DomPrep Journal

Subscribe

Volume 14, Issue 4, April 2018

CBRNE Weapons & Islamic State – A Bad Combination
By Richard Schoeberl

Improving Local Health Department Cybersecurity
By Justin Snair

Five Steps Toward Enhancing Climate Resilience
By Emily Wasley

In Search of Infrastructure-Proof Emergency Alerts
By Rodrigo (Roddy) Moscoso

Also inside...

Podcast: Bringing Specialized Training to All Communities

Interview with two leaders from the National Domestic Preparedness Consortium, moderated by Andrew Roszak

GasLit

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

DomPrep Journal is electronically delivered by the IMR Group Inc., P.O. Box 810, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; also available at www.DomPrep.com

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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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

Featured in This Issue

Pictured on the Cover: (top row) Schoeberl, Source: iStock.com/RomoloTavani; Snair, Source: Snair, 2018; (second row) Wasley, Source: ©iStock.com/leolintang; Moscoso, Source: Project Loon, 2013

Publisher's Note

By Martin D. Masiuk

To say the information business has undergone a huge transformation would be an understatement. Today's readers expect content to be relevant, factual, and free. As a publisher, my challenge has been to adapt to this 21st century requirement and still rely on a 20th century business model. I have always valued and sought after important decision-making readers and was able to convince advertisers that DomPrep's targeted and stellar demographics were reason to purchase the advertisements that have supported this publication. Unfortunately, advertising continues to dwindle with more and more companies not having an appetite to promote their products with traditional advertisements.

So, what to do? After twenty years of providing critical information to thousands and thousands of first responders, medical receivers, emergency managers, local-state-federal authorities, nongovernmental organizations, and the private sector, the DomPrep property is just too valuable to end, but it needs to change. In today's world of social media, fake news, and young readers wanting information in 50-word gulps, I must question my current business plan.

To react to the current environment, adjustments are being made. The number of articles published is being reduced. Additional changes are under consideration as I seek a new long-term strategy. To do so, I will be asking for your help.   I will reach out to the readership via Survey Monkey for specific input.

I look forward to receiving your feedback.

Sincerely yours,

Martin (Marty) Masiuk
publisher@domprep.com

CBRNE Weapons & Islamic State – A Bad Combination

By Richard Schoeberl

The recent developments concerning the nerve agent attack in the United Kingdom and their alleged country of origin, Russia, have raised fears in the international community. The ease of the attack raises concerns about terrorists utilizing similar methods. This raises questions about the likelihood of a similar attack against the West.

The alleged Russian nerve agent, Novichok, used in the recent attacks in the United Kingdom is so scarce that rarely has anyone outside of Russia handled this type of agent. Russian chemist Vil Mirzayanov, who now lives in the United States and helped design the agent Novichok, told NPR that he has no doubt that Russia was directly involved in the attempted murder of Russian ex-spy Sergei Skripal and his daughter Yulia Skripal. Although the chances are miniscule that criminals or a terrorist organization would be able to steal Novichok from inside Russia, it is concerning nevertheless that there have been previous instances where chemical, biological, radiological, nuclear, and explosive (CBRNE) weapons have been sold – or attempted to be sold – on the black market that came directly from Russia.

The black market would be a clear path for the Islamic State to obtain materials that could be used in a CBRNE attack. In 2015, the Federal Bureau of Investigation (FBI) and Moldovan investigators ran a sting operation against a suspected arms smuggler in Moldovia attempting to sell to what he thought was a representative from the Islamic State high-grade uranium (Cesium 137). The smuggler was intentionally seeking a Middle Eastern buyer, so the weapon could be used on "the Americans." As indicated in the recent 2018 Worldwide Threat Assessment Intelligence report, produced by the Director of National Intelligence, both state and non-state actors have already demonstrated the development and use of CBRNE weaponry. The report emphasizes that, "chemical materials and technologies – almost always dual-use – move easily in the globalized economy, as do personnel with the scientific expertise to design and use them for legitimate and illegitimate purposes." The Islamic State is the first non-state actor to combine a projectile delivery system with a banned chemical warfare agent, according to the Combating Terrorism Center.

According to a NATO Review report, there is a "very real – but not yet fully identified risk – of foreign fighters in the Islamic State's ranks using chemical, biological, radiological or nuclear (CBRN) materials as weapons of terror against the West." Like al-Qaida, the Islamic State has also sought the use of chemical and biological weapons. Although al-Qaida's efforts were merely aspirational at best, the Islamic State actually achieved the goal of chemical weapon acquisition. During congressional testimony in 2016, the then Director of National Intelligence James Clapper stated that the Islamic State's use of chemical weapons is the first time a terrorist organization has done such since 1995, when the organization Aum Shinrikyo used sarin gas on the subway in Tokyo. The United Nations has been investigating the use of chemical weapons in Syria and Iraq and have concluded the Islamic State has acquired and used chemical weapons on many occasions. According to the 2018 Worldwide Threat

Assessment, the Islamic State has been previously linked to sulfur mustard attacks and several chemical weapons attacks within Syria and Iraq. Experts believe the Islamic State's arsenal of weapons includes mustard gas and chlorine. Michael Morell, former Central Intelligence Agency (CIA) deputy and acting director, stated that "ISIS has for some time said that they want to acquire weapons of mass destruction and to use them and they've actually been able to manufacture chemical weapons in Iraq and Syria and use them on the battlefield."

Following a thwarted attack in Paris, France, in 2015, then French Prime Minister Manuel Valls discussed before Parliament the possibility of the Islamic State using CBRNE weaponry against the West, saying, "I say it with all the precautions needed. But we know and bear in mind that there is also a risk of chemical or bacteriological weapons." The West has reason to be with the Islamic State's desire to employ CBRNE attacks. A laptop was recovered in the battlefield in 2014 from an Islamic State stronghold inside Syria. Information within the laptop, aside from jihadist instructional propaganda on bomb making, was a 19-page instructional document discussing the development of biological weapons and instructions on how to weaponize the bubonic plague. The laptop also contained a 26-page fatwa on the use of weapons of mass destruction and a passage from Saudi jihadi cleric Nasir al-Fahd stating, "If Muslims cannot defeat the kafir (unbelievers) in a different way, it is permissible to use weapons of mass destruction, even if it kills all of them and wipes them and their descendants off the face of the Earth." Officials believe the laptop belongs to a Tunisian national who was studying chemistry and physics and was teaching himself biological weaponry.

According to NATO Review, an unsettling concern is that the Islamic State had previously stolen 90 pounds of enriched uranium from Mosul University in Iraq. Although it would be extremely difficult for a member or someone pledging their allegiance to the Islamic State to smuggle a CBRNE weapon into the country, the fear looming is that someone already in the country who is radicalized is provided instructions on how to build such weapons. The 2018 Worldwide Threat Assessment Intelligence report stressed that the United States will likely see an increase in homegrown extremism and many will "continue to be inspired by a variety of sources, including terrorist propaganda as well as in response to perceived grievances related to U.S. Government actions." The Islamic State, known for the "do-it-yourself" propaganda magazine *Rumiya*, has previously sparked the increase in knife welding and vehicle attacks across the globe by promoting the use of these "homegrown" style attacks through explicit instructions in its popular online magazine.

Although a recent issue of *Rumiya* has not been published instructing how to carry out specific CBRNE attacks in the United States, there has been increased "chatter" intercepted by U.S. Intelligence indicating that the Islamic State has been discussing how to replicate in the United States the deadly chlorine and mustard gas attacks previously carried out in Iraq and Syria. "I think we need to be more

©iStock.com/RomoloTavani

worried about them making it here. This stuff is difficult to transport, it's difficult to get it by customs and immigration. I think it's more likely that they send the recipe here to their followers and they make it here," according to Michael Morell, former CIA deputy and acting director. Although the development of this type of weaponry requires advanced technology and sophisticatedly trained personnel, those could be more readily available in the United States as opposed to the battlegrounds in Iraq and Syria. According to the Combating Terrorism Center, a chemical attack by the Islamic State cannot be ruled out should the organization seek to deploy a rudimentary poison gas device in the United States.

In 2017, Australian counterterrorism officials disrupted a plot where four men, directed by the Islamic State, planned to use an improvised chemical dispersion device containing hydrogen sulfide. A clear demonstration of the Islamic State's ambition to use CBRNE attacks in the West, following the model of those carried out by the terrorist organization in Iraq and Syria. The threat of CBRNE use by the Islamic State within the United States is more than plausible. The Department of Homeland Security (DHS) is actively working to thwart this threat, according to DHS official Col. Lonnie Carlson: "We're putting capabilities out in the field right now to counter this threat that 6 months ago, we probably never would have thought of happening … the bottom line is … the threat is real."

There certainly is an undeniable threat by unknown knowns within the United States. Unfortunately, the threats can come from those inspired and radicalized by the Islamic State – homegrown or those returning from the battlefield in Iraq and Syria – regardless, the threat is real and disturbing. The Islamic State has made use of a widely available industrial chemical – chlorine – abroad and likely could employ the same scenario within the borders of the United States. The use of encrypted technology is increasingly concerning with terrorist groups using encryption that allows them not only the opportunity to radicalize followers online communicate anonymously, but additionally serve as an online institution for furthering the education of wannabe jihadists.

Recently, the Islamic State published on its Furat Wilayah channel (encrypted messaging app Telegram), an English-language series promoting lone-wolf jihad encouraging would-be jihadists and supporters to inject food for sale in markets with cyanide poison. Fortunately, thus far in the West, the majority of homegrown terrorists plotting attacks have selected only methods that have not included the employment of CBRNE. However, today's fearful climate foreshadows looming plots. Although it is perhaps difficult to determine how realistic a chemical attack is from terrorist organizations, the probability rises, mirroring growing fears.

Richard Schoeberl, has over 22 years of security and law enforcement experience, including the Federal Bureau of Investigation (FBI) and the Central Intelligence Agency's National Counterterrorism Center (NCTC). He has served at a variety of positions throughout his career, ranging from supervisory special agent at the FBI's headquarters in Washington, D.C., to acting unit chief of the International Terrorism Operations Section at the NCTC's headquarters in Langley, Virginia. Before his managerial duties at these organizations, he worked as a special agent investigating violent crime, international terrorism, terrorist financing, cyberterrorism, and organized drugs. He also was assigned numerous collateral duties during his FBI tour – including a certified instructor and member of the agency's SWAT program. In addition to the FBI and NCTC, he is an author and has served as a media contributor for Fox News, CNN, PBS, NPR, Al-Jazeera Television, Al Arabiva Television, Al Hurra, and Sky News in Europe. Additionally, he has authored numerous articles on terrorism and security. He is currently the Program Chair of Criminology and Homeland Security at Martin Methodist College.

Improving Local Health Department Cybersecurity

By Justin Snair

Cyberattacks against local governments are becoming a new normal, yet the nation is not doing enough to prepare local health departments (LHDs) from such attacks. More than just a technological issue addressed by information technology (IT) professionals, cyberattacks can threaten lives and result in losses of integrity, availability, confidentiality, and physical destruction of assets. Cyberattacks can erode the trust and confidence communities have in LHDs and can introduce legal and liability issues when breaches of protected patient health information occur. LHDs should consider cyberattacks, and the myriad of nontechnical issues that may result, as part of their all-hazards preparedness efforts.

Stories of cybercriminals attacking entire local and county government systems have become more common in the past year. Recent events include a cyberattack in Dallas, Texas, that managed to set off all 156 emergency alarms in the city, a ransomware attack in Mecklenburg County, North Carolina, that slowed the county government to a crawl, and another in Atlanta, Georgia, that disabled critical systems, forcing many city workers to revert to paper. While these incidents have not yet presented widespread or prolonged disruptions to LHD services, considering the effect of such a scenario has become increasingly important.

> *Hypothetical scenario: You are a director of a local health department (LHD). Your community government recently completed updating its computer systems for all departments, integrating mobile and medical devices, servers, and workstations, and enabling computer-controlled building automation technology to regulate heating and cooling, lighting systems, door locks, alarms, and refrigeration units in all county facilities. LHD personnel have networked desktop and laptop computers, voice over IP (VOIP) landlines, mobile phones and emails, and an electronic reporting system for vaccines administration. The United States is several months into a moderate to severe influenza season and your LHD is holding influenza vaccine clinics at several locations across the county.*
>
> *The LHD is also one year into a chronic disease and environmental monitoring research project funded by a federal agency and a private technology firm. The research data for this project are stored on your county government's computer system. There is news of a computer ransomware – a program that infects a computer, blocks access by encrypting key components, and demands a ransom be paid for the restriction to be removed – spreading across the internet through networks and removable drives, downloading files, and stealing information. You receive word that staff members who are setting up a flu vaccine clinic are having trouble connecting to the electronic medical record system on the county computer network. VOIP phones services are routinely unavailable throughout the day. You receive word from your research staff that data are no longer*

> *accessible. You learn that many of the county computers, including the systems for tax payments, birth and death certificates, county sewer and water, and facility heating and cooling, are locked with a ransomware message; demanding a $23,000 payment in Bitcoins to unlock the computers.*
>
> *You consider activating the LHD's emergency response plan, but are uncertain if a cyberattack requires such a response. Your county emergency manager and executive leadership call a department head meeting to discuss what to do and decide to not pay the ransom. Two weeks have passed since the attack began and county services have been severely interrupted. The county IT department is slowly restoring services, albeit with significant loss of data. It was learned that an infected USB drive, obtained from a public health preparedness conference as a giveaway, was the culprit.*

The technical assets available to and services provided by this hypothetical LHD are typical and routine, like countless actual health departments throughout the nation. Unfortunately, many LHDs could also find themselves similarly affected by cyberattacks. Therefore, it is important to consider cyberattacks as part of all-hazards planning, which begins by considering the following questions:

- What is the role of an LHD in cybersecurity incidents?
- What are the most critical systems at risk of compromising public health in the event of a cyberattack?
- If a cybersecurity incident occurred, could LHD operations continue?
- Does the community have contingency plans in place for a cyberattack?
- Who at the state and federal levels of government should be contacted regarding a cyberattack?
- Would a cyberattack trigger the activation of the emergency response plan?
- Who is identified as the community lead in such an event?
- Does the community emergency operations plan include an air-gapped network and equipment (i.e., a physically isolated secure computer network)?
- Will a county or local community pay in the event of ransomware? If not, is it prepared for consequential data loss and privacy breaches?
- When should the public be notified and what information should be shared about cyber incidents?

In addition to presenting technological issues, cyberthreats to LHDs can be classified in terms of their capacity to introduce losses of integrity, availability, confidentiality, and physical destruction. Cyberattacks could erode the trust and confidence that communities have in LHDs and government services, and can introduce legal and liability issues when breaches of protected patient health information occur. As such, federal agencies, academic institutions, national public health representative organizations, and state and local government agencies should work collaboratively and strategically to improve preparedness for LHD cybersecurity incidents.

Cyberrisks to Local Health Departments

The local public health system is comprised of all public, private, and voluntary entities, and their human, infrastructure, and virtual assets, responsible for the health and wellbeing of communities. As part of this system, roughly 2,750 LHDs across the nation provide services that include: food safety, vaccinations, epidemiological surveillance, disaster preparedness planning, emergency response, laboratory testing and coordination, health information exchange, health communication and outreach, community resilience building, public-private sector planning and exercises, hazard and risk assessments, and protection of all sectors from natural and manmade hazards. The *10 Essential Public Health Services* are the activities that a local public health department should undertake to ensure the health, safety, and security of the communities it serves. Table 1 describes how such services could be impacted by cyber incidents.

From a national critical infrastructure protection perspective, LHDs are part of the Healthcare and Public Health (HPH) sector, one of sixteen national critical infrastructure sectors deemed so vital that the failure or degradation of its systems, networks, or assets would have a severe impact on national security, safety, and health. Efforts to protect the critical infrastructure of the HPH sector is coordinated at the national level through various public and private councils and information sharing organizations. LHDs are also interconnected with and interdependent on many other sectors, such as those responsible for water/wastewater, energy, transportation, critical manufacturing, and supply chain. Local public health is vital to the continued security and welfare of our nation, but relies heavily on technology to deliver services and is increasingly vulnerable to cyberattacks. Unfortunately, several factors inhibit optimal cybersecurity of local public health organizations.

First, the local public health departments are highly variable. The system is made of thousands of independent nodes, each providing services to the public using many different technological assets and levels of resources. Therefore, cybersecurity risk is not uniform and preparedness approaches need to be customized. Often, LHD technological assets are covered under broader jurisdiction-wide IT programs, contributing to a lack of focus on cyberthreats by LHD professionals. In addition to preparing for cybersecurity threats, in the wake of active shooter events, communities around the nation are examining their physical security postures. The implementation of increased physical security measures and practices across local governments, including LHDs, also add a layer of complexity as nearly all of these measures have some type of cyber element. In a challenging budget environment, often the physical security programs and cybersecurity programs are competing for the same limited funds. Additional efforts to further bring these two areas together and truly look at threats and risks across the enterprise would allow LHDs to maximize their limited funds. The enterprise view at the cyber-physical nexus would allow LHDs to analyze and determine true risks and determine which can be reduced and which need to be accepted.

Second, at the national level, investments in improving HPH sector cybersecurity have largely focused on healthcare entities and connected industry partners. Nearly all cybersecurity materials and tools produced at the national level focus on healthcare service providers – not LHDs. This omission is not surprising, as LHD cyberrisk is not as well understood as the risks to healthcare, nor is there a sufficient evidence base from which to

Table 1. Impact of Cyberattacks on 10 Essential Public Health Services

Essential Public Health Service	**Key Local Health Department (LHD) Activity**	**Example of Vulnerability**
Monitor health status to identify and solve community health problems	Health surveillance	Computer systems that collect and transfer data are vital for both active and passive surveillance.
Diagnose and investigate health problems and health hazards in the community	Analysis of health information	Loss of access to information hinders the ability of LHDs to diagnose problems in the community.
Inform, educate, and empower people about health issues	Delivery of health information	Attacks on information dissemination systems limit the ability of LHDs to share information.
Mobilize community partnerships and action to identify and solve health problems	Electronic coordination and planning	Loss of electronic communication reduces the effectiveness of community partnerships when needed most.
Develop policies and plans that support individual and community health efforts	Policy development	Educating policymakers on the public health effects of cyberthreats to formulate better policies and planning reduce the effects of a cyberattack.
Enforce laws and regulations that protect health and ensure safety	Gathering of public health data	The loss of infrastructures reduce the ability to report notifiable diseases or health violations.
Link people to needed personal health services and ensure the provision of health care when otherwise unavailable	Emergency response activities that provide people with necessary health services, including access to appropriate medical care	Loss of infrastructure causes the denial of utility services needed to maintain the health of the public. Hospitals encounter reduced capacity to provide medical care with the loss of a hospital system.
Ensure competent public and personal health care workforce	Many activities, including outbreak management, emergency response, and disease tracking	The continuing loss of staff and funding make it difficult for LHDs to meet public needs. Increased strain on the system due to a cyberattack magnifies this problem.
Evaluate effectiveness, accessibility, and quality of personal and population-based health services	Assessment of public health interventions	Evaluation of health interventions requires data storage and communication to measure progress toward goals.
Research new insights and innovative solutions to health problems	Data collection for outbreak response research	Research during a cybercrisis is limited due to loss of infrastructure and records.

Source: Adapted from "Cybersecurity Threats to Public Health," by Daniel J. Barnett, Tara Kirk Sell, Robert K. Lord, Curtis J. Jenkins, James W. Terbush, and Thomas A. Burke. World Medical & Health Policy, 5:1. 2013.

develop LHD-focused cybersecurity policies and preparedness materials. Furthermore, for many years, representative organizations for public health were not adequately funded to participate in the national-level HPH sector cybersecurity efforts or to produce cybersecurity materials for LHDs.

Snair, 2018

Third, although there are Information Sharing Analysis Organizations/ Centers (ISAO/ISAC), vital avenues for analysis and sharing of threat information, improving the overall cybersecurity posture of state, local, territorial, and tribal governments (e.g., multi-state information sharing analysis centers), there is no ISAO/ISAC focusing specifically on local public health cyberthreats. The missions of the two existing HPH sector ISAO/ISACs – Healthcare Ready and National Health Information Sharing and Analysis Center (NH-ISAC) – more closely align with the needs of healthcare entities and adjacent stakeholders, such as those involved with the medical supply chain. Though the U.S. Department of Health and Human Services (HHS) awarded a grant in 2016 to the NH-ISAC to help share information on cybersecurity and engage participation of healthcare and public health sector, very little effort appears to be focused on the cybersecurity concerns of LHDs.

Fourth, public health organizations, possibly overwhelmed by other, well-understood priorities, dedicate very little attention to cybersecurity. It is not often viewed as a priority or even considered at all.

Action Items for Improving Local Health Department Cyber Preparedness

Cyberattacks against local governments are becoming a new normal, yet the nation is not doing enough to prepare for and mitigate the risks to the local public health from such attacks. However, there are signs of change. Recently, the National Association of County and City Health Officials (NACCHO), the representative organization for LHDs, was funded by the HHS Office of the Assistant Secretary for Preparedness and Response (ASPR) to more fully participate in HPH sector cybersecurity efforts and to produce cybersecurity materials for public health departments. The 2018 Preparedness Summit's closing plenary session – *A Troubling Gap: Why Cyber Security Matters to Public Health Emergency Response* – aims to help attendees classify potential cyberthreats and identify tactical strategies for responding to cyberattacks within their communities. Other thought leaders also advocate for improved public health cybersecurity preparedness, for example:

- The Cadmus Group has published several cyber-related articles, such as *When Pandemic Management Meets Cybersecurity* and *Embrace the Cyber Security-Physical Security Nexus*, which help raise awareness about cyberthreats to public health departments and governments.

- The American Public Health Association published Public Health Increasingly Facing Cybersecurity Threats: Health field a top target for attacks, presenting some of the risks encountered with a public health cyberattack.
- Cyber Georgia 2017, an annual convening of industry, academia, and government to examine cyberthreats presented the panel discussion Cybersecurity and Public Health, Emergency Preparedness and Response, which examined hospital and public health department preparedness for emergencies and simultaneous denial of service attacks.
- SGNL Solutions and LAR Consulting developed the *Local Public Health Department Discussion Guide for Cybersecurity* and are testing the prototype with public health professionals during a workshop at the 2018 Preparedness Summit.

These efforts, along with the leadership of the ASPR, demonstrate a large step toward improving local public health cyber preparedness. However, more can and should be done. Below is a list of action steps that can be taken by four key stakeholders involved in the public health system.

Federal agencies:

- Recognize the distinction between the healthcare and public health components within the HPH sector, the vulnerability of local public health entities to cyberthreats, and the unique consequences of a cyberattack on the public health system;
- Provide resources to academic research institutions to conduct research to thoroughly understand the complex risk relationships between cybersecurity and local public health;
- Use research to develop evidence-based policy and practices to address this threat;
- Fund the development of local public health cyberthreat assessment tools;
- Develop future legislation and regulations that fully account for the interactions between cybersecurity and local public health;
- Advocate for and ensure appropriate representation of local public health entities on federal cyber working groups and federal cyber programs/projects; and
- Establish a public health ISAO/ISAC, or fund an existing ISAC, that is truly focused on coordinating, collaborating, and sharing vital physical threat and cyberthreat intelligence and best practices among local public health entities.

Academic institutions:

- Conduct new research to thoroughly understand the cybersecurity risk of and consequences to local public health;
- Work with research funders, local public health practitioners, and evidence translation professionals to develop evidence-based practices and policies for cybersecurity; and

- Develop curricula to educate emerging public health professional of cyberthreats and mitigation techniques.

National public health representative organizations:

- Coordinate with academia on research efforts and the development of evidence-based policy/practices;
- Assist with the development and dissemination of local public health cybersecurity needs assessments and tools;
- Advocate for the appropriate representation of local public health equities on federal cyber working groups and federal cyber programs/projects;
- Develop communication materials to raise awareness of cyberthreats to local public health; and
- Develop tools and resources to assist local public health entities in understanding cyberrisk and improving incident preparedness.

State and local government agencies:

- Recognize and prioritize cybersecurity as a public health issue;
- Integrate cyber scenarios into public health training and exercise programs;
- Conduct cyberrisk vulnerability assessments or include public health in existing assessments;
- Understand the implications of the physical-cyber nexus and foster better coordination among IT security, physical security, and public safety/ preparedness teams; and
- Develop cybersecurity-specific emergency operation procedures and contingency plans.

It is important to remember that preparedness is a journey, not a destination. These actions are not meant to be comprehensive but, as with many issues, cyberattacks threaten local public health and the people that depend on it. Although there will continually be new threats to address and manage, identifying and taking small but systematic and coordinated steps are necessary for preventing or mitigating the many potential public health consequences that could follow a cyberattack.

Justin Snair, MPA, is the founder and principal consultant of SNGL Solutions, a service-disabled veteran owned small business that helps clients connect across research, policy, and practice communities to better identify, understand, and solve complex health and security challenges. He has 14 years experiencing working in local and county government, homeland security, public health, the military, and with federal government partners. He served as a senior program officer with the National Academies of Sciences, Engineering, and Medicine, where he directed the Forum on Medical and Public Health Preparedness for Disasters and Emergencies, the Standing Committee on Medical and Public Health Research During Large-Scale Emergency Event, and several other health security efforts. He was previously a public health officer with the Acton Health Department in Massachusetts and served as a combat engineer in the U.S. Marine Corps and is a veteran of Iraq war. He holds a Master of Public Administration degree from Northeastern University's School of Public Policy and Urban Affairs, where he concentrated on critical infrastructure protection and information assurance, and graduated from the Executive Education Program at Harvard University's National Preparedness Leadership Initiative.

Bringing Specialized Training to All Communities

Since 1998, the National Domestic Preparedness Consortium (NDPC) has been preparing first responders for a wide range of natural and human-caused incidents. Sponsored through the U.S. Department of Homeland Security/Federal Emergency Management Agency (DHS/FEMA) National Preparedness Directorate, the NDPC includes seven training partner organizations, each with different lanes of core capabilities:

- Center for Domestic Preparedness (CDP) – specializing in mass-casualty hospital training and tactical operations training in contaminated environments
- The Energetic Materials Research and Testing Center (EMRTC) – specializing in explosives, live explosives, and incendiary devices training
- National Center for Biomedical Research and Training (NCBRT) – specializing in training for weapons of mass destruction, counterterrorism, and other high-consequence events
- Texas A&M Engineering Extension Service (TEEX) National Emergency Response and Recovery Training Center (NERRTC) – specializing in incident management, infrastructure preparedness, cybersecurity, sports and special events, emergency medical services, senior and elected officials training and public information
- National Nuclear Security Administration/CTOS-Center for Radiological/Nuclear Training (NNSA/CTOS) – specializing in weapons of mass destruction (WMD) and radiological/nuclear training
- National Disaster Preparedness Training Center (NDPTC) – specializing in natural hazards training
- Transportation Technology Center, Inc. (TTCI)/Security and Emergency Response Training Center (SERTC) – specializing in training for surface transportation involving hazardous materials, weapons of mass destruction, and emergency events

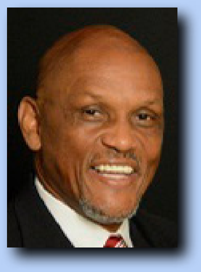
In this podcast, DomPrep Advisor Andrew Roszak talks with NDPC Chairman Colonel Alphonse Davis, U.S. Marine Corps (Retired), and Jeffrey Mayne, director of Louisiana State University's NCBRT, to learn more about the Consortium, its partners, the trainings offered, and its ability to adapt to the nation's constantly changing training needs. For example, recent shooting incidents have increased the demand for campus emergency active shooter programs. The NDPC has created a standardized training model that is applicable to all emergency management disciplines. The training courses are offered at no cost to local, state, and tribal agencies. As of 31 December 2017, the NDPC has trained more than 2.7 million participants.

Listen now to learn more about NDPC, its partners, and this vital training resource.

Andrew Roszak, Moderator,

Senior Director for Emergency Preparedness, Child Care Aware® of America

Andrew Roszak, JD, MPA, EMT-P, serves as the senior director for emergency preparedness at Child Care Aware of America. He's worked at the National Association of County and City Health Officials, MESH Coalition and the Health and Hospital Corporation of Marion County, Indiana. Roszak was also a senior advisor for the U.S. Department of Health and Human Services; on the Budget and HELP Committees of the United States Senate; and at the Illinois Department of Public Health. He is admitted to the Illinois and District of Columbia Bars and is admitted to the Bar of the U.S. Supreme Court. Find him on Twitter: @AndyRoszak.



Alphonse Davis,

Chairman, NDPC

Alphonse Davis serves as the deputy director of the Texas A&M Engineering Extension Service (TEEX) and chairman of the NDPC. Previously, he served as director of TEEX's National Emergency Response and Rescue Training Center, where he oversaw the Agency's Homeland Security National Training Program Cooperative Agreement with the U.S. Department of Homeland Security. Affiliated with TEEX since 2004, he serves as TEEX's principal representative to two national training consortiums: the National Domestic Preparedness Consortium (NDPC) and the National Cybersecurity Preparedness Consortium (NCPC). He also serves on the advisory board for the National Center for Spectator Sports Safety and Security (NCS4) at the University of Southern Mississippi. A 27-year veteran of the U.S. Marine Corps, he holds a bachelor's degree from Southern University, an MBA from Averett University, and a Master of Science degree from the National Defense University, Industrial College of the Armed Forces.

Jeffrey Mayne,

Director, LSU's National Center for Biomedical Research and Training

Jeffrey Mayne, director of NCBRT, worked for the Louisiana Department of Wildlife and Fisheries (LDWF) for over 31 years. He retired as the chief of law enforcement in 2014, but remained employed with the agency until joining LSU-NCBRT. He also served as Louisiana's state boating law administrator within the National Association of State Boating Law Administrators. He played a key role in the development of a national state/federal cooperative marine law enforcement program authorized in the Magnuson-Stevens Fishery Conservation and Management Act. He earned his undergraduate degree from Louisiana State University (LSU) with studies concentrating in political science, sociology, and corrections, and his master's degree in public administration from LSU as well.

BIO FIRE
FilmArray

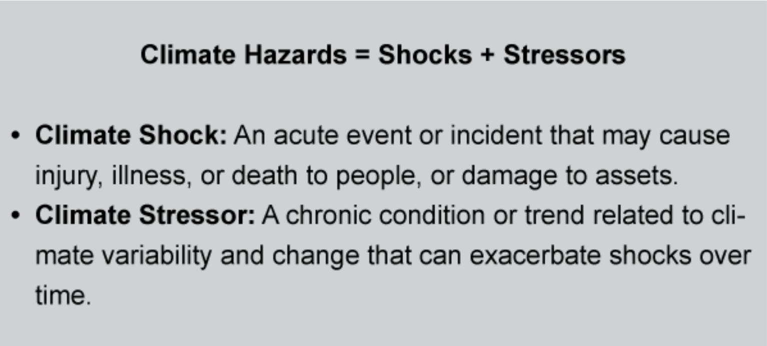
Five Steps Toward Enhancing Climate Resilience

By Emily Wasley

People, communities, businesses, and governments around the world are already experiencing the devastating human, economic, and environmental consequences of a changing climate. Many have been impacted by "acute climate shocks" such as wildfires, hurricanes, floods, heatwaves, and severe winter storms – resulting in the loss of lives, livelihoods, and infrastructure. Five steps can help emergency managers build a path to enhance their climate resilience.

In 2017, 16 climate and extreme weather-related disasters had losses exceeding $1 billion, associated with a combined total of 362 deaths across the United States (see Figure 1). This compares to the annual average of $5.5 billion weather and climate disasters between 1980 and 2016. More notable than the high frequency of these events is the cumulative cost, which exceeded $300 billion in 2017 – a new U.S. annual record. That shatters the previous U.S. annual record cost of $214.8 billion in 2005 associated with the impacts of Hurricanes Dennis, Katrina, Rita, and Wilma.

People and communities are now faced with more extreme and frequent climate shocks and, when combined with "chronic climate stressors" – such as increased temperatures, declining snow cover, changing precipitation patterns, increasingly frequent and/or intense drought incidence, and rising sea levels – result in "climate hazards." As climate hazards become more prevalent and impactful, they must be integrated comprehensively into hazard mitigation plans and exercises (facilitated simulations or scenarios of a plausible future). To improve outcomes during and after disasters, emergency managers should incorporate climate hazards (both the acute shocks and chronic stressors) as they engage in the "continuous cycle of planning, organizing, training, equipping, exercising, evaluating, and taking corrective action in an effort to ensure effective coordination during incident response," as described on the U.S. Department of Homeland Security's website.



Climate Hazards = Shocks + Stressors

- **Climate Shock:** An acute event or incident that may cause injury, illness, or death to people, or damage to assets.
- **Climate Stressor:** A chronic condition or trend related to climate variability and change that can exacerbate shocks over time.

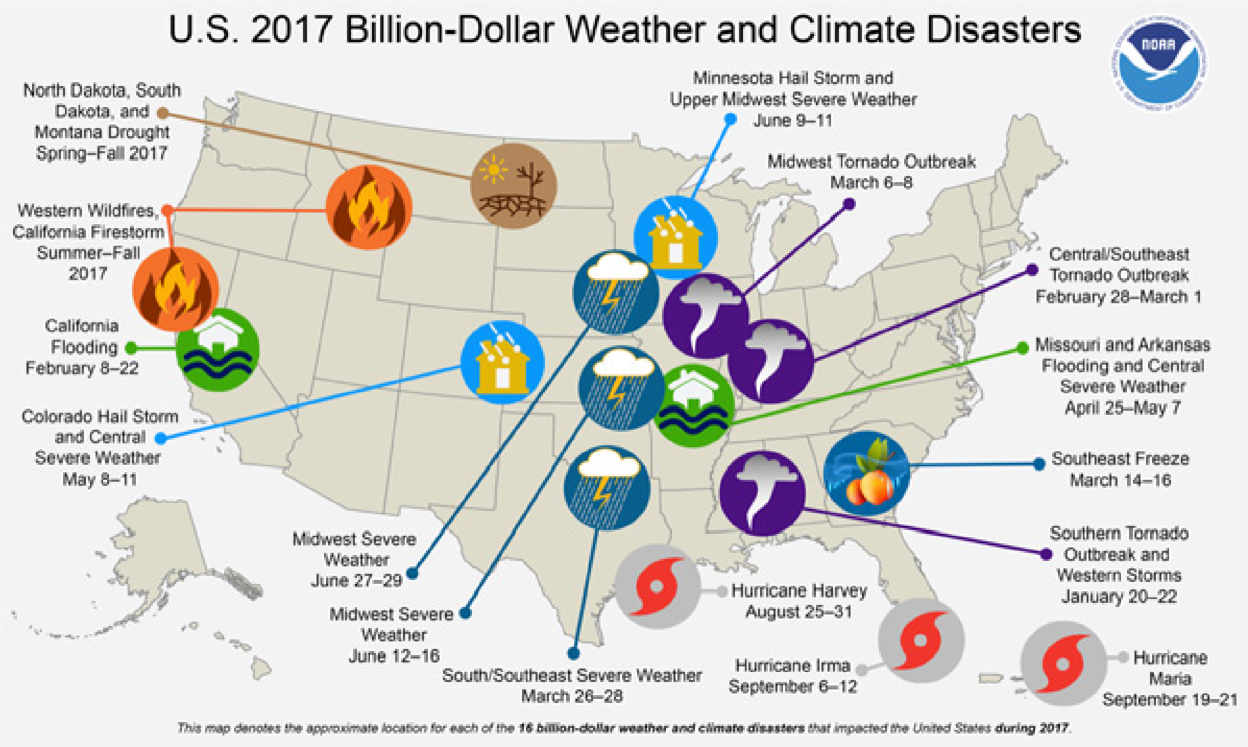

U.S. 2017 Billion-Dollar Weather and Climate Disasters
NOAA
North Dakota, South Dakota, and Montana Drought Spring–Fall 2017
Minnesota Hail Storm and Upper Midwest Severe Weather June 9–11
Midwest Tornado Outbreak March 6–8
Western Wildfires, California Firestorm Summer–Fall 2017
Central/Southeast Tornado Outbreak February 28–March 1
California Flooding February 8–22
Missouri and Arkansas Flooding and Central Severe Weather April 25–May 7
Colorado Hail Storm and Central Severe Weather May 8–11
Southeast Freeze March 14–16
Southern Tornado Outbreak and Western Storms January 20–22
Midwest Severe Weather June 27–29
Hurricane Harvey August 25–31
Midwest Severe Weather June 12–16
South/Southeast Severe Weather March 26–28
Hurricane Irma September 6–12
Hurricane Maria September 19–21
This map denotes the approximate location for each of the 16 billion-dollar weather and climate disasters that impacted the United States during 2017.

Fig. 1. U.S. 2017 Billion-Dollar Weather and Climate Disasters. During 2017, the U.S. experienced a historic year of weather and climate disasters. In total, the U.S. was impacted by 16 separate billion-dollar disaster events tying 2011 for the record number of billion-dollar disasters for an entire calendar year (*Source:* NOAA-NCEI, 2018).

A key challenge in integrating climate change into hazard mitigation or resilience planning is that many other priority hazards exist, including earthquakes, disease outbreaks, cyberattacks, and more. However, if left unmanaged, climate change would significantly exacerbate these other hazards, creating unprecedented challenges by multiplying the threats. For example, a heatwave could stress the already outdated and aging energy grid to the point of failure, which could:

- Leave the grid vulnerable to a cyberattack;
- Result in a complete shutdown of energy utility operations;
- Leave many without power during the heatwave;
- Provide unauthorized access to the personal and financial records of millions of customers; and
- Endanger the health and financial safety of U.S. citizens.

Turning this challenge into an opportunity to successfully execute an all hazards approach must incorporate climate hazards into exercise scenarios. This integrated scenario planning helps planners proactively understand the cascading effects of these combined hazards and allows them to take a systems approach to solutions instead of isolating the hazards from the start. The goal is to collaboratively and comprehensively analyze, design, and exercise future scenarios that allow emergency managers to assess their capacity, prioritize and plan for hazards, protect their assets, and ultimately thrive in the face of a changing climate.

Exercising & Preparing for Climate Hazards Through Resilience Planning

It can be difficult to know where to start when incorporating climate hazards into emergency management and hazard mitigation planning. The steps below, compiled through years of lessons learned, outline how emergency managers can get started on the path to successful climate resilience.

Step 1: Establish a Team

Effective climate hazard preparedness and resilience involves a team – an inclusive yet nimble team – consisting of people who are responsible for protecting critical assets (built, natural, and social) from a variety of hazards to enhance overall resilience. The purpose of the team is to collectively identify and address climate hazards that the organization, community, or region is facing.

When forming a team, be sure to include members within the whole community, as they have valuable insight into historical and current hazards, and are often the first responders when events occur. Consider individuals and groups such as the local departments of health and human services, employment and economic development, housing, emergency management, environmental health, parks and recreation, water and wastewater, or public works along with planning commissioners, boards of supervisors, environmental justice representatives, urban and transportation planners, faith-based organizations, climate scientists or research centers (these tend to be housed within universities), and commercial organizations.

Including groups from many perspectives also brings together many types of resources. For example, faith-based groups can provide a variety of resources from physical shelters to emotional and/or psychological safe houses for those affected by climate hazards. Commercial establishments can do the same. For example, during Hurricane Sandy, IKEA™ offered one of its Brooklyn stores as shelter, which was not only helpful for the community, it was smart marketing for the company – a proverbial win-win.

Step 2: Explore Climate Hazards & Cascading Effects

With a team in place, begin exploring the various climate hazards that the community has faced in the past, and future hazards they are likely to face based on climate models available at the regional or local scale. Many communities have conducted a Threat and Hazard Identification and Risk Assessment (THIRA), a process developed by the Federal Emergency Management Agency (FEMA) that helps communities map their specific risks to core capabilities and is required to be eligible for FEMA funding. Reviewing the latest THIRA is a good place to start, as it provides the team with an understanding of the community's existing hazards (including climate change).

Once climate hazards have been identified, the cascading effects (both the risks and opportunities) on the various systems, services, and assets upon which the community depends can then be mapped to connect the dots between the climate hazards and their impacts on the whole community. For example, consider climate hazards related to water and their impact on water utilities and surrounding communities. Water utilities provide drinking water to homes, workplaces, schools, hospitals, and public buildings. Unless these utilities actively exercise potential scenarios that identify weaknesses in their systems, they can be exposed to multiple threats, creating devastating impacts on their customers, infrastructure, and overall reputation.

As the team considers various climate hazards and their cascading effects on the community, the emphasis should also be on understanding how these interact with, or exacerbate, non-climate hazards that the community has identified (e.g., cybersecurity attacks, disease outbreak, health crisis, and aging infrastructure).

Step 3: Investigate Options & Prioritize Actions

Once the team has identified the current and future hazards and their cascading effects, the next step is to understand the community's capacity to manage them. Benchmark what has already being done within the community to prepare for, adapt to, and enhance resilience to climate hazards, and then consider what may need to be added to accommodate the cascading effects identified in Step 2. A local government, business, or university may already have conducted a climate hazards assessment and developed a Climate Action Plan that incorporates adaptation or resilience actions. Build off what has already been done; it is critical to leverage existing efforts.

If left unmanaged, climate change would significantly exacerbate many other hazards, creating unprecedented challenges by multiplying the threats.

Part of benchmarking should include exercising. Be sure the team is role playing, acting out true-to-life scenarios, and exercising beyond their abilities. If the team exercises only to capacity, they do not learn their limits. Exercising beyond their limits helps them better understand where improvements should be made.

Step 4: Plan for & Operationalize the Hazards

This step is the culmination of all previous steps. In this step, the team incorporates climate hazards, cascading effects, and associated actions to address the hazards into a new climate resilience plan, or existing plans, that help address future hazards the community faces. Ideally, the team would incorporate climate resilience into broader emergency management or continuity of operations plans, creating strategies that are co-beneficial. It is worth noting that some states and/or jurisdictions may require a separate document, particularly for funding or grant money.

Regardless, the plan(s) should include a broad array of actions that addresses multiple hazards that have been identified in Step 2. It should define who plays what role, particularly in cross-functional/multidiscipline inclusive plans, including actions that not only enhance resilience to current and future climate hazards, but actions that also support sustainability. Many actions that enhance climate resilience are also beneficial for sustainability, such as diversifying energy resources.

Step 5: Act & Continually Improve

Finally, take lessons learned – through exercising or information gathering – and incorporate them into an updated plan regularly. Frequently monitor and evaluate the effectiveness of the plan and update it accordingly. Plans should be updated annually, biennially, or as frequently as required for associated funding. However, they should not go more than two years without updating given the rapid changes in hazards that may be occurring (e.g., more intense wildfires and mudslides than previously experienced) and the capacity of the team and community to manage these changes. If there are additional funds to invest, be sure to invest them where they would be most effective.

©iStock.com/leolintang

Lastly, think about the future of the local community: what values and assets does this community provide; its resilience to climate change; and the ability of its residents to thrive in the face of changing conditions. If there are doubts about the community's future under a business-as-usual approach, it is time to prepare for and address climate hazards. By creating more resilient communities, their people, assets, and legacies can prevail.

Emily Wasley has more than 13 years of experience working with a variety of private, nonprofit, academic, and government organizations on domestic and international climate change research, policy, and strategy. She serves as director of Cadmus' Climate Security, Adaptation, and Resilience Practice. Prior to Cadmus, she served as the Inform Decisions and Adaptation Science Program manager for the U.S. Global Change Research Program (overseen by the White House Office of Science and Technology Policy), as well as a science translator for federal agencies developing their agency adaptation plans, as a technical climate expert supporting the former Administration's preparedness pilots, and contributing author of the Third National Climate Assessment's Adaptation Chapter. She is a certified Change Management Advanced Practitioner (CMAP) and Decision Making for Climate Change professional. She holds an M.A. in Environmental and Natural Resources Policy and a B.A. in Public Policy and Environmental Studies. She also serves as an adjunct fellow for the American Security Project and a member of the U.S. Green Building Council's LEED Resilience Working Group.

In Search of Infrastructure-Proof Emergency Alerts

By Rodrigo (Roddy) Moscoso

The increased reliance on emergency text alerts to receive warnings of natural or manmade disasters is a capability that most people have come to expect. Listening to broadcast radio warnings of severe weather happening miles away has transformed into more precise, geo-located alerts that target specific locations. The benefits of this technology are profound and should lead to people taking action when an alert comes in because they know that the threat is timely and accurate to their locations. New technologies could save many lives during future disasters.

Notwithstanding human or technological errors that do occur – for example, the erroneous North Korean missile alert in Hawaii or nonstop weather alerts that drive people to disable the alert feature on their phones – these alerts have the ability to save lives in ways not possible only a few years ago. Unfortunately, as powerful as these systems and smartphones are to pinpoint locations or to receive and display alerts specific to nearby life-threatening situations, this capability would fail if there is no "last mile" signal to communicate with handheld hardware.

Lessons Learned From Wildfires in California

As the recent wildfires in California demonstrated, this communication channel is vulnerable to the same disaster it is trying to warn against – everything burns, including cell towers and power lines – and without coverage, lives may be in danger. After fires ravaged California's wine country in October 2017, Sonoma County Sheriff Rob Giordono noted that "communication problems in general have been difficult," due to the size and scale of the fire, which ultimately killed more than 40 people and destroyed 3,500 homes and businesses. In Sonoma County, the fires disabled 77 cellphone towers, some due to power failures. Without cell coverage in the immediate area of the fires, emergency alerts could not be delivered to smartphones. Although Giordono noted that residents who registered for county alerts for their landline phones would receive warnings, this assumes that homes have a traditional (and self-powered) twisted copper pair landline connected to a hard-wired telephone. For the increasing number of people who have either discontinued using their landline phones or have moved to an internet phone service such as Vonage or MagicJack, these "landline" alerts would only arrive if these houses still have internet service.

Given the power outages reported throughout the fire-ravaged region, that may be a poor assumption. Giordono also noted that residents can sign up for alerts through Nixle, which the Sonoma County Sheriff's Office and many other jurisdictions across the nation use to disseminate information about weather, law enforcement, and traffic alerts, as well as other events that may affect a given county or jurisdiction. Nixle uses multiple alert pathways, including cellular, wi-fi, and email to send alerts. However, Nixle is equally dependent on cellular or broadband internet to deliver alerts. In the case of the Sonoma wildfires, areas hit hardest and quickly – and notably without power for cell towers or home cable modems – would not receive these alerts.

Geo-Targeted Alert Systems

Despite dependencies on commercial infrastructure (commercial power and wireless providers), the Federal Communications Commission (FCC) and the Federal Emergency Management Agency (FEMA) are moving ahead with the development and use of geo-targeted emergency alerts as part of the Federal Wireless Emergency Alerts (WEA) system. WEA notifications can be received on most newer cellphones, and are delivered as unique text-like messages accompanied by a full-volume alert tone "to warn the public about dangerous weather, missing children, and other critical situations." By default, these alerts are enabled on all WEA-capable cellphones. However, at the commercial wireless carrier's discretion, users can opt out of "emergency" and "Amber" alerts occurring in their region. However, "Presidential Alerts" cannot be blocked.

On Thursday, 5 April 2018, the FCC and FEMA conducted the first test of the WEA system across the 21 jurisdictions that make up the "National Capital Region" around Washington, D.C. Between 10:00 and 11:00 a.m. (EST), approximately 5 million people received the test alert. Since WEA notifications are targeted at phones that are identified to be in a specific geographic area (defined by the "county" the phone is in), *all* cellphones – even those just visiting the D.C. area – received the alert. Although lessons learned from the erroneous "missile alert" in Hawaii have been carefully considered, and the word "TEST" will be clearly denoted in the message, it was still a jarring experience for many. Public safety agencies were

A Google X "Loon" balloon (Source: Project Loon, 2013).

prepared for a barrage of calls to 911. However, the test went off with few technical issues, and most people received the alert as expected.

The power of the WEA, Nixle, and other alert notification systems used by emergency management agencies are a huge step forward in being able to notify people in specific areas of imminent, life-threatening situations. When seconds count – such as an approaching tornado or severe weather event – these alerts can save lives. However, the wireless infrastructure for delivering the alerts is a core dependency that has no backup.

Following Hurricane Maria, the infrastructure-ravaged Caribbean islands had no commercial power, and cell service was unavailable to millions. In the case of Hurricane Maria, the National Weather Service was able to provide advanced warnings to residents, providing ample time for preparation. However, when the damage became catastrophic for residents who lost everything, WEA could have been used to notify residents in specific areas or places where they could find shelter, food, and water. Unfortunately, although most people had cellphones with enough power to receive alerts – at least for several hours following the hurricane – there was no way for these alerts to be sent.

Emerging Technologies

In Puerto Rico, the FCC authorized the use of Google Alphabet's Project Loon, which provided high-altitude balloons to deliver cell service to the island. However, that was several weeks after the event. Despite strategies to put such balloons (or other mobile cell service solutions) in place more quickly in the future, the window of time following a catastrophic event is small. When commercial infrastructure is unavailable or, as in the case of the Sonoma County wildfires, the people being alerted are just minutes away from imminent danger, there is no readily available backup solution. That said, efforts to build an "earth-proof" cell system have recently received a boost.

On 29 March 2018, the FCC gave SpaceX its approval to build a space-based cellular service. This represents its "first approval of a U.S.-licensed satellite constellation to provide broadband services using a new generation of low-Earth orbit satellite technologies." SpaceX will likely be the first of many space-based cellular broadband solutions to develop in the future. Although SpaceX is focusing its initial service offering to underserved parts of the world, arrangements with FEMA to utilize this new service could be negotiated to use this infrastructure during loss of infrastructure emergencies before and after incidents. For Sonoma County and citizens in Puerto Rico immediately after the hurricane, a resilient space-based system could have become a lifesaver. In the meantime, when infrastructure fails, having an emergency evacuation and shelter-in-place plan remains the best advice.

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

GRIFFIN G510
FLIR