increased dependency on a just-in-time supply chain, as well as human-caused and natural disasters.

The mindset of preparedness equates transferring ability into capability with consistent measures of success and failure.

Developing a New Vision

The preparedness mindset begins with interdependency between micro-level communities and macro-level communities. Impacts will be both in the physical and cyber spaces. COVID-19 has emphasized this vulnerability in planning efforts and should be highlighted within the preparedness stage of emergency management. Social media and the hunger for accountability will drive responsibility for government agencies to prepare for domestic emergencies with a nexus to global interdependency.

As with climate-related threats, pandemic recovery operations, and emerging cyberthreats, imagine what the next event impacting the domestic homeland might be. The current characterization and definition of domestic preparedness has been punished by this pandemic. Policy-driven and profit-driven agencies have been stretched to the maximum. It is time to push the boundaries of domestic preparedness and review current strategies in how industries and municipalities communicate and identify roles and responsibilities. Developing a new vision of domestic preparedness, in anticipation of the next big catastrophe, might be the next important trend in national risk resiliency.

Nathan DiPillo currently serves with the California Office of Emergency Services as a Critical Infrastructure Analyst in the State Threat Assessment Center. Prior to state service, he functioned as a Critical Infrastructure Specialist with the Department of Homeland Security and has 25+ years in the emergency management and security industry. In addition, he served as a non-commission officer (E7) with the California State Military Department, Army National Guard with the 223rd Training Command. He continues to champion the public and private partnerships. He received a Master of Emergency Management/Homeland Security MSEMHS focused on Domestic Security Management and Leadership from National University.

Dräger

Looking for American-made N95 respirators?

MADE IN ★ USA ★ SINCE SEPTEMBER 3, 2020

With a new plant in the USA, Dräger has you covered

For ground personnel working in dusty environments, respiratory protection is essential. The Dräger X-plore® 1750 N95, our next-generation particulate filtering facepiece respirator, offers distinct improvements in comfort and protection. And it's now made right here in the US.

FOR MORE INFORMATION VISIT WWW.DRAEGER.COM

Dräger. Technology for Life®

Protecting GPS Satellites, Signals, and America

By Domestic Preparedness Journal and
The Resilient Navigation & Timing Foundation

On 17 November 2021, the Domestic Preparedness Journal and the Resilient Navigation & Timing Foundation hosted a panel discussion on the vulnerabilities of the global positioning systems (GPS) and potential efforts to deter attacks on and interference with GPS satellites and signals.

The Honorable John Garamendi, Congressman for the 3rd District of California and Chair of the House Armed Services Readiness Subcommittee, provided an introduction. Dana A. Goward, President of Resilient Navigation and Timing Foundation, and David Olive, Principal at Catalyst Partners LLC, moderated the discussion.

The panel included:

- Dr. Scott Pace, Director of George Washington University's Space Studies Institute and Former Executive Secretary at the U.S. Space Council
- George Beebe, Vice President for Studies at the Center for the National Interest and author of "The Russia Trap"
- Greg Winfree, Director of the Texas Transportation Institute and Former Assistant Secretary of U.S. Department of Transportation

Essential Asset, High-Priority Target

GPS is essential to the nation's economy, safety, and security. Its positioning, navigation, and timing (PNT) services have been integrated into so many critical applications and infrastructure that many homeland security officials have called it a *single point of failure for critical infrastructure*.

This integration makes GPS a high-priority target for non-state and nation state adversaries. Government reports released this summer have discussed serious and growing threats to all U.S. space assets from Chinese and Russian anti-satellite weapons. "Kamikaze," "Russian Doll," and "Kidnapper" satellites, as well as terrestrial lasers, have all been added to ongoing concerns about signal jamming and spoofing.

Increasing the threat to the United States are terrestrial Chinese, Russian, and Iranian systems that provide their populations' GPS-like services making those nations less vulnerable to disruption of space-based services. This has created a technology resilience gap, a strategic asymmetry that could easily lead to an escalating series of responses and armed conflict.

What the Panelists Say About GPS Vulnerabilities and Solutions

Despite being an integral part of daily life, GPS is vulnerable to numerous threats. All critical infrastructures are in some way dependent on GPS – some much more so than others. GPS signals are weak and easy to disrupt. Numerous intentional and unintentional activities can have devastating effects, including but not limited to the following: denial of service, intentional wide area jamming, spoofing, environmental threats, solar activity such as coronal mass ejections, anti-satellite lasers, kinetic threats, accidental satellite damage, and degradation.

Building resilience is the way to combat these various threats and protect GPS systems and the timing signal. For example, a terrestrial-based navigation system (e.g., eLoran systems) could provide a solution because satellite systems (high-frequency, low power) are more vulnerable to spoofing than eLoran (low-frequency, high power). Although diversity in systems and having an alternative source for GPS are key to resilience, the limiting factor is the ability of the nation to build systems fast enough and at scale to outpace the threats.

Of course, it is not only a question of what needs to be done, but who should do it – the public or the private sector. It can be problematic trying to separate the civilian and military responsibilities because any private-sector threat can become a national security concern. In many cases, it is necessary for industry to work with government to reach common goals. Private sector industries can generally innovate at a faster pace but may lack the resources. The federal government may have the resources but moves slowly.

Panelists Answer Additional Questions

The 60-minute panel discussion share a lot of information from subject matter experts on protecting global positioning systems and building national resilience. However, not all the questions could be addressed in that timeframe. Below are additional questions that were submitted by participants and answered by the experts.

Question 1:

> *Which three sectors are not using GPS as stated by Greg Winfree?*

Answer from Greg Winfree:

> *Great question, and thanks for asking! As we discussed on the panel, it is hard to imagine any critical infrastructure not using some service from GPS, and they all do.*
>
> *At one time the Department of Homeland Security (DHS) determined that the National Monuments and Icons, Water and Wastewater Sector, and*

Agriculture and Food critical infrastructure sectors did not use GPS timing. We now know that is not true. GPS timing enables wireless networks and SCADA systems which enable a wide variety of services for all those sectors. GPS is especially important in precision farming, as I mentioned.

So, an old soundbite that I won't use again! Thanks for making me take a look at it!

Question 2:

If the U.S. were to commit to building a terrestrial alternative to GPS (covering both military and civilian uses), how long might that take?

Answer from Dana Goward:

It depends upon how the U.S. went about it. If the administration decided to build a government owned and operated system, it would likely take eight to twelve years as discussed on the panel. Not only would money have to be appropriated, but the responsible department would have to create a major systems acquisition staff and follow an extensive set of formal procedures.

On the other hand, there are numerous mature technologies available today from commercial entities that could provide services to complement and backup GPS. If the government decided to contract for these services, it could take only two or three years for the funding to be approved, contracts to be let, and to have the services up and running.

Question 3:

What other ground-based location systems are there besides LORAN?

Answer from Dana Goward:

There are a number of mature technologies that are available. In January, the Department of Transportation reported to Congress on a demonstration of some of these. That report is available here. The demonstration was not all inclusive, though, and other systems are in operation and more are being developed. As examples, two of RNT Foundation's corporate supporters, Locata and iPosi, did not participate in the demonstrations.

These systems vary greatly in what they do and how they do it. Some provide location only, some timing only, and others provide both. Some provide highly precise information over limited areas, some are slightly less precise but cover much larger areas.

The RNT Foundation recently published a white paper discussing requirements and evaluation criteria for timing services the government might be interested in as ways to complement and backup GPS. This paper also that also applies to location services and is available here.

Question 4:

What are the pluses and minuses to e-Loran?

Answer from Dana Goward:

Every system has its pluses and minuses. Here are a few for eLoran.

Pluses:

- *Signal – eLoran uses a powerful, difficult to disrupt signal at least a million times stronger than GPS. The navigation and timing signal can also carry additional information. As a new build, it could incorporate all the most modern encryption, authentication, and cyber protocols.*
- *Cost & Coverage – The effective range of transmissions can be a "continental" system as transmitter ranges are 800 to 1,000 miles radius over land and 1,500 miles over water. This means less infrastructure and expense per area covered compared to many other systems. The Air Force developed deployable versions of Loran in the 1960s and 1970s that they and the Coast Guard installed and operated in the United States, Vietnam, and Italy. So, conceivably coverage could be established wherever it was needed.*
- *Transmission Site Maintenance and Security – Hardware on Earth can be more easily maintained and upgraded. Technology serving the homeland would be on sovereign U.S. territory and added physical security could be easily implemented if deemed necessary.*
- *International Issues – Other nations, some friendly, some not, operate eLoran, or its equivalent. Having a U.S. system would make us more knowledgeable about other nations' capabilities. This could also be the basis for apolitical international cooperation.*

Minuses:

- Accuracy – GPS accuracy, depending upon conditions and receiver quality, is o*ften around two feet. Some terrestrial systems can achieve centimeter accuracy. eLoran, in its current configuration, has only been demonstrated to an accuracy of 15 to 30 feet.*
- *Coverage – At the current state of the technology, it cannot provide global coverage. Land-based Loran coverage can only serve land masses and ocean areas within about 1,500 miles of land.*
- *Existing Infrastructure – While the federal government still owns most of the former Loran sites within the U.S., most of the towers have been taken down or* are no longer serviceable.

Click here to watch this 60-minute panel discussion on protecting global positioning systems and building national resilience.

Transportation Security in a Holistic Homeland Security Enterprise

By Daniel Rector

Transportation security is the act of ensuring the protection and continued functioning of mobility systems for both people and commerce. It includes air, maritime, and all forms of surface transport. Transportation security is an enormous undertaking involving all government levels, the private sector, volunteer organizations, and the public. These organizations must work together to identify, prepare for, and respond to any threats or hazards that could affect the transportation infrastructure or the people and goods that travel within it.

In the United States, transportation security is a neverending and constantly evolving mission. The U.S. Department of Homeland Security (DHS) outlines the transportation security strategy of the United States in its 2020 Biennial National Strategy for Transportation Security Report. In the that report, DHS outlined four overarching guiding principles to develop and implement the strategy.

The first principle was to maintain an agile and adaptable security posture. The agency sought to accomplish this by relying on intelligence analysis and through the completion of regular risk assessments. The goal is to move into a prevention mindset rather than maintaining a reactionary posture.

The second principle was to highlight the importance of partnerships. Since much of the transportation infrastructure is maintained and operated by private companies, DHS recognizes the need to work in unison with the entire community to increase transportation security.

The third principle is to ensure privacy and civil rights are protected and maintained as transportation security is improved. Government agencies must not overstep their authority or violate the freedoms of citizens within the country while attempting to improve safety.

The fourth principle stated in the report was accountability. The agency recognizes that DHS, its private partners, along with local and state law enforcement organizations, are all accountable to the public. The organization acknowledges that it is the government's responsibility to maintain open communication with all interested parties and report on project progress.

Transportation Security Goals

Based on the above principles, the 2020 Biennial Report outlined the following three specific goals of the strategy:

- Manage risks to transportation systems from terrorist attacks and enhance system resilience.

- Enhance effective domain awareness of transportation systems and threats.
- Safeguard privacy, civil rights, civil liberties, and the freedom of movement of people and commerce.

DHS used these goals to develop security plans for the aviation, intermodal, maritime, and surface transportation sectors. The security plans for each industry are included as appendixes within the 2020 Biennial Report. Further, the report outlines a path forward through six areas of opportunity:

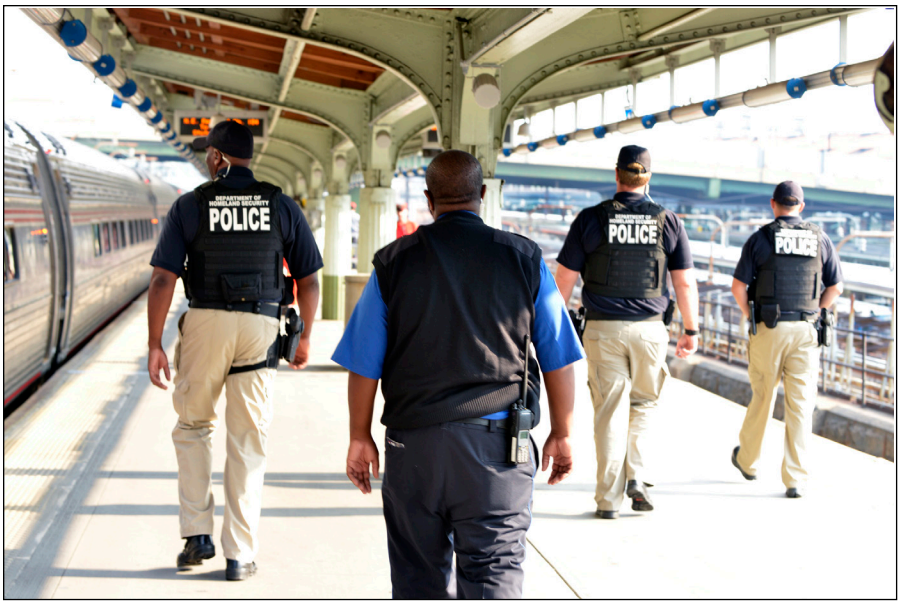
Key transportation security goals include building awareness of and managing risks, enhancing resilience, safeguarding privacy and civil rights.

- Increase risk-based assessments, which form the basis for all future planning and response operations.
- More effectively share information among partner organizations and continually develop more efficient and effective intelligence platforms and products.
- Increase and more effectively utilize security exercises. Exercises are the best way to train and prepare for any threats identified during a risk assessment.
- Create a better understanding of supply chain resilience.
- Create a better understanding of cyber system vulnerabilities.
- More effectively use research and development initiatives to improve security and drive technological investments.

Successful execution of a transportation security strategy within such a large country involves the cooperation and coordination between many partners at the local, state, and federal level. Two lead agencies in this effort are the Transportation Security Agency (TSA) and the U.S. Customs and Border Protection (CBP). Both organizations are components of the Department of Homeland Security. TSA and CBP must collaborate with all transportation stakeholders in the aviation, mass transit, highway transportation, railway, pipeline transportation, intelligence, and law enforcement sectors to ensure the security of the people and cargo that utilize the transportation infrastructure of the United States.

Transportation Security Agency

Established following the 9/11 attacks, the mission of TSA is to "strengthen the security of the nation's transportation systems while ensuring the freedom of movement for people and commerce." The agency is tasked with screening 100% of cargo coming into and moving within the United States. Additionally, the organization scrutinizes every passenger attempting to board flights within, or headed to, the country. TSA conducts its mission through a multi-layered approach. The most visible of which are the checkpoints passengers pass through at airports. Beyond the public-facing actions of airport checkpoints, TSA also conducts intelligence gathering activities, random searches of planes and airport facilities with canines and other detection equipment, and passenger manifest screening.



DHS and TSA work with Amtrak and law enforcement partners to keep the passenger rail system safe (*Source:* Barry Bahler, 3 September 2015).

TSA personnel also work as federal air marshalls and flight deck officers. These individuals have the legal authority to enforce U.S. laws and defend aircraft from attempted takeover. Since TSA does not conduct passenger screening outside the United States, the agency does require all airports that are last points of departure to the United States to uphold stringent security standards.

Although the Transportation Security Agency is most commonly associated with the aviation sector, the agency also works to safeguard surface transportation. TSA uses its intelligence and analysis capabilities to assist partners with conducting risk assessments across mass transit and rail transportation systems. TSA also operates with various law enforcement partners to increase the security of railways. TSA is one of several agencies part of Operation RAILSAFE. The operation aims to plan and exercise incident response, counterterrorism, and other security capabilities through random inspections of passengers and baggage, explosive screening by both canines and detection equipment, and increased security patrols on trains, at rail stations, and along railway right-of-ways.

Customs and Border Protection

The CBP's mission is to protect the American people by securing the country's borders and ensuring the lawful movement of goods. Aside from the border patrol duties that the agency is most known for, CBP also is responsible for monitoring the vast amount of cargo arriving at land and seaports. According to CBP, each year, over 11 million containers arrive at the nation's seaports, 11 million travel across land borders by truck, and 2.7 million travel by rail.

Much like TSA, CBP uses a multi-layered approach to ensure the safety of the American public. One of these layers is the Customs Trade Partnership Against Terrorism (CTPAT) program. Through this program, CBP partners with international supply chain stakeholders. The partners include foreign governments, importers, manufacturers, and others. When these organizations agree to partner with CBP, both parties work together to identify security gaps, share intelligence information, and implement measures to improve the safety of supply chains.

CBP has implemented another layer of protection through the Container Security Initiative (CSI). CSI was established in the months following the September 11 attacks in

2001. The program works to identify potentially dangerous containers originating outside the United States and intercept them on foreign soil before posing a threat to the country. CBP has a team of agents operating in foreign ports authorized to intercept and inspect suspected containers before they are loaded onto ships heading to the United States.

Strategy Improvement Recommendation

A previous *Domestic Preparedness Journal* article proposed a change to DHS that would result in a holistic homeland security enterprise. The change was recommended due to how the DHS was established and organized. Transportation security is one area where DHS's haphazard establishment has resulted in a crossover of mission areas and a lack of continuity between organizations.

Part of that recommendation was to reorganize the entire Department of Homeland Security. The reorganization would resemble the structure of the Department of Defense (DOD), where each service has an Office of the Chief of Staff as the leadership center. To achieve this reorganization, DHS could restructure its many component agencies to fall under specific offices according to mission set and primary function.

As part of the proposed holistic homeland security enterprise, the TSA would fall under the "Chief of Border Security" office along with CBP. The change would simplify the mission set of the subordinate organizations and increase communication speed and simplicity. By bringing both of these agencies under the same leadership umbrella, all policy and strategies concerning transportation security would be directed to a single point rather than across multiple departments, agencies, and components of DHS.

The Solution – Restructure

Within the United States, the TSA and the CBP each play a prominent role in transportation security. They work together with other DHS components, state and local governments, and private sector partners to share intelligence, plan, and respond to threats on the nation's transportation infrastructure. One difficulty these organizations face is the current organizational structure of DHS, which makes it difficult to share information. A solution to this problem lies in restructuring the DHS organizational chart to one more similar to the Department of Defense, with chiefs taking the lead of each mission set. If the United States wishes to continue to improve transportation security with a practical and evolving strategy, then a reorganization of DHS could be a critical step.

Daniel Rector, MS, CEM, is a military veteran with 12+ years of experience in homeland security and emergency management operations. He served as a damage controlman in the U.S. Coast Guard and as a survey team chief on a National Guard Weapons of Mass Destruction – Civil Support Team. His career is supported by a Master of Science degree in Emergency Management and current coursework toward a Doctorate of Management with a Homeland Security focus. He has completed multiple courses in CBRN response and detection from the Defense Nuclear Weapons School, Idaho National Laboratory, Dugway Proving Grounds, the U.S. Army CBRN School, and the U.S. Army CCDC Chemical Biological Center, among others. He has completed the FEMA Professional Development Series and the Homeland Security Exercise and Evaluation Program (HSEEP) Course. He is a Certified Emergency Manager (CEM), a licensed HAZMAT echnician, Confined Space Rescue Technician I/II, and EMT-B. He is a recipient of multiple awards for excellence, including being the only National Guard soldier ever named the Distinguished Honor Graduate while simultaneously being nominated by his peers for the Leadership Award at the CBRN Advanced Leaders Course.

Running Into Danger – Firsthand Accounts of 9/11

By Catherine L. Feinman

This year marked the 20th anniversary of the 9/11 attacks. Many events were held to commemorate the lives that were lost and to honor those who survived yet still ran into the danger zones to save lives in New York, Pennsylvania, and Washington, DC. However, one special event hosted in Washington, DC on 30 September 2021 was particularly impactful as it recounted that fateful day through firsthand accounts. Some presenters have told their stories many times over the years while others shared their heroic actions publicly for the first time in two decades. The District of Columbia's 2021 Interoperability Summit "20 Year Anniversary of the September 11, 2001 Attack on America: Never Forget," was organized by the District of Columbia Homeland Security and Emergency Management Agency's (HSEMA) Office of the Statewide Interoperability Coordinator (SWIC), in conjunction with the Metropolitan Washington Council of Governments (MWCOG) and the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency's (CISA) Emergency Communications Division (ECD).

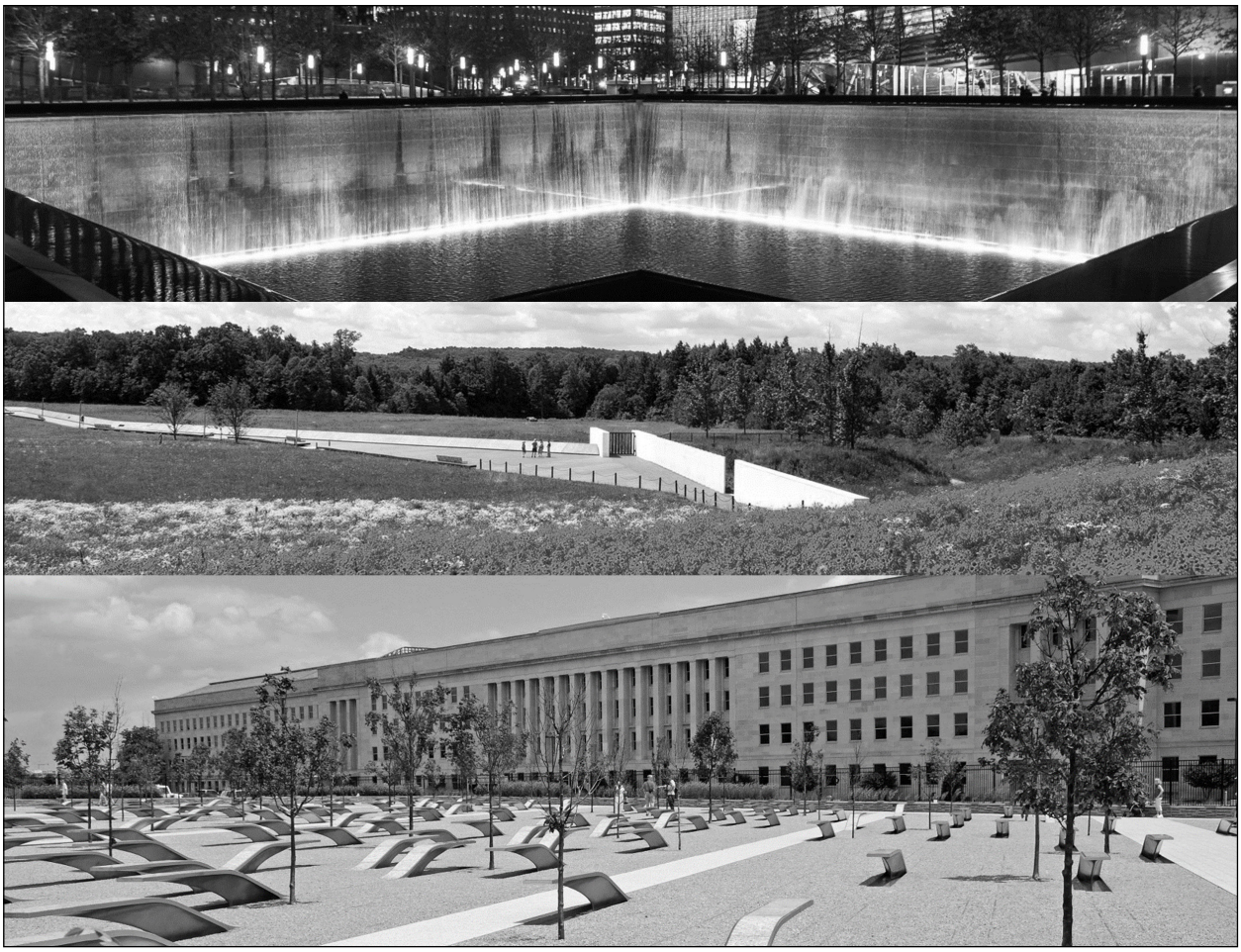
When under attack, most humans have an innate fight-or-flight response – run away from the danger or confront the attacker. However, emergency responders are not like most humans, and 9/11 proved that. When terrorists used planes to attack the United States, there was nobody to fight that day. Running away from the fires and destruction was an easy choice for most, but still not an option for others. There was work to do and lives to save.

Firefighters who narrowly escaped the buildings that collapsed went back into the burning pile repeatedly. Other first responders who were safe outside the hot zone converged at ground zero to help save as many lives as possible. Ordinary people who also could not accept fleeing as the only option traveled by land and water to help in any way they could to evacuate the survivors and save anyone who might have been trapped or injured. Spiritual leaders and counsellors provided much-needed support as despair set in.

Over the years, there has been no shortage of media coverage related to 9/11. However, the summit organized by the HSEMA SWIC, MWCOG, and CISA ECD this year was particularly impactful. The daylong lineup of first-hand accounts – from those on the ground, in the water, and in the air – covered raw and at times emotional behind-the-scenes perspectives from all three crash sites. The 9/11 attacks are well known, but it is difficult to imagine what it must have been like to be there on that day. The summit described the tragedy through the eyes of those who endured it.

Technology – Or Lack Thereof

The third annual District of Columbia Interoperability Summit in September 2021 was different than the previous two summits. Preparedness and response professionals



Compilation photo of three 9/11 memorial sites: New York (top), Pennsylvania (middle), Washington, DC (bottom). *Source:* Office of the Statewide Interoperability Coordinator, District of Columbia Homeland Security and Emergency Management Agency (2021).

have many technological tools and equipment to communicate effectively during an emergency. This annual event has been providing critical information on how to maintain communications when a disaster disrupts normal operations. For example, the 2020 summit, "Preparing for the 59th Presidential Inauguration in the 'New World'," focused on the expansion of utilizing *team collaboration tools* as a mean to communicate amid a global pandemic. However, the 2021 summit did not offer much on technology. Instead, it went back to the turning point in interoperable communications.

Before 9/11, firefighters, law enforcement officers, boat captains, emergency managers, helicopter pilots, etc. did not realize how critical real-time interagency communications would be. Technology also was not what it is today. No previous event involved a similar nationwide response with simultaneous fractures in multiple critical infrastructure sectors. In particular, the 9/11 chain of events exposed significant gaps in interoperable communications: agencies using incompatible radio frequencies, working in silos, and having equipment that fails when it is needed most. As a result, the actual response depended on previous trainings, instinct, and most importantly relationships.

Lessons From the Past

It is challenging to confront current and future threats without examining and learning from past events. Likewise, it is possible to become so dependent on modern advanced technology that it is difficult to remember what to do without it. Many changes were made and needed to be made to address the communications gaps exposed on 11 September 2001. However, some of the interoperability lessons that were highlighted at the summit and that need to be remembered today were not just about the deficiencies in technology, but about the true grit of the responders and the effectiveness of the relationships – those established before the attacks, those created in the aftermath, and those that have been sustained and strengthened over the past two decades.

Welcome sign at the summit. *Source:* Office of the Statewide Interoperability Coordinator, District of Columbia Homeland Security and Emergency Management Agency (2021).

The 2021 Interoperability Summit drew 530 virtual and in-person attendees representing 27 states and 3 territories. The 10-hour event is summarized in the recently released After Action Report (AAR). Key takeaways from the presentations, links to many of the video recordings, and survey results are all included in this report.

The fires at ground zero in New York burned for four months, but the events of that day and the heroic actions that followed should remain burned in memories forever. The next generation of responders did not experience firsthand that tragic day and the nationwide unity that followed. Emergency preparedness and response professionals have proven time and again that they do not run from danger, but into it. They must also continue to pass on the lessons learned and demonstrate the relationship-building skills that connected colleagues and strangers when other communications were lost. Now that the 20th anniversary of the 9/11 attacks has passed and 2021 comes to an end, one of the most important takeaways for future emergency preparedness and response professionals is to never forget.

Click here to download the District of Columbia's 2021 Interoperability Summit After Action Report.

Catherine L. Feinman, M.A., joined Team DomPrep in January 2010. She has more than 30 years of publishing experience and currently serves as editor-in-chief of the DomPrep Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and resilience communities. She also is the risk and safety coordinator and emergency medical technician (EMT) for Hart to Heart Transportation. She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

TELEDYNE
FLIR
Everywhereyoulook™

WE'VE GOT YOUR BACK. LITERALLY.

high sensitivity detection is now able to fit in a simple backpack.

The identiFINDER R700 Backpack Radiation Detector (BRD) offers a hands-free capability for broad-area radiological search and monitoring missions. The identiFINDER R700 provides the user all that is required to successfully perform wide-area searches quickly, efficiently and confidently. Providing the ultimate versatility, the identiFINDER R700 can be placed for stationary monitoring at makeshift checkpoints, fence-line monitoring, and other temporary screening locations. When coupled with radiation monitoring software, the identiFINDER R700 can be used as a fixed-site monitoring tool.

LEARN MORE AT FLIR.COM/R700