October 2023 EST 1998 MONTHLY EDITION

Domestic Preparedness Journal

REAL-WORLD INSIGHTS FOR SAFER COMMUNITIES

VOLUME 19 ISSUE 10

Business Office: 313 E Anderson Lane, Suite 300 Austin, Texas 78752

Staff that makes this publication possible:

Jasper Cooke – Publisher

Catherine "Cathy" Feinman – Editor

Bonnie Weidler – Publications Liasion

Madison Leeves – Marketing Coordinator

About the Staff

About the Advisors

Cover design: Madison Leeves.

For more information about the cover, please contact us at journal@tdem.texas.gov

Table of Contents

Graphic by Madison Leeves

Paul Cope

Director of the Master of Science in Homeland Security: Law and Policy Program, University of Kansas Law School

Paul Cope joined the University of Kansas Law School as the director of the Master of Science in Homeland Security: Law and Policy Program in 2021. He previously served as the chief of Cyber Law and Policy for the Kansas National Guard. As the lead cyber legal advisor, he provided legal guidance to leaders, addressing and developing national security policy and procedures to include cyber and intelligence incident responses. His former service with the Kansas National Guard includes appointment as the legal advisor (chief counsel) to the adjutant general of Kansas. He continues to serve as a judge advocate in the Kansas Army National Guard, where he holds the rank of lieutenant colonel. He earned a B.A. in Political Science from Pittsburg State University in 2006 and a J.D. from Washburn University School of Law in 2009.

Charles Guddemi

Director Statewide Interoperability Coordinator, Operations Division, DC Homeland Security and Emergency Management Agency

Charles Guddemi is the District of Columbia's Homeland Security and Emergency Management Agency's (HSEMA) statewide interoperability coordinator (SWIC). He is responsible for coordinating interoperability and communications projects involving voice, data, and video. He chairs the District's Interoperable Communications Committee and Cellular Industry/WiFi Provider Working Group. He serves as the secretary for the Statewide Interoperability Executives Council, is a member of the National Council of Statewide Interoperability Coordinators and current co-chair of FEMA's Region III Regional Emergency Communications Coordinators Working Group. He also participates on several Metropolitan Washington Council of Governments (MWCOG) committees and working groups. He joined HSEMA after a 25-year career with the United States Park Police (USPP). His assignments included working in Washington, D.C., New York Field Office, San Francisco Field Office, and the National Park Service Northeast Regional Headquarters in Philadelphia, Pennsylvania. He achieved the rank of deputy chief serving as the commander of the Services Division.

Mary Schoenfeldt

Board President, Green Cross Academy of Traumatology

Mary Schoenfeldt, Ph.D., is the board president of Green Cross Academy of Traumatology and has responded to countless disasters. She is an emergency management professional specializing in community and school crises and has a passion for disaster psychology. She is a faculty member of FEMA Emergency Management Institute, an adjunct faculty at Pierce College, and a subject matter expert for the U.S. Department of Education. She also serves clients through her consulting business. She can be reached at yoursafeplace@msn.com

Click here to meet the rest of the advisors


Graphic by Madison Leeves

Technology: Can't Live With It, Can't Live Without It

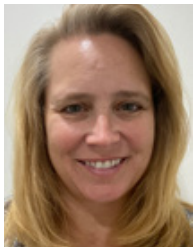
By Catherine L. Feinman

Technology marches forward continually, going from the introduction of smartphones and the launch of social media in the early 2000s to self-driving vehicles and augmented reality devices less than 20 years later. Such rapid changes challenge community leaders and emergency preparedness professionals in building truly resilient communities.

The October edition of the *Domestic Preparedness Journal* takes a deeper dive into some of these considerations within national preparedness, critical infrastructure, and emerging technologies. Events like the COVID-19 pandemic exposed planning gaps, not because the plans did not exist but because the plans were not familiar, inclusive, or scalable enough to ensure effective action when needed. Issues like food security and basic community needs reached critical levels in some areas. Organizations without specific plans for a pandemic rose to the challenge of addressing these issues and creating programs that will benefit communities long after returning to normal daily activities.

The 2021 Report Card for America's Infrastructure gave the U.S.'s aging infrastructure, which communities across the nation rely on for their daily activities, a C-. Critical factors may be overlooked when focusing on one's own company, agency, or jurisdiction. Hospitals, for example, rely on much more than just the Healthcare and Public Sector. It is essential to understand how that sector influences and is influenced by other critical infrastructure sectors, each of which also has evolving preparedness issues to consider in the decision-making process.

Concerning technology, there is no doubt that this factor is challenging to keep up with. It often seems complicated to believe that so much has changed in a relatively short period, thinking back to the earliest childhood memory of what technology looked like back then. Plans and processes have changed drastically regarding technology's impact on information, communication, learning, and other core tasks, and the articles this month address some of those issues.



Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as Editor of the *Domestic Preparedness Journal*, 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 recovery communities. 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.

Source: Unsplash/Ashkan Forouzani

COVID-19 – Emergency Plans and Readiness Exercises

By Rick Christ

The valuable lessons that COVID-19 taught community leaders about their emergency preparedness plans were often painful and expensive. However, not learning from those lessons would disrespect the virus's 6.9 million victims worldwide. There are no good excuses for these failures. While it is true that COVID-19 was a "novel" virus, that only mattered to virologists as they developed a vaccine. To everyone else, it was a virus – like the influenza virus – and plenty of warning and money was allegedly spent preparing for pandemic influenza. These plans' failures had little to do with the genomic sequence of the virus itself and more about what these plans were not:

- Familiar,
- Equitable and inclusive,
- Interconnected and scalable,
- Clear and actionable, and
- Resilient.

Familiarity

An internal unpublished after-action report that Crisis Prevention & Response Inc. conducted in 2022-2023 for a large midwestern state found that four of the five public health leaders who signed the most recent version of the state's pandemic plan in 2016 had left the agency by February 2020. As such, it is possible that the new senior public health leadership did not use that document during COVID-19 because they did not know it existed.

Signatures on plans are not formalities but rather the only way to know that leadership "owns" them. In the after-action report, since the leaders' successors did not sign the plan, there was no evidence that they were familiar with or aware of it, much less invested in it.

Making plans familiar to all stakeholders (senior leadership and the rank and file) subsequently includes training and exercising. Four key elements of a solid plan include:

- *Organizing* – Who (by position) will execute each plan element? Each element should be staffed three deep because the agency cannot count on everyone being in place when the crisis occurs or staying in that position until the situation ends.

- *Equipping* – What space, stuff, and systems are required to execute the plan? If all these elements are not normally in place (see the section on scalability below), where will the excess come from, and how will it be paid for? Within systems, what essential information elements are necessary to manage the problem? Where do those elements come from, and how do they get where they need to go?
- *Training* – Does everyone mentioned in the plan know how to execute the elements assigned to them? Training includes:
    - Familiarization with the organization,
    - Familiarization with the plan,
    - Technical training on relevant parts of the plan,
    - General emergency training, and
    - Leadership training for team leaders.
- Consider using a Position Task Book to document each person's progress toward excellence.
- *Exercising* – Are elements of the plan exercised frequently enough so that (a) people are comfortable with their roles and responsibilities, and (b) flaws are identified and resolved? Tabletop exercises can help find the plan's flaws, drills can test its execution, and full-scale exercises can determine how well they work in the larger picture of response activities.

Equitability and Inclusiveness

Frequently, a handful of well-intentioned emergency managers write plans with little influence from the people they intend to protect. As a result, planning documents are not actionable for many community members. "Nothing about us, without us!" plead advocates for vulnerable populations, including those with access and functional needs. More than translating documents into Spanish (though that is a good start), equity starts with understanding the people disasters may impact and recognizing these stakeholders' strengths and vulnerabilities. Inclusivity means including representatives from these populations in the development and testing phases.

Interconnectedness and Scalability

Planners often write each document from that agency's perspective on a single concern. One example of a siloed process is separate plans for COVID-19 testing and contact tracing. Contact tracing begins with a positive test result, but health agencies did not immediately connect these two systems. Without this connection, test results came back from disparate laboratories – each in their own format and through different channels, including fax and postal mail – and the data could not readily flow into a contact tracing program. The errors and delays that manual data handling caused gave time for the disease to spread before some patients could be contacted with their results.

Another example of siloed data processing is damage assessment information after a storm. For example, the local building department inspects the property to determine the building's safety for occupancy and files a damage report. A paper copy is then available to the property owner and other city agencies, each needing to track that property and manage information before the homeowner can obtain a permit to start repairs.

When exercising plans, it is imperative to know where each essential element of information comes from and how it gets safely to where it needs to go. Planners should ask how information is shared between agencies and with the public. If an agency cannot process data at scale, those within the agency cannot properly serve their constituents in an emergency.

Clarity and Actionability

Using passive voice may indicate that crucial information is missing. For example, "Employees will be notified" fails to identify *who* will notify employees and *how*. Exercises can dig deep into these vague statements and indicate how to make documents more precise for the agencies who own these plans. Without good communication and clarity in communication elements, agencies cannot fully execute their plans.

Questions to answer include:

- Who (by position) sends messages (and who fills in if the primary person is unavailable)?
- Are those messages pre-scripted, or must they be written and approved ad hoc (and, if so, what is that process)?
- Are the messages effective and accessible to all?
- What is the primary channel of communication for each message to each audience?
- How does the agency know and record that it received messages?
- What is the secondary communication channel in case the first is unavailable or fails to produce a response from all recipients?
- Do employees and other stakeholders know how to respond to these messages?

Reviewing the plan elements needed in a discussion-based exercise at this level of detail would add clarity and actionability to the document.

Resiliency

Each plan, written in a vacuum, assumes that the rest of the world will continue to operate under normal conditions when a particular crisis occurs. A significant lesson learned in the past few years is that crises are not independent isolated events. For example, major civil rights events occurred during COVID-19, as did some hurricanes. As such, mass gathering and sheltering plans that did not account for the pandemic were fraught with danger. In addition, all planning documents must work during a prolonged power outage because multiple other problems could result from the same storm or nefarious act that caused the power outage.

During the testing phase, consider how this plan might support other emergency plans during simultaneous catastrophes, each with cascading effects.

Improving Emergency Plans

There are many ways to improve the emergency planning process, including the following:

- Build plans to deliver essential services to constituents despite the risks rather than building them around the risks themselves.
- Include every constituent with a stake in the process, especially vulnerable and marginalized communities.
- Incorporate clarity and resilience in each document. Agencies will execute many plans on bad days with little practice and oversight. Make success possible, if not easy. Ensure multiple plans work seamlessly together within the organization and between stakeholder organizations.
- Test plans to ensure they work as intended. Keep testing because essential parts – like the people who execute them, the systems, and the locations – may change frequently.

Continuous improvement, not perfection, is the goal. If each activation of a plan, and each exercise of that plan, is carefully evaluated and documented, then the after-action report and improvement plan will contain a list of corrective actions to improve the plan, including: the organization of the plan (who does what); the equipment, facilities, and systems needed to execute the plan; the training of personnel to execute the plan; and future exercises of that plan. All plans should have a regular review schedule so organizations can ensure their policies and procedures stay current.

Rick Christ advises emergency management agencies and healthcare preparedness organizations worldwide on training and exercises. He has been designated a Master Exercise Practitioner and a Professional Continuity Practitioner by the U.S. Federal Emergency Management Agency. He designs, delivers, and evaluates exercises for state and local governments. He is a Lean Six Sigma Green Belt and an apostle for continuous improvement. Christ is a senior consultant with Crisis Prevention and Response, Inc.

(*Source:* Unsplash/ Ivan Bandura

Water and Wastewater Sector Perspectives

By Elston Johnson

The Cybersecurity & Infrastructure Security Agency (CISA) defines the Water and Wastewater Systems Sector as one of "16 critical infrastructure sectors." Due to the essential nature of water in so many aspects of society, this sector faces numerous challenges in maintaining the high level of service necessary to the communities they serve.

What Makes This Sector Critical To The Nation, And What Possible Effects Does It Have On States And Local Communities?

Water plays an integral role in daily life. Without a safe and sufficient supply of drinking water or proper disposal and treatment of wastewater, the daily lives of most Americans would be significantly impacted. Without access to clean water for drinking, food preparation, and bathing, individuals are more susceptible to disease from exposure to contaminants. Absent proper collection, treatment, and disposal of wastewater effluent, individuals and the nation's water bodies could be exposed to biological and chemical contaminants. Industrial processes essential for manufacturing and other utility services, such as electricity generation, are impacted by water and wastewater service disruptions.

On August 1, 2023, the Federal Emergency Management Agency (FEMA) announced they were implementing the new "Water Systems' Community Lifeline" construct according to the Environmental Protection Agency (EPA) Water Resilience website. FEMA explains that the implementation of this construct will help the agency "increase effectiveness in disaster operations and better position the agency to respond to catastrophic incidents." This announcement further emphasizes the importance of the Water sector in the security of the nation's communities.

On August 30, 2023, Florida was dealing with the landfall of Hurricane Idalia, which by that time had already caused close to 300,000 power outages. The impacts of Hurricane Idalia came less than a year after Hurricane Ian made landfall in Florida, resulting in more than 2.5 million customers in the state without power. The loss of power contributes to the loss of drinking water and wastewater services due to the need for electricity to power some treatment units.

The Texas Comptroller of Public Accounts assessed the impacts of Winter Storm Uri on the Texas Economy in a 2021 Fiscal Note to the 87th Legislature. In the Fiscal Note, the University of Houston Hobby School of Public Affairs conducted a survey and found that almost half (49%) of Texans had a water service disruption. The disruptions were caused by the extreme cold temperatures freezing water distribution lines, customer service lines, interior commercial and residential plumbing, valves, and other equipment

used in the water distribution process. Additional disruptions occurred as the frigid temperatures resulted in the loss of electrical power for several facilities. The Comptroller's Fiscal note also indicates the impacts of Uri resulted in economic losses between $80 billion and $130 billion and claimed at least 210 lives. The disruption of water service highlighted how integral the Water and Wastewater Systems Sector is to society's normal functions. Some of the common health impacts of water service interruptions include diarrhea and other gastrointestinal diseases. An example of an industry impacted by the disruption of water service is restaurants:

> *The interruption of electrical service is an imminent health hazard in any food service establishment, particularly because it can hamper a facility's ability to refrigerate and cook foods, as well as sanitize properly.* (*Power Outage Preparation & Recovery, Steritech*)

What Are This Sector's Key Assets And Interconnected/Interdependent Systems (Physical Or Cyber)?

For water supply facilities or public water systems, the key asset is the source of water that is being captured and conveyed for treatment. For example, larger cities such as Houston, Texas, obtain the majority of their water to treat and provide to their customers from a combination of lakes and rivers. Smaller communities such as Brookings, South Dakota, primarily obtain their water from wells that pump water from underground aquifers. Once treated, the sourced water is distributed to customers for one or more potable water uses. Wastewater is captured from commercial facilities and residences and then conveyed to a wastewater treatment plant to receive additional treatment prior to disposal into a waterbody or onto land through irrigation.

The collection, conveyance, distribution, and treatment systems for water and wastewater comprise various equipment and facilities such as pumps, piping systems, and treatment units. These treatment facilities transfer water through a series of units to remove contaminants through processes that include adding chemicals for enhanced solids separation, filtration, and additional chemical application of disinfectants. The treated water is then distributed to customers through a combination of storage facilities, pumps, and a network of underground pipes, commonly called the distribution system. Drinking water systems are required to treat water by using the facilities listed above to reduce or remove a standard set of contaminants called the National Primary Drinking Water Standards from water prior to serving it to customers.

In the same way, wastewater is collected from commercial facilities and residences through a separate network of underground pipes and pumped to wastewater treatment plants for treatment before discharge into a lake, river, stream, or soil through irrigation systems. Wastewater treatment plants are typically issued site-specific permits that list contaminants and the levels they must be reduced to in the wastewater before the wastewater can be discharged into a body of water or used for irrigation.

Both drinking water and wastewater treatment units are typically made up of basins to apply chemicals to water and provide detention time to allow biological and chemical reactions to remove contaminants from water. In addition, these facilities are increasingly being monitored and operated remotely using an information system known as industrial control systems (ICS) or supervisory control and data acquisition (SCADA) systems. The National Institute of Standards and Technology defines ICS as "an information system used to control industrial processes such as manufacturing, product handling, production, and distribution." More integration of the ICS and SCADA systems into the Water and Wastewater Systems Sector has provided a point of access for cyber criminals to access and attempt to compromise the operations of the water and wastewater treatment facilities. These systems comprise the sector's key assets and are necessary for the continued provision of safe drinking water and properly treated wastewater.

An example of how vital the ICS and SCADA systems are to water systems is the remote intrusion into the SCADA system of the City of Oldsmar's water treatment plant in 2021. The online intruder was able to manipulate the ICS controls for the chemical dosing system. Fortunately, a water system operator noticed the changes and was able to deter the intruder. Listen to what investigators said about the Florida City water treatment system "intruder" hack.

What Are This Sector's Dependencies (Physical, Cyber, Geographic, And Logical) And Interdependencies With Other Critical Infrastructures?

The collection, conveyance, distribution, disposal, and treatment processes for water and wastewater depend on the Chemical, Energy, Critical Manufacturing, and Transportation Systems sectors. The treatment processes rely heavily on chemicals, electricity, equipment, and

supplies to properly remove or treat contaminants. Additionally, the equipment and tools used to repair and maintain this equipment are impacted by disruptions in these sectors. Impacts on the Transportation Sector increase the time to obtain essential chemicals and parts necessary for treatment. The trend of more automation coming into the Water and Wastewater sector has significantly increased the dependency on both the Energy and Critical Manufacturing sectors. More automation has resulted in the need for different types of high-tech equipment like Smart Water meters that rely on parts that have to be manufactured and shipped to the water and wastewater systems.

Electricity is essential for producing drinking water and the treatment of wastewater. The pumps used to move water and wastewater through treatment units as well as drinking water distribution systems and wastewater collection systems, require electricity to operate. Some examples of treatment units are pumps used in a number of municipal water and wastewater treatment applications including sedimentation basins to facilitate solids separation, chemical application, and ultraviolet light for disinfection. Public health and the environment can be adversely impacted without the timely distribution of drinking water to customers or the collection of wastewater for transport to treatment plants. According to the EPA's Power Resilience Guide, "Inoperable pumps at a drinking water utility can … make firefighting difficult, and cause local health care facilities and restaurants to close." The guide also states, "For wastewater utilities, pump failure may lead to direct discharge of untreated sewage to rivers and streams or sewage backup into homes and businesses."

Water systems heavily depend on the Chemical, Critical Manufacturing, and Transportation Systems sectors because of the need for chemical compounds for the treatment processes of both drinking water and wastewater. The chemical manufacturers produce the chemicals essential to the treatment processes required to treat drinking water to safe quality levels. Chemicals are also used in the processes to treat wastewater to appropriate levels for disposal. These chemicals need to be transported to drinking water and wastewater treatment facilities all over the country. Interruptions to normal transportation routes from human-caused or natural incidents can cause supply chain shortages that can impact the amount of chemicals and other equipment and supplies available for use by water and wastewater utilities.

An example of the effects of supply chain interruptions is in the EPA case study on the Des Moines Water Works (DMWW) water utility and the COVID-19 impact on Carbon Dioxide production. Carbon Dioxide is necessary for some of the treatment processes at the DMWW and is defined as a "byproduct of other processes, including the manufacture of ethanol, oil and natural gas refining, and ammonia and hydrogen production." The case study stated that the "Lack of drivers on the road and the lowered demand for ethanol led many ethanol manufacturers to reduce their production levels or, in some cases, shut their plants. When this happened, CO_2 shortages quickly followed."

The role of the Critical Manufacturing Sector and the impacts on that sector from the COVID-19 pandemic were also researched by the EPA, which published, "Understanding Water Treatment Chemical Supply Chains and the Risk of Disruptions, December 2022." The report evaluated the supply chain risks of 46 chemicals used as either raw materials or direct additives in water treatment. A number of factors were evaluated including the chemicals, "Applications in Water Treatment, Manufacturing Process, Domestic Production, Trade and Tariffs and History of Shortages" (see the EPA's Understanding Water Treatment Chemical Supply Chains and the Risk of Disruptions).

What Are This Sector's Current And Emerging Vulnerabilities, Hazards, Risks, And Threats?

The Water and Wastewater Systems Sector faces increasing threats to the mission of providing safe drinking water and adequately treated wastewater to its customers. The sector faces vulnerabilities, hazards, risks, and threats associated with aging infrastructure and the increase in extreme weather events. The impact of extreme weather events, like Hurricanes Harvey and Katrina, are familiar and costly threats to water utilities in the coastal areas of the United States. These types of events have caused significant structural damage from flooding, high winds, and power outages. The National Oceanic and Atmospheric Administration (NOAA) reports that these two events are the costliest weather events ever to impact U.S. coastal areas. NOAA's Office for Coastal Management says, "Hurricane Harvey alone had total costs of $125 billion – second only to Hurricane Katrina in the period of record, which had an approximate cost of $161 billion."

The August 2023 water main break in Times Square, New York, is an example of the consequence of not adequately addressing aging infrastructure. Based on a report from CBS News New York, "The pipe that broke in Midtown on Tuesday was more than 120 years old. The water main break is putting a spotlight on a major issue across the country: aging infrastructure."

Aging infrastructure, particularly the deterioration of drinking water distribution lines and wastewater collection lines, can threaten public health and the environment. Leaking distribution lines can provide a pathway for microbial and chemical contamination of treated water distributed to customers. Deterioration of wastewater collection lines can result in untreated sewage spilling on the ground or into creeks, lakes, rivers, and streams.

The major emerging threat for the Water and Wastewater Systems Sector is cyberattacks. Cyberattacks have occurred at all types of water and wastewater utilities. According to the HackerNoon website:

> *[I]n 2021, twin cyberattacks hit water sector facilities in San Francisco, California, and Oldsmar, Florida. Both attacks involved the use of a remote access program called TeamViewer. This app is commonly used in the utility industry for tasks like remotely monitoring water treatment and supply data. However, hackers abuse it to manipulate water sector companies' systems illegally. Luckily, both attacks were stopped before they caused any harm.*

The constant threat of cyberattacks has become a reality for all critical infrastructure sectors. The American Water Works Association (AWWA) Report on Cybersecurity Risk and Responsibility in the Water Sector states:

> *Cyber risk is the top threat facing business and critical infrastructure in the United States. Government intelligence confirms the Water and Wastewater Sector is under a direct threat as part of a foreign government's multi-stage intrusion campaign.*

The AWWA report also describes the impacts of a cyberattack on water utilities and how devasting those impacts can be for a community:

> *Attacks causing contamination, operational malfunction, and service outages could result in illness and casualties, compromise emergency response by firefighters and healthcare workers, and negatively impact transportation systems and food supply.*

The impacts described illustrate how disruptive a cyberattack can be to a water utility and the critical role the Water and Wastewater Systems Sector plays in maintaining public health and safety. Cyberattacks on the industrial control systems can have a significant impact on the operations of a water utility. Equally as damaging are ransomware attacks on water utility billing systems. The well-publicized ransomware attack on the City of Atlanta demonstrates how a cyberattack can severely impact a utility:

> *For roughly a week, employees with the Atlanta Department of Watershed Management were unable to turn on their work computers or gain wireless internet access, and two weeks after the attack, Atlanta completely took down its water department website "for server maintenance and updates until further notice."*

The importance of addressing cybersecurity issues is highlighted by the recently released U.S. Environmental Protection Agency memorandum, "Addressing PWS [Public Water Systems] Cybersecurity in Sanitary Surveys or an Alternate Process" (Radhika Fox, Assistant Administrator, EPA, March 3, 2023). The memorandum outlines some approaches the EPA requires of State Drinking Water programs to ensure public water systems put in place measures to protect their facilities from cyberattacks. States and Water Associations are challenging the approach and process outlined in the memorandum, but all agree on the importance of taking actionable steps to address the growing threat of cyberattacks on water utilities.

How Would A Human-Caused, Natural, Or Technological Disaster Impact This Sector's Preparedness, Response, And Recovery Efforts?

Human-caused and natural disasters' impact on the Water and Wastewater Systems Sector is typically significant. The preparedness, response, and recovery efforts utilized during the disaster differ based on the incident and the utility's resilience to the hazards associated with the incident.

As mentioned above, natural disasters such as droughts, floods, hurricanes, tornadoes, and winter weather can substantially impact water and waste facilities' ability to provide water service to their customers. A common impact of hurricanes is flooding due to excessive rainfall and storm surge. Water and wastewater treatment plants can be inundated with flood water and must be taken offline until the water recedes and repairs are made. Lack of water service can slow emergency response and recovery efforts. Responding personnel must provide alternate potable water supplies to the affected populations and themselves. Impacts to wastewater lift

stations result in "untreated sewage can back up into homes, businesses, and critical facilities and flow into waterways, causing a threat to public health and the environment."

Human-caused disasters can also have devastating impacts on water and wastewater facilities. Increased production of chemical compounds has increased the risk of accidental contamination of treated water. In the *Baseline Information on Malevolent Acts for Community Water Systems* report, the EPA states, "Utilities experience accidental contamination of finished water twice per year, and 10% of these incidents have significant public health or economic consequences." These types of incidents would impact health care facilities, residential areas, manufacturing facilities, and emergency services' water use. Response and recovery efforts would slow significantly until potable water service is restored, requiring disposal of contaminated water and decontamination of the water utility facilities.

Without a safe and sufficient drinking water supply or proper wastewater disposal and treatment, most people's daily lives would be significantly impacted.

Earlier in this article, some examples described impacts on the technological capabilities of water and wastewater systems by cyberattackers over the last few years. The increased use of automation in all critical infrastructure sectors has increased susceptibility to severe cyberattack impacts. Another example from HackerNoon is that, "in 2018, the Onslow Water and Sewer Activity Authority in North Carolina had to shut down its IT network after two back-to-back ransomware attacks."

Due to the unique nature of each water and wastewater utility, the consequences can worsen based on each impacted utility's preparedness, response, and recovery capabilities. The AWWA Cybersecurity Risk and Responsibility in the Water Sector report discusses how the variability in structure and governance can cause significant obstacles to managing cyber risk. The report highlights that water and wastewater utilities typically have a "fractured organizational structure, often embedded within a multifaceted municipality." The report also mentions that "a prevalence of legacy – sometimes antiquated – systems increase the challenges of managing cyber risk."

What Else Do Emergency Preparedness, Response, And Recovery Professionals Need To Know About This Sector?

One of the main activities that can increase the Water and Wastewater Systems Sector's overall preparedness, response, and recovery activities is more coordination and recognition of the interdependency with other critical infrastructure sectors. Continued coordination efforts outside of response and recovery incidents between the Water and Wastewater Systems Sector and representatives from the Energy, Food and Agriculture, Chemical, Healthcare and Public Health, Emergency Services, and Transportation Systems sectors will increase overall community-level resilience. Understanding the water supply and wastewater treatment needs of each of these sectors can drastically improve resilience at the local level. The EPA's Community-Based Water Resiliency Guide provides examples of the types of interdependencies. The key for the Water and Wastewater Systems Sector is to interact with the other critical infrastructure sectors in their communities to ensure effective information exchange and adequate planning.

The Water and Wastewater Sector can provide opportunities such as educational and public outreach campaigns for the other sector partners to understand how crucial their partnership with the Water and Wastewater Sector is to maintaining stability locally, regionally, and nationally. Regular coordination through Local Emergency Planning Committees (LEPCs) and involvement in other community-wide activities and organizations will also improve awareness and visibility of this sector.

Elston Johnson has more than 25 years of experience in the water industry. His expertise includes drinking water and wastewater permitting, regulatory compliance, and preparedness. Mr. Johnson has worked with all sizes and types of water and wastewater utilities, assisting with the development of emergency response plans and risk assessments as well as providing training on a variety of water security topics. He received a Bachelor of Science Degree in Bioenvironmental Sciences from Texas A&M University and a Master of Science in Environmental Science from the University of Texas at San Antonio.

National Tribal Emergency Management Conference (*Source*: Harmony Holland, September 16, 2023).

National Preparedness Efforts Among Tribal Communities

By Lynda Zambrano and Catherine L. Feinman

Shortly after the September 11 terrorist attacks in 2001, the lead author attended a Washington State Homeland Security meeting on behalf of the Tribe she was working for. Armed with the knowledge that the Tribe patrolled more than 4,417 square miles of Puget Sound, which included an international border, international shipping lanes, oil refineries, the statewide ferry system, naval bases, and more, the Tribe had great assets and intel to contribute to homeland security efforts. The primary mission was to learn more about the new U.S. Department of Homeland Security, its programs, and the new relationships that were being forged. The secondary mission was to learn more about the new grant opportunities that were being offered to help better protect the homeland. However, noticing that she was the only tribal representative and only female in the room – and that none of the allocated funding was going to the Tribes – she recognized that not including the Tribes could leave large gaping holes in the process and put the country at great risk. That experience launched an emergency management career that has been building interest in emergency management practices among tribal communities throughout the United States and Canada.

The National Tribal Emergency Management Council (NTEMC) originally began as a sub-committee of a regional homeland security council and a pilot project in 2002 and was formally established in 2008 as a 501c3 not-for-profit organization to assist the Tribes with the development of all public health and public safety programs, to include their offices of emergency management, homeland security programs, and public health. The NTEMC announced in 2010 its mission to help build emergency management agencies and functions within Tribes across the entire country. With hundreds of years of combined experience, council members include tribal men and women who bring a wealth of background knowledge in emergency management, law enforcement, firefighting, forestry, emergency medical services, agriculture and food sovereignty, hazardous materials, utility and water resources, communications, and elected leadership. Tribal emergency managers share many similarities with their nontribal counterparts, but there also are key differences.

While adhering to the mission areas and core capabilities outlined in the National Preparedness Goal, tribal emergency management tends to be more personal. Governing a Tribe can be likened to protecting a large family and extended families and all their homes and properties across a large geographic area. In addition, historically, nomadic people and cultures are now tied to specific geographic regions. Instead of their traditional movement toward food and survival resources, they are learning to adapt and overcome the challenges of modern society and influences that have altered their way of life. For example, the tribal custom of drying and storing food has transitioned to current freezing, freeze drying, and canning methods to preserve seasonal food sources throughout the year.

Annual Tribal Conference

The NTEMC Annual Conference was held in person on August 11-18, 2023, for the first time since COVID-19 restrictions were lifted in Tulalip, Washington. The Tulalip Tribe welcomed everyone (tribal and nontribal attendees) to their homeland with a prayer song, opening prayer, and full presentation of the colors by distinguished members of The United States Joint Services Command. The event brought together a mixture of rich cultures and many disciplines of emergency management.

Because tribal emergency management is a family endeavor, conference participants included husbands and wives, parents and children, and others described as "like family." As relationships develop, they quickly move beyond typical business transactions. Tribes do not all have established emergency management agencies. Still, they naturally embody the traits of emergency preparedness and response by retelling stories passed down through generations about great disasters (e.g., Thunderbird and Whale, which is about an earthquake and tsunami) and passing down survival skills such as hunting, fishing, and gardening.

Common Concerns With Unique Challenges

Emergencies such as earthquakes, tsunamis, volcanoes, mudslides, and food insecurity are not unique to tribal communities, but there are additional considerations and challenges that tribal leaders must consider. Some issues shared by conference participants could be found within any jurisdiction – for example, identifying and addressing *all* the potential hazards, building hazard-specific programs for areas prone to that hazard (e.g., wildfire management), gaining leadership buy-in to build emergency management capabilities, and recruiting and retaining volunteers. The following concerns, though, are more specific to Tribes:

- Lack of coordination between tribal and nontribal communities;
- Losing cultural heritage and practices such as locally growing food, using traditional cooking methods, hunting, fishing, etc.;
- Lack of understanding of tribal sovereignty within multijurisdictional planning programs;
- Nontribal government agencies' expectations that Tribes will handle their emergencies without outside assistance;
- Gaining agreement from tribal leadership within and across Tribes;
- Fear of food supply issues due to the interconnectedness of the ecosystem, climate, and species decline;
- Historical trust issues among Tribes concerning outside agencies;
- Conflicts between tribal, county, state, and federal politics;
- Misconceptions that tribal gaming equates to wealth and less need for external assistance;
- Cultural resources and properties not being included in national priorities; and
- Difficulty meeting requirements of federal relief funding when they conflict with the timeframes and resources Tribes need to apply.

Other issues include large-scale daily operations typically handled by federal agencies in international border communities. For example, the Blackfeet Reservation in Browning, Montana, which covers 1.5 million acres, provides a backup emergency operations center for NTEMC for future disasters that affect tribal communities in the northwestern region. Spanning about 60 miles of the Canada-U.S. border, the Blackfeet Nation is responsible for disaster and homeland security services, including air and land patrols for reconnaissance and surveillance of human trafficking, drug smuggling, terrorist threats, and other illegal activities.

The NTEMC also helps coordinate other large-scale disaster and humanitarian operations. For example, during the COVID-19 response, NTEMC joined forces with Farmer Frog (a sister non-profit and national distribution operation that specializes in farming systems and food sovereignty) to collect and distribute food, personal protective equipment (e.g., masks and gloves), and other supplies to tribal communities and the surrounding area. In the first two years of the COVID response, together, they distributed more than 200 million pounds of food, water, and supplies.

Action Items for Nontribal Agencies and Organizations

At the NTEMC Conference, leaders acknowledged that they want what is best for their Tribes, which sometimes means working with outside entities. However, some collaboration barriers still exist. Here are suggestions that tribal participants shared that could help outside entities bridge the gaps that exist between them and their tribal partners:

- Identify and build relationships before a disaster;
- Clarify the roles and responsibilities of outside agencies before a disaster;
- Establish and meet mutually beneficial expectations;

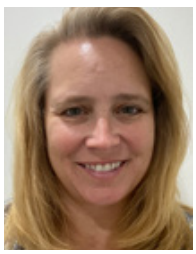
- Develop recovery plans together with tribal and nontribal governments;
- Consider coordinating with tribal communities to meet assistance thresholds when making county and state funding requests;
- Make informational resources more available, especially to remote villages;
- Include trauma-informed care into the plan for out-of-the-norm events;
- Ask the right questions before, during, and after a disaster (e.g., One Tribe answered "No" when asked if it was affected by a mudslide because the mudslide did not go into the village. However, if the Tribe were asked, "How did the mudslide affect you?" the answer would have been it disrupted the power, connectivity, transportation, and other critical resources the village depends on.);
- Understand that many tribal food sources are hunted and gathered seasonally and are not as replaceable in grocery stores as in other communities;
- Ensure that fundraising efforts match the resources needed for daily life, which may differ from nontribal community needs;
- Learn from Tribes about their resources, tribal customs and practices, spiritual needs, and leadership processes.
- Respect cultural differences such as ceremonial items, worship customs, and sacred places; and
- Avoid stereotypes and misconceptions (e.g., tribal members pay taxes, own vehicles, and do not all live in teepees).

Here are a few examples of federal agency efforts to build better tribal relations:

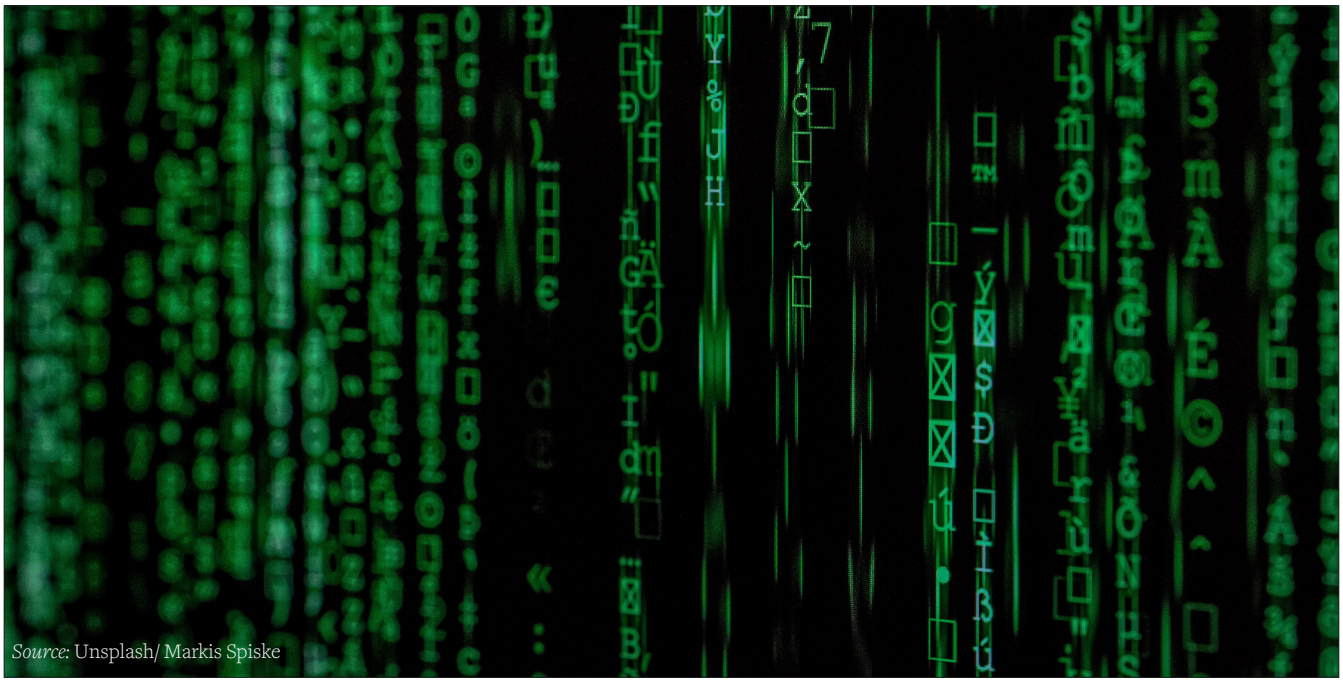
- Read and ensure that local tribal emergency managers are aware of the Federal Emergency Management Agency's (FEMA) 2022-2026 National Tribal Strategy, which FEMA released in August 2023;
- Review the U.S. Government Accountability Office's Tribal and Native American Issues webpage to learn more about tribal concerns;
- Learn how the Cybersecurity and Infrastructure Security Agency (CISA) and the FirstNet Authority are expanding tribal emergency communications with Tribes across the country;
- Consider building outreach programs and engaging tribal liaisons to bridge preparedness and response gaps (e.g., U.S. Geological Survey and U.S. Bureau of Indian Affairs).
- Learn about the National Advisory Council (NAC) to FEMA.
- Learn about the efforts of the U.S. Department of Homeland Security to establish the first ever Tribal Homeland Security Advisory Council (THSAC).

The NTEMC identified four main questions that tribal emergency managers must ask to reach their preparedness goals: (1) Who do we talk to? (2) What do they do? (3) How can we collaborate? (4) How can we reinvigorate our customs and traditions to better prepare the next generation? Nontribal emergency managers should ask the same questions and contact their tribal counterparts to build partnerships and collaboration. Mutual respect and understanding are the starting point for bridging the gaps in disaster preparedness, response, and recovery efforts.

Lynda Zambrano is the executive director of the National Tribal Emergency Management Council, a nonprofit organization providing free consultative services in homeland security and emergency management as it pertains to the areas of planning, mitigation, response, and recovery for more than 277 member tribes throughout the United States.



Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as Editor of the *Domestic Preparedness Journal,* 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 recovery communities. 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.



Source: Unsplash/ Markis Spiske

Information Technology Sector Perspectives

By Paul Galyen and Nathan DiPillo

The Information Technology (IT) Sector is one of the 16 critical infrastructure sectors under Presidential Policy Directive 21 (PPD-21) and is critical to the nation's security, economy, public health and safety, government, and academia, and provides citizens with IT Sector services such as the internet. According to the U.S. Department of Homeland Security (DHS), the vision of the IT Sector is "to achieve a sustained reduction in the impact of incidents on the Sector's critical functions."

What Makes This Sector Critical to the Nation and What Possible Effects Does It Have on States and Local Communities?

The IT Sector produces and delivers products and services that support the effective operation of the worldwide information-based civilization. As technology becomes more integrated into daily functions, the dependency on IT and the IT Sector grows exponentially. In a 2001 interview, Bill Gates said, "The advance of technology is based on making it fit in so that you don't really even notice it, so it's part of everyday life." IT products and services also have become essential to other critical infrastructure sectors' daily operations and services. Government, commercial, and industrial collaborations and partnerships are crucial for enhancing IT products and services and identifying continuous risk reduction across critical infrastructure sectors. The IT Sector is connected to other prime lifeline systems like communications and energy, which sustain thriving communities. The IT Sector was added to the DHS critical infrastructure sector to encompass all types of IT systems. Although this definition is broad, this sector will become more complex with other technology integration like position, navigation, and timing systems, artificial intelligence, and other future technologies.

The IT Sector is a function-based sector encompassing physical hardware and wires, virtual systems, network operations, and cybersecurity controls for the private and public sectors. Figure 1 describes the six critical functions that support services and product production.

IT advancements in the past two decades have been the epicenter of transformation for private sector operations and processes. They have revolutionized the workplace regarding efficiency, convenience, and effectiveness in serving customers and employees. However, the federal government and some state governments have missed out on technological innovations and digital transformation largely due to poor management of IT projects – leading to technology projects being hundreds of millions of dollars over budget, implementation taking years rather than

months, and delivered technologies being obsolete by the project's completion.

What Are This Sector's Key Assets and Interconnected/Interdependent Systems (Physical or Cyber)?

The IT Sector comprises three major industrial groups critical in manufacturing and delivering IT products and services. These three industry groups are IT hardware and equipment, IT software and services, and semiconductors and semiconductor equipment, which comprise IT equipment's physical components.

IT depends on hardware and equipment, broken down into three main industries: communications equipment; technology hardware, storage, and peripherals; and electronic equipment, instruments, and components. IT communications equipment includes routers, switches, telephones, and switchboards. The companies within these industries produce communication equipment, including satellite communication, and local area network (LAN), wide-area network (WAN), and metropolitan area network (MAN) capabilities. Technology hardware, storage, and peripherals include computers, laptops, printers, motherboards, processors, graphical processing units, and mobile devices like tablets and cellphones. Electronic equipment, instruments, and components include companies that make equipment like barcode scanners, transformers, security systems, resistors, lasers, and electric coils. All these physical parts and pieces depend on a consistent qualitative supply chain. After the emergence of COVID-19, demand for semiconductors increased, but their slow supply chain impacted vehicle and other medical equipment production.

The IT software and services industry group includes companies that provide internet services, as well as companies that provide software and IT services like cloud environments. Internet services include Internet Service Providers (ISPs) and companies that offer interactive services or online databases, such as social networks, online shopping, or search engines. IT services include companies that provide IT consulting or data processing services to private sector companies or government departments. Finally, software consists of any software for business or consumer use, ranging from enterprise software, systems software, and education software to entertainment such as video games.

Semiconductors use materials (e.g., silicon) that can conduct electricity under specific conditions but not others, making them ideal for controlling electrical currents. This industry group includes semiconductor manufacturers and companies that make peripheral equipment for semiconductors.

What Are This Sector's Dependencies (Physical, Cyber, Geographic, and Logical) and Interdependencies With Other Critical Infrastructures?

Power, cooling, raw materials, and data transmissions are the highest dependencies for the IT Sector to provide products and services that allow other critical sectors to operate optimally. Since these dependencies span physical and geographical, supply-chain interruptions or the above-listed dependencies would adversely impact this sector's continued operations. COVID-19 highlighted gaps in the IT equipment supply chain. According to Bloomberg:

> *The semiconductor shortage has been described as due to a "perfect storm" of factors. Prior to 2020, there were already difficulties in obtaining inputs for production, including semiconductor manufacturing equipment used to make older varieties of chips, and components used in electronic assembly such as diodes, capacitors, and substrates.*

Providing IT services is power-intensive. Any electricity supply interruption would severely impact IT products and services, resulting in a massive disruption to operations because of the strong physical dependency on the Energy Sector and local energy operations. Large data centers providing cloud services by companies like Microsoft, Amazon, and Google consume energy to power hardware, provide cooling, and ensure the overall operation of the support hardware, such as storage servers, routers, switches, and physical security controls. In 2022, Microsoft announced it would pay over $800 million in extra energy costs to operate its data centers worldwide. These large data centers have alternative or backup power supplies for short power outages or power disruptions, but a large-scale power outage or power shutdown would significantly affect their services.

Cooling is imperative when running data centers that provide services on a global scale. Many data centers

rely on industrial-scale cooling equipment to keep hardware from overheating due to prolonged operation and service uptimes. Cooling centers also may depend on remote monitoring operations. Without proper cooling, the components within equipment such as processors, transceivers, resistors, motherboards, or other electronic microchip components could be destroyed. Although most companies manage "on-premises" data centers, some have been considering alternatives to cool their data centers efficiently and reduce their carbon footprint. For example, Microsoft has been exploring the idea of underwater data centers to increase the performance and reliability of data centers.

Raw material supply and transportation issues also can arise when suppliers experience operational interference. IT equipment and hardware materials include plastics, steel, aluminum, copper, platinum, gold, and silicon:

- Plastics, steel, and aluminum are necessary for building equipment cases or chassis and protect internal components, like the motherboard and central processing unit. These physical dependencies rely on the output of another functional linkage between the input and output of more than two assets or commodities.
- Due to its electrical and thermal conductivity, copper is abundant in electrical appliances or devices in homes and offices. Copper is highly pliable and malleable, making it perfect for applications in cabling, wiring, and internal electronic components.
- Gold is useful for bonding transistors, printed circuits, and diodes for wires due to its excellent ductile and malleable properties.
- Platinum is ideal for its corrosion resistance and strength under extremely high temperatures and is in computer parts and components.
- Silicon is an abundant and plentiful element and is a central component for making solid-state drives and transistors.

Data transmission (i.e., digital communication) is the transfer and reception of data through a digitized analog signal or digital bitstream transmitted over a point-to-point or point-to-multipoint communication channel. Data transmission could broadly be considered broadcasting. Some information systems depend on other physical or virtual systems to provide a service or complete a transaction. Some examples include a webpage communicating with a database that tracks user login information to verify if the user's credentials are authorized to access a system or an email system communicating with another email system to deliver a message. A dependence of this communication is the undersea internet cables that connect the internet from one continent to another. These cyber and physical dependencies span the need for communications equipment to have faster speeds and the need for fiber networks and processes that provide faster or more efficient data transmission.

What Are This Sector's Current and Emerging Vulnerabilities, Hazards, Risks, and Threats?

One key risk to the IT Sector includes cyberattacks that can target IT systems with insufficient security controls, outdated systems that have not applied security patches, zero-day vulnerabilities, insider threats, or elaborate social engineering attacks that attempt to gain administrator-level credentials. These attempts could allow a malicious actor to access critical systems or disrupt daily operations by tampering or sabotaging hardware or services.

One notable cyberattack in 2010 involved a cyberweapon known as Stuxnet, a powerful computer worm in an Iranian computer that took advantage of a Microsoft Windows zero-day vulnerability and controlled the centrifuges. The worm checked for a specific programmable logic controller (PLC) model that controls industrial machinery like uranium centrifuges. The worm then altered the programming on the PLC and caused the centrifuge to spin out of control while sending data that the PLCs were operating normally back to the operator's computer. The false-normal information made the attack harder to detect and respond to before the worm caused too much damage. Stuxnet's failure to erase its electronic fingerprints and avoid capture raise concern that other unfriendly state and non-state actors might modify and use it to threaten the IT Sector.

A more recent cyberattack against critical infrastructure was the Russian attack on the Ukrainian power grid in 2015. Ukraine suffered a large-scale cyberattack that turned the power off to a major portion of Ukraine's

power grid, causing widespread blackouts for 225,000 Ukrainian citizens. During another power outage in 2017, medical professionals had to resort to pen and paper prescriptions to ensure the distribution of medications to critical patients.

Cybercrime turned the internet into a breeding ground for theft, fraud, and abuse. Cybercriminals took advantage of misaligned networks through the COVID-19 pandemic as businesses moved to remote work environments. In 2020, malware attacks increased 358% compared to 2019. Cybercrime turned the internet into a breeding ground for theft, fraud, and abuse – from simple small criminal rings looking to make money stealing digital information from personal computers to large, organized crime syndicates and nation-state-backed organizations specializing in corporate espionage, extortion, intellectual property theft, and unauthorized access to government classified information.

In 2022, the cost of cybercrimes reached $6 trillion, with 80% related to phishing attacks. One high-profile cybercrime case involved the Chinese company Sinovel Wind Group, which stole intellectual property from U.S. company American Superconductor (AMSC) over three years to boost China's wind turbine production. At the trial, AMSC claimed to have lost over a billion dollars in shareholder equity and about 700 jobs, losing over half of its global workforce due to the theft.

One risk to the IT Sector is the global supply chain and the transportation of goods. The U.S. supply chain relies on having goods and raw materials arrive "just in time." When one piece of the chain fails, the whole system can collapse and halt. The COVID-19 pandemic showed how fragile the supply chain system was and how it greatly impacted the ability for the U.S. to receive raw materials and goods from foreign countries. The pandemic, combined with a semiconductor shortage in 2020, affected the sector's ability to provide computers, mobile phones, car electronics and components, and computer parts and peripherals.

The IT Sector produces and delivers products and services that support the effective operation of the worldwide information-based civilization.

Another risk is the cost of internet services. High costs could lead to minimal efforts to create a secure environment or connect rural communities as the internet becomes a new normal for families and businesses. In a rural Nebraska community in 2023, it cost approximately $53,000 to get internet to homes for the Winnebago Tribe using fiber optics:

> *The U.S. has committed more than $60 billion for what the Biden administration calls the "Internet for All" program, the latest in a series of sometimes troubled efforts to bring high-speed internet to rural areas.*

How Would a Human-Caused, Natural, or Technological Disaster Impact This Sector's Preparedness, Response, and Recovery Efforts?

As climate changes impact the environment, current studies are considering the short- and long-term effects of these changes on the existing critical infrastructure, particularly the power grid and telecommunication. For example, heatwaves reduce the generation efficiency of power grids, increase power transmission and distribution loss, decrease the lifetime of equipment such as power transformers, increase peak power demand, and sometimes force power plants offline, resulting in brownouts or rolling blackouts.

Losing power, technology systems, or telecommunications significantly affects communities, government, and daily operations. For example, Hurricane Sandy in 2012 disabled 25% of U.S. East Coast mobile phone towers. At the same time, the loss of electricity forced many mobile phone carriers and ISPs offline, meaning companies and residents could not send or receive information. Wireless infrastructure, fiber infrastructure, and data centers are at high risk of damage associated with storms, tornadoes, hurricanes, typhoons, tropical storms, floods, heat, and wildfires. High winds and wildfires can incapacitate power lines, transmission towers, telephone lines, and microwave receivers. In 2017, Hurricanes Maria and Irma destroyed 90% of mobile phone towers in Puerto Rico, St. Martin, Dominica, and Antigua and Barbuda.

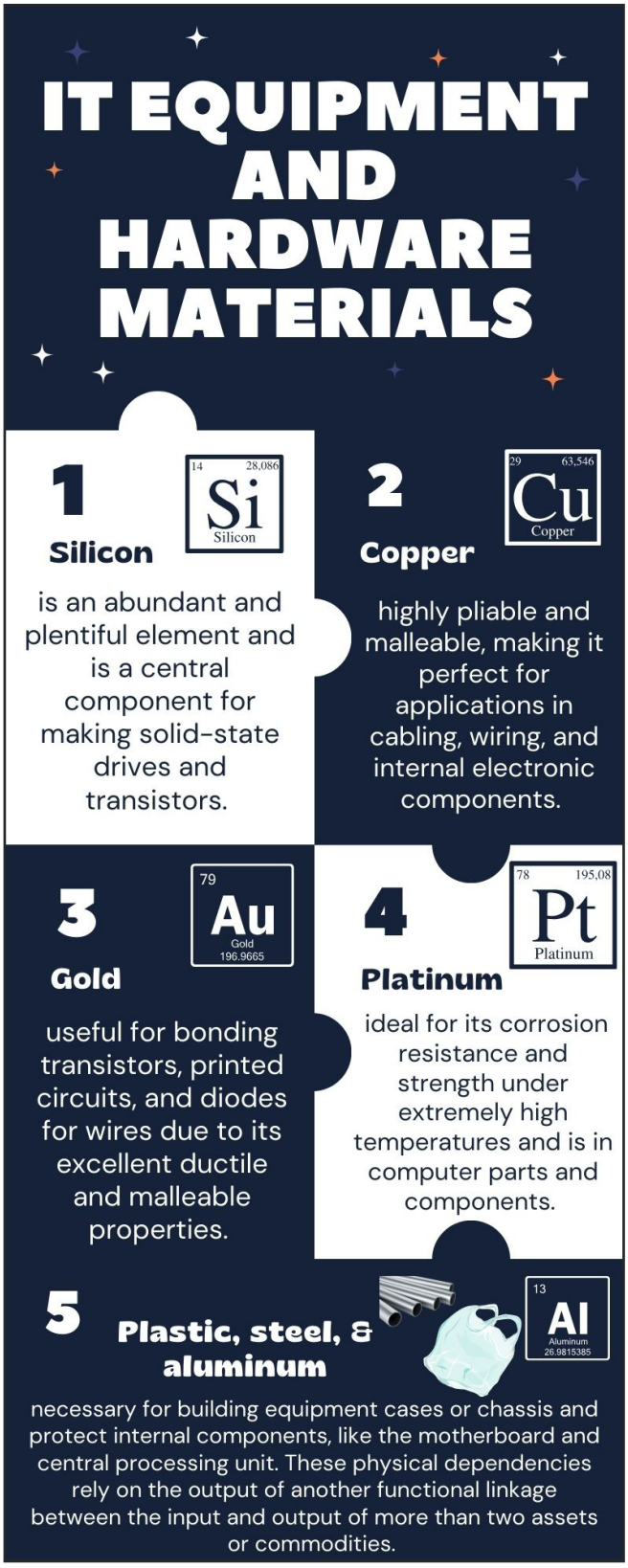
The 1859 Carrington event demonstrated the vulnerabilities of the less advanced world of telegraph communications. The same event today would have a more significant impact due to society's overdependency on IT. Geomagnetic storms and solar flares can wreak havoc on the electrical grid and disrupt

or permanently damage telecommunication equipment, crippling telecommunications and technology systems worldwide. The sun releases plasma energy known as a solar flare, which can dramatically change the Earth's magnetic field and result in a disaster that could disable power plants, transmission lines, power substations, and mobile phone towers for large territories and cities. The Deep Space Climate Observatory (DSCOVR) and the National Science Foundation regularly study solar storms and flares. In April 2001, one of the most significant solar flares in history, which did not directly aim toward the Earth, managed to disrupt Canada's power grid.

Poorly designed network and security misconfigurations can lead to catastrophic human-caused disasters. A security misconfiguration can occur when implementing errors into security settings or not properly applying computer security settings. The lack of security controls or misconfigured security settings creates a security gap for that network, leading to exposure to a cyberattack or a possible data breach. Many security misconfigurations occur when system administrators fail to change or validate a system's default settings, like a default administrative login or default administrative password. Tools such as vulnerability scanners or online resources such as Shodan can detect these default settings. This example of a security misconfiguration is problematic because many cyberattacks begin with reconnaissance – malicious bad actors and hackers looking for a system's default credentials and passwords. Changing the default settings can significantly reduce the risk of a breach or cyberattack.

What Else Do Emergency Preparedness, Response, and Recovery Professionals Need to Know About This Sector?

Power consumption and the type of power are important aspects for all data centers. Most modern data centers use alternate current (AC) power distribution systems. In the past few years, there has been a growing interest in the IT Sector to explore and utilize direct current (DC) power distribution systems as an alternative option. For example, leading telecommunication companies like Verizon and Comcast use DC power for their data centers, which is key when ordering and delivering backup power supplies. Major computer companies also sell servers that can operate on both DC and AC power as a stop-gap measure to help with resiliency. It is imperative to consider both options when designing, servicing, or responding to a data-center emergency.



Each company and government entity is unique and builds on different standards. Building off general plans, communities combine short- and long-term planning efforts for future growth. For example, smaller communities like Loomis, California, are looking at short- and long-term growth efforts. Due to its smaller footprint, considerations like equipment costs and dependencies on outside IT, energy, and

communication providers are crucial to planning efforts. These dependencies build and integrate infrastructure for businesses and homes. In contrast, large cities like New York may have their own power and gas companies (e.g., New York State Electric & Gas). Efforts designed and built in-house can have fewer dependencies on external companies to help streamline communications and emergency preparedness. When emergency managers and planners are part of the city's overall process, they tend to be familiar with the language in emergency operation manuals, laws, and policies.

Emergency responders should consider the type of fire suppression system to use. Water and electronics do not mix, so most data centers use a fire suppressant material to extinguish electrical fires. In the past, halon was the leading choice for data-center non-water fire suppression agents but has been removed as a fire suppression choice as halon depleted the ozone. Although modern data centers have phased out halon in favor of FM-200 or NOVEC 1230 fire suppression systems, responders should be aware that older data centers may still use halon.

Solutions for emergency managers and other preparedness professionals in IT emergencies must be rapid and may be challenging to sort through. All the complexities the IT Sector presents on blue-sky days are doubled on grey-sky days and can be even more complex and confusing. A cyber response plan is vital for local and state governments to have in place. The Cyber Security and Infrastructure Security Agency (CISA) has an Incident Response Plan that helps highlight challenges before a cybersecurity incident, including NIST SP 800-61 standards that help to guide the private sector with computer security incident response.

Applying organizational structure to IT systems and understating incident and vulnerability response also should be part of planning efforts. The document "Federal Government Cybersecurity Incident & Vulnerability Response Playbooks" contains standards that help facilitate better coordination and effective response among affected organizations, enable tracking of cross-organizational successful actions, and allow for cataloging of incidents to better manage future events with guides to analyses and discovery.

The IT Sector is complex and fast-growing, with services and functions that a combination of public and private entities operates and maintains. Although IT resilience differs among businesses and federal, state, and local governments, this sector's dependency on other critical infrastructure sectors creates unique challenges and opportunities. As society becomes more global and the physical and cyber worlds become more integrated, emergency managers, law enforcement departments, and fire agencies will have to better prepare and catch up to threats, policies, and resources to maintain effectiveness in preparedness and response.

Paul Galyen, CISM, is an experienced information security professional skilled in vulnerability management, security architecture, and endpoint security hardening, currently working with the California Cybersecurity Integration Center. Before state service, he worked as a contractor providing cybersecurity and digital forensic analysis for a large IT company and a major aerospace company. In addition, he served eight years as a communications specialist with the United States Army Reserve with the 801st Engineering Company (Horizontal Construction) and the 305th Engineering Company (Route Clearance), including a military deployment to Afghanistan in 2014 in support of Operation Enduring Freedom. He received a Master's of Information Technology Management with a specialization in cybersecurity from Colorado State University Global Campus.

Nathan DiPillo currently serves as a California Governor's Office appointee assigned to the California Office of Emergency Services as a Critical Infrastructure Analyst in the State Threat Assessment Center. Before state service, he functioned as a critical infrastructure specialist with the Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA). He also spent over 15 years with the Transportation Security Administration, where he assisted in standing up the agency with policy development, training, and recruitment. He has over 25 years in the emergency management and security industry, beginning as a resident firefighter/emergency medical technician. He also served with the California State Military Department, and Army National Guard in the 223rd Training Command ending his career as a Sergeant First Class. During that time, he served in many units, finishing his career attached to the 102nd Military Police Training Division in an Opposition Force Unit. He currently serves on a small-town planning commission and assisted in coordinating an emergency family communications group in his local area. He possesses a Master of Emergency Management/Homeland Security from the National University and other Federal Emergency Management Agency (FEMA), U.S. Department of Homeland Security (DHS), and military certifications. He currently serves as an advisor to the *Domestic Preparedness Journal*.

Source: Unsplash/jazzIRT

Healthcare and Public Health Sector Perspectives

By Tanya Scherr & Dan Scherr

On December 10, 2021, a series of tornadoes hit Western Kentucky, including at least one EF-4 that traveled approximately 160 miles through the state. These tornadoes killed over 80 people, damaged more than 15,000 buildings, and caused additional damage and loss of power in the area. Hospitals in the area saw a surge of an additional 500 patients because of the storms, with most facilities already close to capacity from COVID-19 Omicron cases. Additionally, some facilities were on backup power and lacked online systems to document patient care. Emergency crews struggled with downed power lines, communication disruptions, grounding of air crews, and loss of facilities in the area. The hospitals also faced challenges around a lack of water to help patients covered in mud and debris. The success of this region is a direct result of preparation that began years ago when local healthcare providers facing COVID-19 realized the need to work together and plan for disasters and resilience.

The U.S. Healthcare and Public Health (HPH) Sector is "large, diverse, and open, spanning both the public and private sectors." The HPH Sector protects "all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters." The HPH Sector-Specific Plan states:

> *It includes publicly accessible healthcare facilities, research centers, suppliers, manufacturers, and other physical assets and vast, complex public-private information technology systems required for care delivery and to support the rapid, secure transmission and storage of large amounts of HPH data.*

According to the U.S. Centers for Medicare and Medicaid Services, National Health Expenditures (NHE) accounted for $4.3 trillion, or 18.3% of the U.S. gross domestic product. The HPH Sector employed 14.7 million in 2022, accounting for 9.3% of employment in the United States.

The HPH Sector encompasses facilities and services from the private sector across the federal, state, local, tribal, and territorial levels, including direct patient care facilities such as general or surgical hospitals, psychiatric hospitals, ambulatory healthcare facilities, extended care facilities, and individual practitioner offices and clinics. Also, under the HPH Sector are public health agencies, healthcare educational

facilities, health-supporting facilities, laboratories, pharmaceutical production operations, mortuaries, and regulatory and oversight organizations.

What Makes This Sector Critical to the Nation, and What Importance Does It Have to State and Local Communities?

This sector not only provides resources and support critical to health security across the local, state, and federal levels, it is also central to the daily health and well-being of all citizens. Access to adequate healthcare is a critical component of national security and is interdependent with other sectors in supporting the five core mission areas of prevention, protection, mitigation, response, and recovery.

In 2021, there were 139.8 million visits to emergency departments , with 40 million of those injury-related and 13.1% of visits requiring hospitalization. An additional 131 million Americans, or two-thirds of the adult population, use prescription drugs to manage their health . U.S. nursing homes operate at over 70% capacity, and more than 60% of beds in 5,157 community healthcare facilities are occupied.

With this demand, connections, and dependencies so important to daily life, it is essential for emergency managers, sector leaders, and officials at all levels to identify potential weaknesses and improve resilience. The COVID-19 pandemic exposed weaknesses in the HPH Sector worldwide, some of which are now additionally exploited by cyberattacks for financial gain. The complexity of the sector defies a simple policy change or regulation to ameliorate risks and challenges, which demands engagement and a dedicated effort to ensure the effectiveness of this sector.

What Are This Sector's Key Assets and Interconnected/Interdependent Systems (Physical or Cyber)?

The HPH Sector is interconnected with and dependent on at least seven other critical infrastructure sectors. Issues or incidents in emergency services, energy, information technology, transportation, or water services can significantly and widely impact the industry. However, the most critical asset is its workers. From running the facilities to caring for patients, shortages in staffing directly affect all aspects of the sector. Patient outcomes are at risk when staffing shortages exist in any area, not just in patient care. For example, business office staff shortages can decrease revenue flows for a hospital if they do not have timely follow-up on claims.

Due to the resource-intensive nature of healthcare, the HPH Sector is heavily dependent on transportation and distribution networks, as laid bare during the COVID-19 pandemic. Maintaining adequate supply chains and transportation networks is vital for the HPH Sector's overall performance. There are critical assets across the country, with most facilities owned and operated by private industry. Some facilities may be small but represent the main healthcare service for the population, a trend in more rural areas exacerbated during the pandemic.

Healthcare is increasingly moving toward electronic health records, billing, and telehealth services, increasing the sector's reliance and dependence on Information Technology and Communications and vulnerability and risk for cyberattacks. As these attacks increase, it is important to continue assessing controls in place to protect physical and digital content.

What Are This Sector's Dependencies (Physical, Cyber, Geographic, and Logical) and Interdependencies With Other Critical Infrastructures?

The HPH Sector includes a complex array of physical and cyber assets and is highly dependent on the following sectors for service delivery and continuity of operations:

- *Communications* – This sector supplies situational awareness and helps coordinate healthcare activities during routine and emergency operations. During emergency operations, this sector is critical in providing information to the public and facilitating resource sharing and response across the industry. The communications sector also is crucial in expanding the use and reach of telehealth options. These options can improve outcomes for at-risk populations like the elderly and those lacking specialist services in their areas.
- *Emergency Services* – This sector, consisting of service facilities, systems, and personnel, is the first line of action in emergency response. The HPH Sector relies heavily on the Emergency Services

Sector to prevent and mitigate consequences following a disaster. Some services provided include patient transportation, decontamination, safety and security, and triage.

- *Energy* – The HPH Sector, like many others, relies on the energy sector to sustain operations. Facilities have varying abilities to maintain operations during an extended power failure, and extended power outages also impact supporting sectors that, in turn, degrade the HPH Sector's ability to function effectively. Power supply issues also can hamper sterilization, life-sustaining equipment, intensive care and operating units, and refrigeration for vaccines and medications.
- *Information Technology* – With the HPH Sector's ever-increasing reliance on information technology, any degradation in support and service can impact the quality of care. Computers are integral for every sector aspect, from patient care to pharmaceutical manufacturing and distribution to financial management.
- *Transportation Systems* – The HPH Sector relies on transportation and distribution to supply everything from personal protective equipment to medication, without which the sector cannot deliver services. Patients cannot receive care or reach healthcare facilities without effective transportation systems, whether they are private or public. Transportation barriers for healthcare include reaching and serving at-risk populations, contraction of public transportation, long transit times, particularly in rural areas, and reduced funding for transportation projects.
- *Water and Wastewater Systems* – The HPH Sector relies on potable water for infection control, sanitation, dialysis, laboratory needs, climate control, sterilization, drinking water, and other uses.

With over 6,000 hospitals, 400 health systems, 26,000 nursing homes, and countless other facilities in every state and territory across the country, the HPH Sector relies heavily on and is interdependent with other sectors. The nature of operations across the country varies, but no healthcare facility can operate in a vacuum.

What Are This Sector's Current and Emerging Vulnerabilities, Hazards, Risks, and Threats?

With the complex physical assets, electronic networks, and interconnections with multiple other sectors, the HPH Sector faces threats. Motivations for action against the HPH Sector include financial gain, commercial benefits, intellectual property theft, service disruption, and others. Primary vulnerabilities, hazards, risks, and threats include:

- *Pandemics and health crises* – Even before the COVID-19 pandemic, the threat of emerging or reemerging diseases was a threat to the HPH Sector. With so many issues arising from the pandemic not fully mitigated, additional crises will strain the sector and workers.
- *Natural disasters, extreme weather, and climate change* – With the sector represented in every level of government and across the country, HPH is impacted by every disaster and weather event. These events affect facilities and systems, take a toll on staff, and place staff at risk. Working to meet the community's surge needs while dealing with associated service disruptions is an inherent challenge.
- *Malicious human acts* – An active shooter event or other attack against a facility or a Chemical, Biological, Radiological, Nuclear, or Explosive (CBRNE) attack in the community can cause mass casualties, panic, and disruption of services.
- *Supply chain disruption and corruption* – The just-in-time model of distribution designed and in place before the COVID-19 pandemic could not keep the sector supplied under the weight of workforce shortages, disruptions, and increased demands. Transportation and supply chain shortages significantly impacted healthcare during the COVID-19 pandemic, with product shortages continuing for materials ranging from personal protective equipment to medications.
- *Cyberattacks* – The HPH Sector increasingly depends on health IT and secure storage and transmission to dictate care, maintain records, issue prescriptions, control financial operations, and more. Bad actors may seek to steal patient data, corrupt information, extort facilities or systems, or otherwise impact security. Advanced threats also pose a risk to pharmaceutical companies and the industry, stealing intellectual property for competitive advantage.

- *Space weather and electromagnetic pulse risks* – Severe weather and electromagnetic pulses (EMP) from natural or manufactured sources can impact the power grid. Natural EMP events arise from magnetic storms from the sun, and their impacts can result in either short- or long-term outages and overwhelm supplementary power sources.
- *Internal HPH Sector dependencies and interdependencies* – Due to the HPH Sector's size and complexity, a single point of failure can result in cascading impacts (e.g., the 2009 H1N1 and COVID-19 pandemics affected healthcare and public health workforce capacity).
- *Cross-sector dependency and interdependency risks* – The close connections, dependencies, and interdependencies with other sectors mean a failure or disruption in one sector can significantly impact others, including local disasters. These vulnerabilities are beyond the scope of any one sector to manage, requiring advanced planning to build resilience and contingency plans.

With increased reliance on electronic medical records, electronic prescriptions, and other technology across facilities and organizations, any disruption in internet service or power supplies can have impacts beyond turning off lights and machines. A ransomware attack in August 2023 against Prospect Medical Holdings impacted operations across their system, including 17 hospitals and over 150 clinics. Data from more than half a million patients was then listed for sale on the dark web with a price tag of over $1 million. This is in addition to the ransom demanded to unlock their systems, and it underscores that paying a ransom to an attacker does not guarantee the data breach stops there. This follows a trend dating back for several years, with federal agencies, vendors, and healthcare technology experts noting the increase in attacks and recommending mitigation and improved defenses.

Making up 18.3% of GDP, 9.3% of employment, and saving countless lives, the United States healthcare and public health sector is more than just critical, it is foundational to daily life.

How Would a Human-Caused, Natural, or Technological Disaster Impact This Sector's Preparedness, Response, and Recovery Efforts?

Disasters of any origin can stress the HPH Sector. The Administration for Strategic Preparedness and Response (ASPR) produces a National Health Security Strategy every four years to combat these threats. The 2023-2026 National Health Security Strategy builds on its goals and objectives, guides federal actions for desired outcomes, and recommends implementation activities for state, local, tribal, and territorial partners and the entire HPH Sector. Each disaster listed can have localized or wide-ranging impacts on the HPH Sector.

The risk from intentional CBRNE events increased over the last few years, with advancements in biotechnology, including gene-editing hardware and other technologies, low-yield weapons development, information proliferation, and drone technology. Each attack has the potential to harm large numbers of citizens with the initial attack and cripple the HPH Sector, at least locally, by overwhelming capacity, inciting panic, and disrupting multiple infrastructure sectors in the aftermath. These impacts can broaden if the targets are those the HPH Sector heavily depends on, such as energy, transportation, water, or information technology.

Natural disasters can also have a varied impact on preparedness, response, and recovery efforts, depending on the nature and location of the event. Widespread disasters like hurricanes, ice storms, heat waves, or wildfires can place immense pressure on the HPH Sector across large swaths of territory. Natural disasters have increased in frequency and severity in recent years, driven by climate change, requiring the sector to respond in more significant ways more often. Following the COVID-19 pandemic with continuing supply chain and staffing shortages, these events challenge response and recovery operations, strain surge capacity, and lead to resource competition. According to the World Bank, the COVID-19 pandemic exposed significant weakness in primary healthcare (direct care provided to patients). The exposure of

flaws in the current healthcare structure and systems and insight into the implications of failures in the sector provide a framework for potential improvements moving forward.

The threat of cyberattacks on the HPH Sector from actors both at home and abroad also increased in recent years, with further increases projected. These attacks threaten national health safety, disrupt patient care, and worsen patient outcomes. They can also disrupt response activities and exploit vulnerabilities in critical infrastructure systems, leading to additional disruptions in the HPH Sector as other sectors deal with breaches or other events. Threat actors may target pharmaceutical, biologic, or medical supply chains or target facilities and systems, as patient information is lucrative on the black market. In 2022, this sector experienced 344 cyberattacks, exposing the records for over 26 million individuals, which represents a 12.4% increase in attacks and a 270% increase in victims from 2020 to 2022. These statistics, coupled with the increase in the cost of an average data breach for the sector to $10.93 million, underscores the need for continual improvement. The cost per breach in this sector is up over 50% in the past three years, increasing the risk on hospitals, systems, and other organizations that fall victim to these attacks. These cyberattacks, per the American Hospital Association (AHA), can impact not only privacy but also patient safety.

What Else Do Emergency Preparedness, Response, and Recovery Professionals Need to Know About This Sector?

The success of this sector largely relies on collaboration and communication with other sectors, so they understand the sector, population served, and available resources in times of mass casualty and response. With an all-hazards approach, each event is unique and will require flexibility and adaptability based on the circumstances. Additionally, climate change has increased weather events with more extreme impacts, which is critical from a response and resource perspective.

The structure of the HPH Sector, with care facilities across the country, a network of support services, and the rapid incorporation of technology since the COVID-19 pandemic create opportunities for terrorists or other bad actors. The levels of oversight, governance, and resources present in these agencies and entities across the sector result in varied resilience and response to threats. Additionally, the norms of care across the country depend on the population, training, and support for the sector in each location. When disasters or attacks occur, the need and demand for HPH services can increase significantly and may be complicated by disruptions or increased demands in supporting infrastructure sectors. This may lead to limitations in the ability of this sector to respond to the surge needs and add to the complexity of risk assessment and response. These factors increase the need for community engagement and planning to improve the resilience and security of healthcare moving forward.

Tanya Scherr holds a Ph.D. in Public Policy and Administration with a healthcare and emergency preparedness focus. She is an associate professor in Healthcare Administration for the University of Arizona and has over 28 years of healthcare experience. Along with being a Certified Fraud Examiner since 2011, she is also a former firefighter-emergency medical technician (EMT), previously licensed in several states, as well as holding national certification. She has held several executive and board of director positions for community nonprofits that focus on women's equality, domestic violence, and sexual assault.

Dan Scherr holds a Ph.D. in Public Policy Administration with a terrorism, mediation, and peace focus. He is an assistant professor in Criminal Justice and Homeland Security at the University of Tennessee Southern and program coordinator for the Cybersecurity Program. He is also a co-director of the Honors College. He is a Certified Fraud Examiner and Army veteran with over two decades of experience in homeland security and operations.

Source: ©iStock/Orbon Alija

Emerging Technologies, Part 1 – Information and Communication

By Ian Pleet

Over the years, emerging technologies have played a crucial role in enhancing the effectiveness and efficiency of emergency management efforts. This five-part series looks at some of the more prominent emerging technologies in all-hazards emergency management and presents a classification scheme for these technologies.

Emerging technologies are innovative and cutting-edge advancements in various fields, such as information technology, telecommunications, sensor networks, data analytics, robotics, and artificial intelligence. These technologies show the potential to significantly improve the capabilities and performance of emergency management processes, including preparedness, response, recovery, and mitigation. Emerging technologies offer novel approaches, tools, and solutions to complex challenges posed by disasters and emergencies, enabling more effective decision-making, resource allocation, and stakeholder coordination.

Classification of Emerging Technologies

Emerging technologies are classified based on their application and potential impact on various phases of emergency management. Broad classifications include information and communication technologies, uncrewed vehicles, artificial intelligence and machine learning, and robotics and automation.

In an era of rapid technological advancement, the convergence of *information and communication technologies* (*ICT*) with emergency management, disaster response, and humanitarian relief efforts is revolutionizing how societies approach and mitigate crises. The dynamic interplay between technology and critical sectors has birthed a new paradigm in crisis management that enables real-time data acquisition, efficient communication, and targeted resource allocation, even in the face of the most formidable challenges. From natural disasters to complex emergencies, ICTs have emerged as invaluable tools, empowering responders, aiding survivors, and enhancing the overall effectiveness of disaster and humanitarian initiatives.

In modern technology, a remarkable revolution has occurred in *uncrewed vehicles* – a technological innovation has reshaped industries, expanded possibilities, and transformed how uncrewed vehicles interact with the world. Uncrewed vehicles, often called

autonomous systems or drones, have transcended the traditional boundaries of human-operated vehicles, introducing a new era of automation and autonomy. These vehicles, equipped with cutting-edge sensors, communication systems, and advanced computing, have unlocked many applications across land, sea, and air domains. The intricate world of uncrewed vehicles unveils a tapestry of innovation with significance, capabilities, and myriad ways in which they can shape the future of emergency management.

In the rapidly evolving technology landscape, *artificial intelligence* (AI) and *machine learning* have emerged as groundbreaking paradigms, reshaping how people perceive and interact with the world. AI, in its essence, aims to infuse machines with human-like cognitive abilities, enabling them to perform tasks that typically require human intelligence. Machine learning, a subset of AI, is the driving force behind the recent explosion in AI capabilities. It empowers computers to learn from data without being explicitly programmed.

In emergency management, disaster response, and humanitarian relief, the integration of *robotic systems and automation* has emerged as a transformative force, revolutionizing how societies prepare for and respond to crises. Rapid advancements in technology have ushered in an era where robotics and automation are no longer confined to science fiction but rather play pivotal roles in addressing pressing challenges during times of catastrophe. From natural disasters like earthquakes, hurricanes, and wildfires to complex humanitarian crises, the synergy between human ingenuity and robotic precision has led to innovative solutions that enhance emergency operations' efficiency, effectiveness, and safety.

Emerging technologies are part of a comprehensive approach to preparing for, responding to, recovering from, and mitigating the impacts of disasters.

Enhancing Capabilities

Emerging technologies continue revolutionizing all-hazards emergency management by providing innovative solutions and improving the overall response to disasters and emergencies. As technology advances, emergency management professionals and policymakers need to remain vigilant and adopt innovative tools to enhance their capabilities and protect their communities from the impacts of disasters.

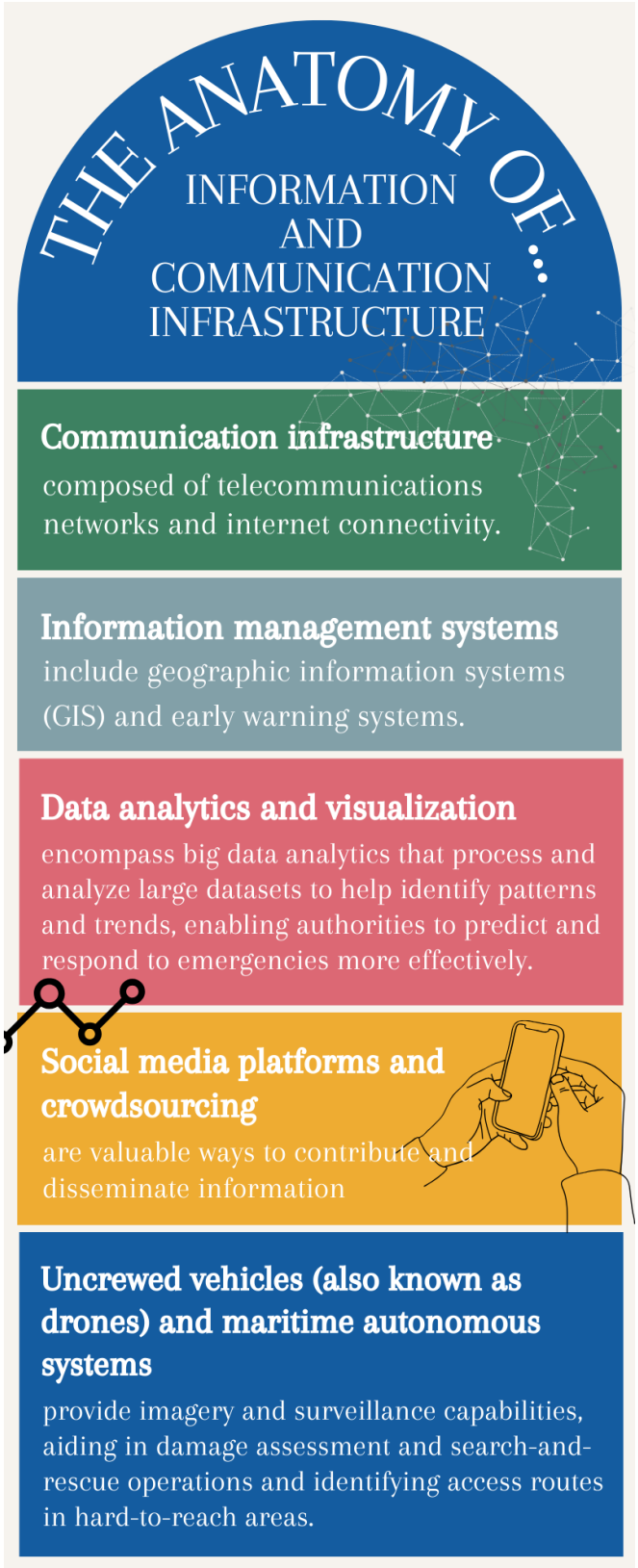
For example, ICT encompasses technologies and tools that facilitate efficient and effective information exchange, processing, and dissemination. By supplying real-time data, communication channels, and decision support systems, ICT enables responders to make informed decisions, coordinate efforts, and deliver aid more effectively during disasters and emergencies.

ICTs are diverse technologies that integrate communication and information processing capabilities. It encompasses hardware, software, networks, and services that facilitate data collection, storage, processing, transmission, and presentation.

Anatomy of the Information and Communication Infrastructure

The *communication infrastructure* is composed of telecommunications networks and internet connectivity. Telecommunication networks are the traditional telephonic networks and modern cellular and satellite communications that ensure redundant and resilient communication channels for responders and affected communities. High-speed internet connectivity provides access and enables real-time data exchange, social media engagement, and stakeholder collaboration.

Information management systems include geographic information systems (GIS) and early warning systems. GIS platforms help visualize and analyze geographic data, enabling responders to understand the spatial aspects of the disaster and make informed decisions about resource allocation and evacuation routes. Emergency Operations Centers use integrated software platforms to support emergency management personnel in coordinating response efforts, requesting and tracking resources, and obtaining, maintaining, and sharing a common operating picture. Early warning systems facilitate the dissemination of early warning messages via short message service (SMS), mobile



applications, and other communication channels, warning and notifying communities about imminent threats and providing instructions on what to do and where to go.

Data analytics and visualization encompass big data analytics that process and analyze large datasets to help identify patterns and trends, enabling authorities to predict and respond to emergencies more effectively. Data visualization tools provide a graphical representation of data, facilitating an understanding of complex information and supporting the decision-making processes.

Social media platforms and crowdsourcing are valuable ways to contribute and disseminate information. During emergencies, social media platforms like X (formerly Twitter), Facebook, and WhatsApp are helpful channels for sharing information, conducting public awareness campaigns, and engaging affected communities. Crowdsourcing allows citizens to contribute real-time information about the disaster's impact, allowing responders to gain situational awareness and identify critical needs.

Uncrewed vehicles (also known as drones) and maritime autonomous systems provide imagery and surveillance capabilities, aiding in damage assessment and search-and-rescue operations and identifying access routes in hard-to-reach areas.

Examples of ICT Applications

These are examples of ICT applications used to respond to and manage emergencies:

- In response to the devastating 2010 earthquake in Haiti, Ushahidi, an open-source crisis mapping platform, was deployed to aggregate and visualize crisis information from various sources. The platform collected data from SMS, social media, and other channels, helping responders identify areas needing immediate aid and providing valuable situational awareness.
- After the Fukushima Daiichi Nuclear Disaster in 2011, Japan used ICT to *monitor radiation* levels and share data with the public. The Japanese government utilized the System for Prediction of Environmental Emergency Dose Information (SPEEDI) system. Japan also used a sophisticated earthquake *early warning system* called "J-Alert," which uses various ICT technologies, including seismic sensors and satellite communication.

This system provides real-time alerts to the public through television, radio, and mobile apps.

- After the Nepal earthquake in 2015, Sahana Eden, an open-source disaster management platform, was used extensively during the response. The platform facilitated the registration of affected people, tracking relief supplies, and coordinating response efforts among various organizations. It provided a centralized database for decision-makers to understand the evolving situation and prioritize resources. In addition, volunteers and organizations used OpenStreetMap (OSM) to create detailed *crisis maps* of affected areas. This crowdsourced data helped aid organizations plan their relief efforts effectively.
- During Hurricane Harvey in 2017, social media platforms like Twitter, Facebook, and Instagram played a significant role in providing real-time information about the disaster. Citizens use these platforms to share updates, request help, and report emergencies. Organizations like the National Weather Service and the Federal Emergency Management Agency also used social media to disseminate information. While not a specific ICT system or manufacturer, the use of these platforms demonstrated the power of crowdsourced data in disaster response.
- After Hurricane Maria struck Puerto Rico in 2017, *Drones* assessed infrastructure damage, delivered medical supplies, and inspected hard-to-reach areas. Companies like DJI provide drones for disaster relief efforts.
- During the COVID-19 pandemic response, which began in 2020, many countries developed *contact tracing applications* to help identify and isolate individuals who may have been exposed. Examples include the NHS COVID-19 app in the UK and the Aarogya Setu app in India. Singapore's TraceTogether and Ireland's COVID Tracker rely on Bluetooth technology. Government agencies and private companies have developed contract tracing apps.
- During wildfires in California, remote sensing and GIS technology from NASA's Fire Information for Resource Management System (FIRMS) are used to monitor the spread of wildfires, assess their impact, and plan evacuation routes. Agencies like CAL FIRE and the California Governor's Office of Emergency Services (CalOES) utilize GIS software and tools from companies like Esri to map fire perimeters, track evacuation routes, and allocate resources effectively.

In conclusion, ICTs are integral to all-hazards emergency management, humanitarian relief, and disaster response efforts. Responders can enhance their situational awareness, coordination, and decision-making processes during emergencies by leveraging communication networks, data analytics, social media, and other ICT tools. The examples cited above demonstrate how ICT has been instrumental in improving disaster response and recovery efforts, underscoring these technologies' critical role in saving lives and mitigating the impacts of disasters. Integrating ICT into emergency management strategies remains pivotal in building resilient and efficient disaster response systems as technology advances.

Parts 2-5 will examine other emerging technologies and consider how modern emergency managers can integrate them into their all-hazards emergency management plans, policies, and procedures.

Ian Pleet is an emergency management consultant who advises his clients on all-hazards emergency management and continuity planning, creating robust training and exercise programs to find gaps, seams, and friction points in their emergency management plans. He is pro-board certified as a Fire Officer IV, Fire Inspector II, and Hazardous Materials Incident Commander. He has been named a Professional Continuity Practitioner by the Federal Emergency Management Agency and is a Department of Defense (DOD) antiterrorism officer course graduate. He holds certificates from Georgetown University in Change Management Advanced Practitioner and Virginia Tech in Wargaming.

Source: Unsplash/miguel angel hernandez

Emerging Technologies, Part 2 – Uncrewed Vehicles

By Ian Pleet

Uncrewed vehicles have many forms: uncrewed aerial vehicles (UAVs), uncrewed ground vehicles (UGVs), and uncrewed maritime vehicles (UMVs). They are autonomous or remotely controlled machines designed to perform tasks without human operators' direct involvement. They have evolved rapidly in emergency management, humanitarian relief, and disaster response. These vehicles offer advantages such as enhanced data collection, accessibility to remote or hazardous areas, and increased operational efficiency, making them valuable assets in addressing all hazards and managing emergencies.

Benefits During Disaster Response

Search-and-rescue operations widely use UAVs for earthquake responses, floods, and other natural disasters. UAVs with cameras and thermal sensors can quickly survey disaster-stricken areas, locate survivors, and identify hazards or blocked pathways for rescue teams. UAVs create high-resolution maps of disaster-affected regions, providing real-time data on the damage extent and helping authorities plan and allocate resources more effectively. Drones can function as flying communication relays in areas with a disrupted conventional communication infrastructure, facilitating coordination among rescue teams and affected communities.

Uncrewed vehicles provide humanitarian relief in remote or inaccessible regions to transport medical supplies, vaccines, and essential medications to disaster-stricken areas, ensuring timely aid to those in need. UAVs can assess the structural integrity of critical infrastructure, such as bridges and buildings, following disasters, guiding engineers and responders in prioritizing repair and reconstruction efforts.

For disaster response, UGVs can navigate challenging terrains to deliver food and clean water to affected populations in disaster zones, especially where traditional transportation is unavailable. With specialized sensors and manipulators, these vehicles can manage hazardous materials in chemical spills or nuclear accidents, minimizing human exposure to danger. Uncrewed vehicles can collect data on environmental conditions, air quality, and pollutant levels, aiding in disaster impact assessment and response planning.

Examples of Uncrewed Vehicle Applications

These are four examples of successful implementation of uncrewed vehicles being used to respond to natural disasters:

- Following the devastating earthquake in Nepal in 2015, UAVs surveyed the affected areas, assessed the damage, and created detailed maps to assist rescue and recovery efforts.
- In response to Hurricane Harvey's aftermath in 2017, the Federal Aviation Administration authorized UAVs to support damage assessment, search-and-rescue operations, and infrastructure inspection.
- During the 2018 Kerala floods in India, UAVs aided in locating stranded individuals, assessing flood levels, and mapping areas to distribute relief materials effectively.
- Australia has extensively used UAVs equipped with infrared cameras to monitor the spread of wildfires, track hotspots, and assess fire damage.

In conclusion, uncrewed vehicles have become valuable tools in emergency management, humanitarian relief, and disaster response efforts. With their ability to collect real-time data, navigate challenging terrains, and perform tasks that might be dangerous for human responders, these vehicles significantly enhance the efficiency and effectiveness of hazardous emergency operations. As technology advances and regulations evolve, integrating uncrewed vehicles in disaster management will save lives and improve response capabilities.

Source: Unsplash/Nathan Dumlao

Ian Pleet is an emergency management consultant who advises his clients on all-hazards emergency management and continuity planning, creating robust training and exercise programs to find gaps, seams, and friction points in their emergency management plans. He is pro-board certified as a Fire Officer IV, Fire Inspector II, and Hazardous Materials Incident Commander. He has been named a Professional Continuity Practitioner by the Federal Emergency Management Agency and is a Department of Defense (DOD) antiterrorism officer course graduate. He holds certificates from Georgetown University in Change Management Advanced Practitioner and Virginia Tech in Wargaming.

Source: Unsplash/hirun

Emerging Technologies, Part 3 – AI and Machine Learning

By Ian Pleet

Artificial intelligence (AI) and machine learning (ML) are transformative technologies that have revolutionized various industries, including emergency management, humanitarian relief, and disaster response. AI refers to developing computer systems to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, and decision-making. On the other hand, ML is "a subset of AI that enables systems to learn and improve from experience without being explicitly programmed" automatically.

AI and ML can enhance preparedness, response efficiency, and decision-making in all-hazard emergency management, humanitarian relief, and disaster response by analyzing vast amounts of real-time data, predicting potential risks, automating tasks, and supporting coordination among response agencies. This comprehensive approach leads to more effective disaster management, reduced human error, and increased adaptability.

Examples of AI and ML Applications

Like the Rush song "Distant Early Warning," AI and ML play a crucial role in early warning systems predicting natural disasters, such as hurricanes, earthquakes, and floods. By analyzing historical data, weather patterns, and sensor data, these systems can provide timely alerts to communities and authorities, allowing them to take preventive measures and evacuate if necessary. For instance, the European Centre for Medium-Range Weather Forecasts (ECMWF) utilizes AI techniques to improve weather predictions and storm tracking.

After a disaster strikes, *assessing the extent of damage* is critical. AI-powered tools, like remote sensing and satellite imagery analysis, can quickly assess the affected areas, identify damaged infrastructure, and prioritize response efforts. The Humanitarian OpenStreetMap Team (HOT) uses AI to analyze satellite imagery to map and assess disaster-affected regions.

Efficiently *allocating resources,* which may be scarce, is vital during relief operations. AI algorithms can optimize supply chain management, route planning, and resource allocation based on real-time data and demand patterns. This optimization helps to ensure that resources reach affected areas promptly. The United Nations World Food Programme (WFP) employs AI to optimize the delivery routes of food aid.

AI-driven *sentiment analysis of social media* posts and news articles can provide insights into affected

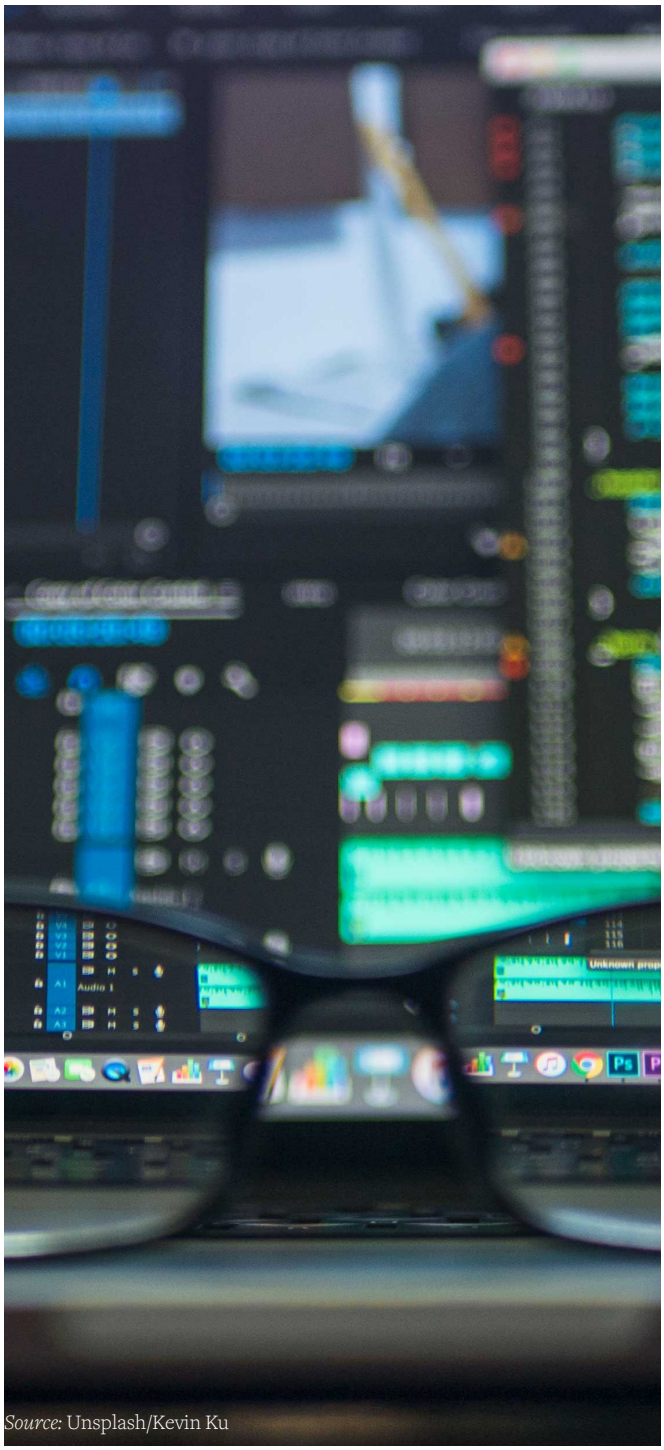
communities' emotional states and needs. This information aids in tailoring response efforts and identifying urgent requirements. To understand the affected population's needs, UNICEF uses AI to analyze social media data during crises.

AI-powered *chatbots* provide real-time information and assistance to affected individuals, relieving the burden on call centers and response personnel. These chatbots can answer queries, offer safety tips, and guide users to appropriate resources. The Red Cross uses AI chatbots to provide support and information during emergencies.

AI and ML can perform predictive analysis of healthcare data, travel patterns, and other relevant information in public health emergencies to predict disease outbreaks and spread. This information enables health agencies to implement timely containment measures. The HealthMap project, developed at Boston Children's Hospital, uses AI to monitor and forecast disease outbreaks.

Incorporating Technologies in Emergency Response Systems

AI and ML have emerged as powerful tools in all-hazards emergency management, humanitarian relief, and disaster response. Their ability to analyze vast amounts of data, predict potential risks, automate tasks, and support decision-making has revolutionized disaster management strategies worldwide. By incorporating these technologies into emergency response systems, authorities can mitigate risks, optimize resource allocation, and provide timely assistance to affected communities, saving lives and minimizing what can be catastrophic impacts from disasters.



Source: Unsplash/Kevin Ku

Ian Pleet is an emergency management consultant who advises his clients on all-hazards emergency management and continuity planning, creating robust training and exercise programs to find gaps, seams, and friction points in their emergency management plans. He is pro-board certified as a Fire Officer IV, Fire Inspector II, and Hazardous Materials Incident Commander. He has been named a Professional Continuity Practitioner by the Federal Emergency Management Agency and is a Department of Defense (DOD) antiterrorism officer course graduate. He holds certificates from Georgetown University in Change Management Advanced Practitioner and Virginia Tech in Wargaming.


EST 1998
Domestic Preparedness
Real-World Insights for Safer Communities
We Cover It All
Subscribe Today!