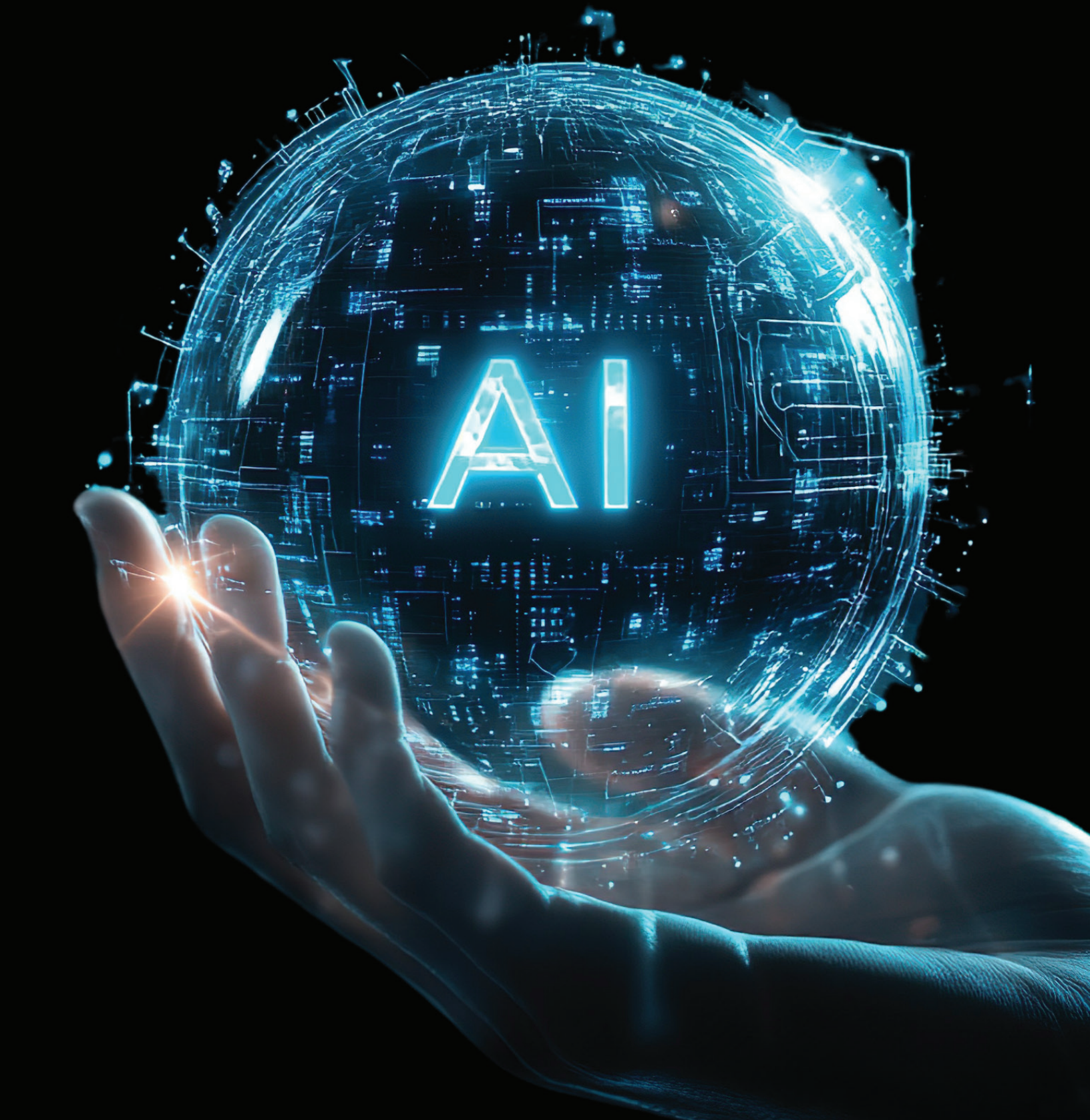
EST 1998

DOMESTIC PREPAREDNESS JOURNAL

VOLUME 20 ISSUE 12

DECEMBER 2024



Take Domestic Preparedness On The Go

December 2024, Volume 20, Issue 12

Cover Source: Generated with AI by lucegrafiar/Adobe Stock.

For more information about Domestic Preparedness, visit DomesticPreparedness.com

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

Editor's Note

Source: Unsplash/Clark Young

Preparing for the Future of Artificial Intelligence

By Catherine L. Feinman

Artificial intelligence (AI) capabilities and possibilities are continuously and rapidly evolving. Although surreal at the time, some of the imagined AI portrayed in The *Jetsons*, *Star Trek*, and many other television shows and movies have become reality. Based on technological advances in recent years, it is clear that the imaginations of today could become reality in the not-too-distant future, so any potential benefits or consequences of AI must be considered across all disciplines.

Emergency preparedness, in particular, involves imagining the likely as well as the what-if scenarios to determine how to combat future threats and hazards. The changing emergency management landscape raises questions about how research and development and technology can support daily tasks and emergency operations centers. Having an AI-ready workforce is critical for meeting today's threats and hazards. To help emergency preparedness and response professionals better prepare for this technological evolution, researchers, policymakers, and community stakeholders across the country are developing partnerships and plans to ensure a human-centric approach to AI development.

The authors in this December edition of the *Domestic Preparedness Journal* provide coverage of the transformative impact of AI on emergency operations and highlight the technological advancements, practical applications, and barriers to implementation and acceptance. With their exponentially increasing speed of development, existing, emerging, and not-yet-created technologies must all be part of the planning process in 2025 and beyond. Domestic Preparedness would like to thank the Pacific Northwestern National Laboratory and the U.S. Department of Homeland Security's Science and Technology Directorate for inspiring this end-of-year edition.

STAY CONNECTED

domesticpreparedness.com

@domesticpreparedness

journal@tdem.texas.gov

512-963-4902

SUBSCRIBE TODAY

Domestic Preparedness

Your Source for Real-World Emergency Insights

Table of Contents

Source: Ar_TH/Adobe Stock

Emergency Management of Tomorrow: Emerging Technologies and Concepts

By Dan Cotter, Christina Bapst-Stump, Ann Lesperance, and Rachel A. Bartholomew

The future of emergency management (EM) is changing fast – and so is the science and technology to protect it. More frequent and intense disasters put pressure on emergency managers and emergency operations centers (EOCs) to share and analyze data faster than ever before and with more reliability and defensibility. In an era of technology innovation, emerging and advanced capabilities like artificial intelligence (AI) can enable better and faster decision-making that saves lives.

However, with new technology comes new challenges. The path to new solutions – even the first step to explore what is on the market – can be overwhelming. Further, no single entity coordinates and disseminates new or breakthrough EM research. Addressing this gap requires a well-articulated vision, a coordinated research program, and strategic investments. A project launched in 2023 with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) is helping sift through the expansive landscape of emerging technology, and EM needs to prioritize research and development requirements and inform future investments for EM.

SETTING SIGHTS ON THE FUTURE

Over the past year, S&T has partnered with Pacific Northwest National Laboratory (PNNL) to execute the Emergency Management of Tomorrow Research (EMOTR) Program to:

- Assess the EM research landscape;
- Assess the AI research landscape;
- Elicit capability needs from EM stakeholders;
- Conduct validation exercises; and
- Identify where technology, such as AI, may benefit the EOC of the Future.

Together, these efforts are navigating the complexities of EM and AI to identify emerging trends, potential challenges, and strategic pathways to guide future investments based on current assessments and projected needs. The results – recommendations informed by practitioners and research and development (R&D) – will spotlight EM capability needs and potential technology to close the gaps.

NAVIGATING THE DEEP, BROAD SEAS OF EM R&D

Navigating the wealth of EM research can seem insurmountable, as thousands of research institutions worldwide are leading disparate and sometimes duplicative efforts. Identifying relevant, overlapping, and complementary research topics in EM can promote transparency and encourage collaboration in the EM research community. PNNL approached the future of EM like any scientific experiment – with a research question: "What R&D is currently funded that addresses EM capability needs?"

Beginning in late 2023, PNNL developed a landscape assessment of EM R&D at U.S. academic institutions, national laboratories, and other research institutes and curated a comprehensive framework of trends, gaps, and overlaps. Analysts used a suite of research databases, key search terms, and analytical tools to filter 36,000 journal articles and 1,600 patent publications to a manageable dataset of 300-plus peer-reviewed and open-source publications (years 2008-2023) captured in an annotated bibliography. The annotated bibliography is formatted in a sortable spreadsheet that allows EM personnel to review recent research in terms of capability needs identified through EMOTR outreach and literature reviews, including data integration and communication, pandemic response, resource management, and threat and hazard detection. (The bibliography is available by request at emotr@pnnl.gov.)

DEFINING AND REFINING EM R&D NEEDS

Every good literature review needs validation – concurrence from credible sources that its findings are an accurate reflection of the field. To that end, the EMOTR team connected with EM personnel and first responders nationwide both virtually and in-person through interviews, focus groups, surveys, and conferences to validate the landscape assessment and capture additional EM-focused capability gaps. These efforts are building an understanding of the current state of information sharing, evaluating the efficiency of current research programs in closing EM capability gaps, and encouraging community coordination to inform overall efficacy of EM research investments.

Through these structured engagements, EM practitioners of all backgrounds and jurisdictions shared perspectives on EM-related technologies and operations, how they are evolving, and how they might impact the homeland security enterprise. The analysis of these EM R&D needs and priorities highlighted areas of research underrepresented in the current research ecosystem that are fit for EM community coordination. In particular, the following were recurring concerns and interests:

- *Technology and technical capabilities* – EOCs must harness real-time data streams from various sources (e.g., sensors, social

media, satellite imagery) to enhance situational awareness and facilitate rapid decision-making.

- *Structure and organization* – EM must balance hybrid operations and overcome challenges in interoperability, flexibility, and scalability.
- *Policy and operations* – Information sharing, resource management, and situational awareness are a priority but face policy, funding, privacy, and trust barriers.
- *Research and development* – Human-centric R&D can explore balancing the psychological impacts of high-stress environments and decision-making with AI tools.

TAKING AI TO TASK IN EM

Determining AI's role in all of this is where it all comes together – the landscape assessment, outreach, and analyses have convened to address the question: "What EM functions can technology – including AI – realistically address?" Through a structured evaluation of the AI and EM landscape and by connecting with subject matter experts to identify areas of synergy and barriers to implementation, a team of analysts, systems engineers, and researchers sought to evaluate and prioritize technologies that will have the most positive benefit to the EM domain. An EM task analysis looked at how AI and other disruptive technologies can benefit the tasks in most need, such as providing greater situational awareness and improving planning, training, response, and risk mitigation. Ultimately, 13 technologies were identified to have a high probability of enhancing EM in the next decade.

To explore these technology and task trends in real-world scenarios, a series of roundtables and tabletop exercises across the nation, in New Hampshire, Wisconsin, and Washington State, took a deeper dive into the future. The exercises convened emergency managers and first responders with diverse backgrounds; federal, state, and local EOC stakeholders; and academic researchers to assess the impacts and benefits of emerging technologies on EM organizations via real-world scenarios, hazards, and injects. Together, this feedback and R&D coalesced into a series of recommendations and priorities for the EOC of the Future, with a focus on:

- AI, automation, and human-machine teaming;
- Data and information sharing;
- Situational awareness;
- Technology integration and interoperability;
- Virtual capacity scaling; and
- Workforce development

CONNECTING THE DOTS FROM AI TO EM

Today, PNNL researchers are actively sharing their findings at conferences nationwide and welcome continued input and engagement to hone their focus as they build an actionable R&D agenda to benefit EM and the EOC of the Future for years to come. The December edition of the Domestic Preparedness Journal includes a diverse cohort of thought leaders and practitioners – a mix of government, academia, and industry – to discuss how new science and technology can support the emergency manager's responsibilities and assess how future technology can be leveraged to empower the EM community of tomorrow.

Dan Cotter is the Executive Director for the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) Office of Science and Engineering. His prior positions with S&T include serving as the Director of Support to the Homeland Security Enterprise and First Responders Group. Before joining S&T, Cotter held positions as the DHS Chief Technology Officer and as the DHS Geospatial Management Officer. His public sector experience also includes twelve years with the Federal Emergency Management Agency. Cotter's private sector experience includes acting as the Geospatial Information Technologies Manager for a large engineering firm, as the President of an airborne light detection and ranging company, and as Vice President of a flood zone determination firm. He was elected as a Fellow of the American Association for the Advancement of Science in 2005. Cotter was recognized for his achievements and leadership skills in 2018 when he received the Presidential Rank Award (Distinguished), the Nation's highest award for career members of the Senior Executive Service.

Christina Bapst-Stump is a Senior Advisor for the Department of Homeland Security Science and Technology Directorate Office of Science and Engineering. She has also served various organizations and efforts within the Department, including the National Information Exchange Model, where she set the strategic vision for the program as well as oversaw operational functions, communications, and outreach. Her previous experience includes Robbins-Gioia, ExxonMobil Corporation, and General Electric, Corporate Research and Development. She has a Master of Business Administration from The George Washington University and a Bachelor of Science in Management from Rensselaer Polytechnic Institute.

Ann Lesperance is the Director of the Northwest Regional Technology Center at the Pacific Northwest National Laboratory (PNNL). She has over 30 years of experience as a researcher and project manager, and her primary focus is developing regional programs to accelerate the demonstration and deployment of new homeland security technologies. Lesperance works with state and local emergency responders and public safety officials and builds regional coalitions of emergency management professionals to understand and help prioritize their operational needs and requirements. Lesperance also has a joint appointment as the Director for the College of Social Science and Humanities Programs at Northeastern University Seattle. In this role, she leads efforts to build the Master's program in Security and Resilience Studies and Urban Informatics.

Rachel Bartholomew is a Science and Policy Advisor and team lead in the Chemical and Biological Signatures Group at Pacific Northwest National Laboratory (PNNL). She has over two decades of experience applying molecular biology to address national security, policy, and nonproliferation challenges. She has served as principal investigator and project manager for a variety of sponsors, including Departments of Homeland Security, Energy, State, and Defense, engaging with a range of domestic and international stakeholders, such as first responders, law enforcement, customs and border personnel, policymakers, and scientific subject matter experts. In 2023, Bartholomew was named Deputy Director for the Northwest Regional Technology Center, a virtual resource operated by PNNL to support local and regional preparedness, resiliency, response, and recovery. Concurrently, she is the Principal Investigator on projects exploring first-responder technology, emergency management, and emergency operations centers of the future. These efforts are leveraging her decades of experience building relationships and connecting with the first responder community to capture and translate their technical requirements into research and solutions. She received her BA in biology from Case Western Reserve University and PhD in animal physiology from Cornell University, where she was a National Science Foundation pre-doctoral Fellow. Her post-doctoral training was completed at the FBI Laboratory's Counterterrorism and Forensic Science Research Unit.

Source: Kevin/Adobe Stock

The Role of AI in Meeting a Great Emergency Management Challenge

By Douglas Yeung and Aaron Clark-Ginsberg

Rumors and misinformation that spread online during emergencies, like hurricanes Helene and Milton, raise concern that content created by artificial intelligence (AI) might make the job of emergency managers even more difficult. After Hurricane Helene, law enforcement and government agencies were forced to devote precious time to combating conspiracy theories, including allegations that land had been bulldozed to cover up dead bodies. Countering this AI-powered misinformation understandably took a toll on responder morale. But at the same time, AI's ability to ingest and synthesize data on hazards, vulnerabilities, and capacities could also prove invaluable in addressing one of the biggest long-standing challenges of emergency management: truly engaging the whole community.

What "Whole Community" Is and Why It Matters

For the Federal Emergency Management Agency (FEMA) and other emergency management agencies, the whole community is both philosophy and approach: one where all community members – people, organizations, and businesses – work together to mitigate, prepare, respond, and recover, and together share the benefits of these emergency management efforts.

Helping the whole community is the mission of emergency management. Because no one is immune to disasters and their effects, emergency management must plan to support all community members. This support may be indirect, like structural mitigation to protect critical infrastructure. Or it may be direct, such as individual assistance programs available to survivors after a disaster.

Likewise, each member of the community has a support role to play. Decades of evidence show that everyone can address risk – from preparing households for disasters to the more general building of community and social infrastructure essential to resilience. These individual actions collectively create whole community resilience to disaster, which in turn bolsters the resilience of individuals and households within the community.

Current Challenges to Whole Community Engagement

Truly engaging the whole community can be daunting. It takes time, which is often in short supply during an emergency. For instance, in response and recovery situations, decisions about allocating limited resources must be made quickly based on limited information.

Engaging the community also requires understanding its specific needs, which can be difficult given the extreme complexity of vulnerability, hazard, and capacity. Widely used metrics of vulnerability, which incorporate socioeconomic factors, for example, offer only a general view and are not designed to capture community-specific needs and capacities that are products of place and scale. Hurricane Maria, which struck Puerto Rico in 2017, offers such an example. Spanish is the dominant language on the island, meaning that people who only spoke English were at a disadvantage in getting their needs met. Yet vulnerability metrics often include English as a second language as one such metric. The hurricane also displaced many Puerto Ricans to the mainland, where they were out of sight and out of mind, speaking English as a second language, and it was difficult to ascertain their needs to support them in the recovery process. Beyond this example, metrics might also fail to capture other elements related to vulnerability, such as certain access and functional needs characteristics.

True engagement means partnering with communities to manage disaster risk. This requires dialogue, not just one-way information sharing. As more is learned about community needs, goals, and capacities, these elements should be incorporated into emergency plans. Understanding a community is critical for local-level planning, but must be supported by regional and higher-level infrastructures. Unfortunately, efforts to use appropriate communication channels, languages, and (trusted) messengers for that dialogue can be limited due to cultural norms of emergency management, resources required for such engagement, and other factors.

Ways That AI Can Support Whole Community Engagement

Current emergency management structures are adaptable in some ways. However, they are also beholden to bureaucratic rules that make it difficult to meet whole community needs. AI technologies may be suited to tackle some of these challenges.

Take chatbots, for example. By talking to people in simple, clear language, chatbots might help with crisis-related communication before, during, and after emergencies. They might be particularly useful for marginalized populations who may be less able to navigate bureaucratic assistance programs. A chatbot on, say, a relief worker's phone could pose conversational questions that determine a person's needs and eligibility. Chatbots could be deployed to spread awareness about local hazards, as well as the steps people could take to prepare. People have already begun to turn to chatbots for mental health support, and that too might grow in use after a disaster.

Other forms of AI, like prediction algorithms, might be used to match people in need with businesses or nonprofits with resources or, perhaps, identify people who are in need

but unable to contact emergency managers. Prediction algorithms can parse massive amounts of data to discern trends that might otherwise not be apparent. In emergency management, algorithms already improve hazard prediction for wildfires, tornadoes, hurricanes, and other risks. Existing AI tools help homeowners and emergency planners identify vulnerabilities, build community resilience, and aid crisis response. These could be expanded to analyze the social dynamics of risk across an entire community and then made available to all involved.

Toward an AI Whole Community Approach

Although AI could be a powerful tool for whole community engagement, it is likely to require additional governance, training, and research and development. Government agencies and first responders may need to adapt AI regulations and procedures to the emergency management context, such as the National Institute of Standards and Technology Artificial Intelligence Risk Management Framework.

Emergency management workforces will also need training to use AI effectively and safely in different roles, and personnel may harbor concerns about their jobs being replaced by AI. Leaders should be aware of and prepared to address these concerns.

Given ongoing challenges with bias in AI, any AI tools will need to be made culturally sensitive and avoid unwarranted assumptions that may lead to inequitable distribution of benefits or mistrust in AI tools. Here, emergency managers can build on an existing track record of involving communities in disaster-related knowledge creation by partnering with them on AI research, development, and implementation efforts. To guard against AI-generated misinformation, emergency managers can ensure that their own social media posts clearly cite evidence, as well as uncertainty, and engage users with calls to action.

Emergency managers today recognize the importance of engaging the whole community in their work. AI has the potential to accelerate these efforts. Using AI as a whole community tool may require, for instance, that policymakers develop regulations or policies that encourage AI tools to protect the whole community from harm while maintaining benefits. Emergency management leaders could develop training for their workforces to effectively deploy prediction models in a way that accounts for potential uncertainties and does not create false certainty. Finally, those in the research community can continue to advance knowledge on the benefits and risks that emergency management AI technologies might bring to communities. All these activities must engage – and be conducted in partnership with – the whole community, ensuring that emergency management benefits all who need it.

Douglas Yeung is an associate director of the Management, Technology, and Capabilities Program within the RAND Homeland Security Research Division, a senior behavioral and social scientist at RAND, and a professor of policy analysis at Pardee RAND Graduate School.

Aaron Clark-Ginsberg is a behavioral and social scientist at RAND and a professor of policy analysis at the Pardee RAND Graduate School.

Source: Generated with AI by Nakarin/Adobe Stock

Opportunities for Artificial Intelligence in Emergency Management

By Alex Hagen and Jonathan (Jon) Barr

Trapped in the whiplash of increasing dystopian headlines describing the latest disaster and utopian headlines about the promise of artificial intelligence (AI), many have asked the natural question: "How can the second save us from the first?" Several entities, including the Naval Postgraduate School and Department of Homeland Security's Science and Technology Directorate, have commissioned studies to explore this exact question, which have uncovered a treasure trove of research, applications, and existing implementations of AI in emergency management (EM). An in-depth landscape assessment conducted in 2024 dug deep into research articles, preprints, code repositories, and surveys at the intersection of applied AI and EM.

In the wake of recent or local emergencies, many articles focus on exceedingly specific threats (e.g., floods), and they apply technologies with the same specificity. It is hard to understand whether that technology could apply to other threats – or even the same threat in a different locality or at a different time. Instead, understanding the landscape of AI in EM requires zooming out to understand each threat and technology in context. This landscape assessment sought to do the following:

- Categorize where the technology applies along the emergency timeline: from the mitigation stage – well before the event – to detection around the onset of the event, on to response to the event, and recovery after the event.
- Identify the applicable domain, for example, a physical system such as a public building, telecommunications infrastructure, the natural environment, or others.
- Evaluate the technology based on scientific data, assessing the data type (such as imagery or geospatial information) and other technical details about the data.

Implementing this framework on hundreds of sources illustrated trends, gaps, and a broader vision for AI in EM. Researchers are finding some of the biggest challenges

in emergency management and tackling them head-on, making great progress with many. Researchers, entrepreneurs, private and public industry, and others have roles to play, as well, but gaps, challenges, and unanswered questions remain. One of the biggest questions is that of *generalization*. In AI, a technology "generalizes well" if it performs its task as well in a future emergency as it did during the emergency in which it was trained. Unfortunately, many AI technologies are so focused they do not generalize beyond the data on which they were trained. Generalization is a gate through which researched technologies must pass before being implemented in a real system. There is also a potential risk if not properly assessed through rigorous testing and evaluation before and during implementation. Another important filter is that of pure feasibility, which is challenging to assess from a technological standpoint.

Emergency management experts must validate each proposed technology against the chaos of real emergencies. This was never more apparent than in the recent discourse between national laboratory data scientists, state and local emergency managers and first responders in New York, and the University of Albany faculty in computer science and emergency management. Applying AI to EM must be done at the confluence of the two fields – understanding the potential and pitfalls of AI technologies (best analyzed by data scientists) but also with an appreciation for the real world that only those who have managed emergencies have.

The landscape assessment garnered insights focused on four technologies foundational to future AI technologies in EM and nine broad technologies with great potential to benefit EM.

A GOOD BACKBONE

Like many other industries are discovering, using AI requires infrastructure that had little reason to exist before AI. This applies to hardware and physical networks but also to the software surrounding AI, and even to the processes and public perception of AI technologies.

Operational AI depends on highly sophisticated infrastructure to enable data delivery to high-powered servers and back to its users in a timely fashion. The increase in demand for graphic processing units (GPUs) – the hardware that runs much of the development of AI models – has been prolific and will be critical. In fact, since emergencies can happen quickly and with little warning, unused computer resources must be kept as "inventory" to be deployed during the event. Network infrastructure will likely be as important to enable AI broadly, but the challenge for network connectivity is amplified in EM, whereas it is normal to require better-than-average network resources in rural, remote, or even destroyed areas. Additionally, such sophisticated infrastructure requires ongoing maintenance and the power to support the infrastructure.

Trusting the output of AI is also crucial to future success in EM. That trust depends on the governance of and communication about AI – from setting reasonable policies of how public entities adopt AI technologies to allowing for human overrides at the time of the event. Feedback garnered from EM practitioners during stakeholder outreach for the landscape assessment heard fundamentally opposite arguments regarding these points: Some believe that "the most cutting-edge AI should be used because people's lives are at stake," yet others believe that "we can't use AI technologies until it is completely mature and trusted because people's lives are at

stake." The outcome of that argument – and it may not be homogeneous across all countries or states – will have an outsized effect on how AI contributes to EM. However, trusting AI goes beyond simply understanding the output of the specific technology and expands into trusting that the whole system – data, network, software, and all – has not been compromised by malicious actors. Cybersecurity will, therefore, grow in importance as AI is further incorporated into EM.

ENABLING TECHNOLOGIES

Assuming that a trusted AI infrastructure, as described above, will be in place to support AI applications in emergencies, the landscape assessment identified nine technologies predicted to have a large impact on EM in the next decade. Among the list was also the most possible with current technology: Using AI-enabled productivity applications can assist emergency managers in the repeated and sometimes mundane tasks of their daily jobs – from turning emergency plan outlines into full reports to converting their notes into a full after-action assessment. Chatbots and other tools are being released to the private sector to do this in a general context. With some modifications for the EM sector, it could ease emergency managers' considerable workload. Additionally, using AI as a means of public-facing communication could help emergency managers ensure that everybody gets the right information in the right way during emergencies. The ability of emerging AI-driven capabilities to produce better translations and modify them to avoid fearmongering is exciting. Finally, the "broadband" ability of AI to tend to large amounts of data creates opportunities for more effective and efficient planning. This would allow emergency managers to use AI as a planning assistant, with the benefit of fact-checking previous events to avoid historical missteps or checking others' plans to avoid allocating the same asset twice during the same emergency.

That same "broadband" ability is beneficial on the ground as well. AI-filtered domain awareness promises to provide only essential and consequential information to the emergency manager, as opposed to the overwhelming data environment they currently grapple with. That capability will also improve its ability to predict and detect emergencies before and during onset, predict a storm's course, and measure effects during and after an event. While many technologies already perform these tasks, there is room for improvement in detection and how well the ability to generalize to the future. Additionally, adding new data streams, such as chemical sensors or radiation detectors, will benefit prediction capabilities, but this technology is currently nascent.

In the future, the technologies underlying modern AI can be pushed further. Modern optimization methods, including reinforcement learning, can improve the routing of traffic, assets, and resources during an emergency, sometimes with automation. Using risk models in conjunction with these improvements can also help minimize overall consequences, even when the worst consequence is rare and hard to foresee.

THE NEXT GENERATION

The landscape assessment was cognizant of the current and evolving state of technology – some of the new and exciting concepts in the literature (and researchers' surprise at them) highlighted the calcification of old ways of thinking. To combat this, researchers solicited ideas from one of the best sources for off-the-wall ideas: a room full of 100 college students, bribed with free food. In this

"sandpit" exercise, performed at the University of Albany in conjunction with its College of Emergency Preparedness, Homeland Security and Cybersecurity, students were asked to perform in one day what many researchers do for their career: Identify an important EM challenge, create an AI-enabled solution to the problem, and validate and report on that solution.The students conceptualized everything from an AI-enabled clearinghouse for privately owned resources to chatbot systems that could reroute needed supplies during an emergency event. These ideas fortified belief in the above technologies – with a majority of ideas pertaining to efficient asset deployment through modern optimization.

LOOKING FORWARD

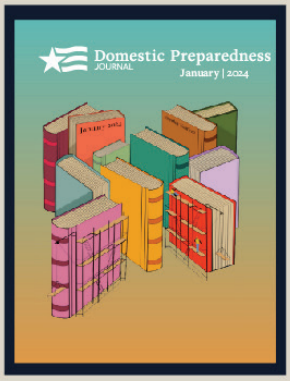
Performing this landscape assessment, which started pessimistically, was an exercise in optimism. So often when discussing a possible EM challenge, there is already an AI technology that could alleviate or even solve that problem. It should be encouraging, not frightening, to practitioners to see how much research is connecting challenges with AI solutions, and also how students – the next generation – are thinking about the field. While there are still infrastructure hurdles that AI will need to overcome in EM, AI technologies will be the subject of deserved utopian press as they begin to help practitioners prevent, mitigate, and recover from emergencies.

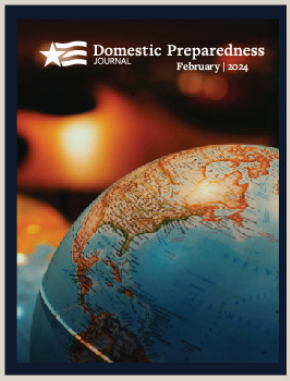
Alex Hagen is a data scientist who works broadly across detection and material interdiction spaces to improve analysis using modern machine-learning methods. After a half decade designing neutron detectors and active interrogation techniques and subsequently analyzing data from such experiments, he knows how to combine field implementation with advanced analytical techniques. His research has been published across many nuclear engineering and physics journals, including Journal of Physics, Nuclear Instruments and Methods, and the Transactions of Nuclear Science. His conference presentations have taken him across the world, including to the International Conference of Nuclear Engineering in Prague and the Advanced Computing and Analysis Techniques Conference in Saas-Fe, Switzerland. He has contributed to several high-energy physics collaborations, including Belle2, and PICO. He holds a PhD, MS, and BS in nuclear engineering from Purdue University.

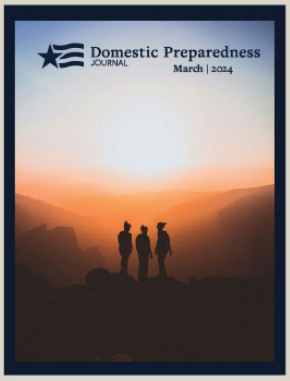
Jonathan Barr is a senior systems engineer with Pacific Northwest National Laboratory's Threat Prevention and Resilience Group. Barr works extensively with stakeholders across the national security and first response communities to understand their operational needs and develop research roadmaps to develop and implement the advanced technologies to meet those needs. He has applied his experience in developing human-centric artificial intelligence concepts and technologies to support the Institute of Electrical and Electronics Engineers in their work to develop ethical AI standards and certifications. Barr is an INCOSE-certified systems engineering professional with an MS in mechanical engineering and materials science from Washington University in St. Louis, graduate certification in medical sciences from the University of Washington, and a BS in mechanical engineering from Kansas State University.

SHARE YOUR INSIGHTS

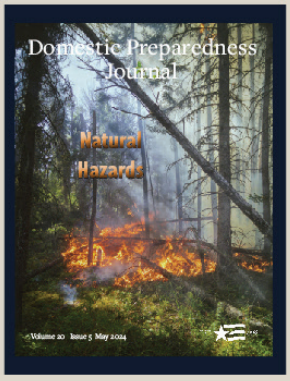
EST 1998

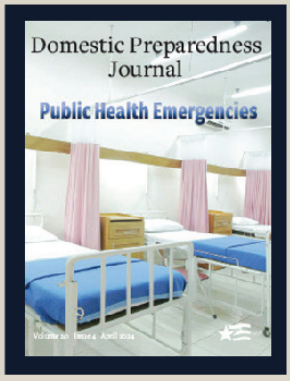


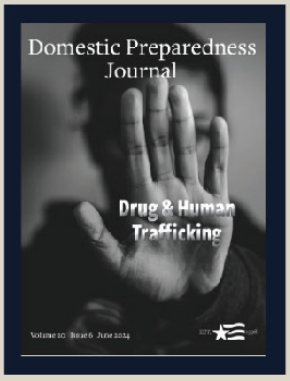




Domesticpreparedness.com/subscribe







SUBMIT AN ARTICLE TO THE JOURNAL

WWW.DOMESTICPREPAREDNESS.COM/AUTHORS

Source: Generated using ChatGPT 4o

Introducing AI to the Emergency Management Workforce: A Case Study

By Lenora G. Borchardt

Artificial Intelligence (AI) is not coming to the emergency management (EM) workforce – it is already here and has been for a while. For example, every time an online search is done using a standard browser, its embedded AI tool searches through the web to provide you with the answer you most likely want. If you have allowed it to do so, the search engine will also learn from engagement over time to refine future searches' answers and push targeted information (e.g., articles or products for sale) based on its continually evolving profiles. This article provides a case study on how a generative AI-based lesson was incorporated to address an EM training course experiencing a widening gap in student outcomes generated by some students' unstructured use of AI.

In this program, faculty observed some student groups completing their work much more quickly and with a wider variety of content. In contrast, others struggled to complete the assignment in the allotted time. The difference was the use of the modern version of high school's "CliffsNotes" but instead of the printed yellow and black printed study guides, these students were using ChatGPT's GPT-4o generative AI tool to create a dynamic guide that answered their specific questions on demand. Recognizing the "culprit," faculty had a choice: ban or embrace its use. Considering the pro-adoption trends in EM and education, the choice was clear: A student-led activity was created to build AI competencies that successfully elicited full engagement and improved content quality.

GETTING TO THE BOTTOM OF STUDENT OUTCOMES

This case study was conducted during a 2024 National Emergency Management Advanced

Academy training program sponsored by the Emergency Management Professional Program through the Federal Emergency Management Agency's National Disaster and Emergency Management University. The program delivers four one-week sessions in a forced-sequential cohort model. It was a local delivery with approximately 20 participants from several U.S. states. The target population was current mid- to late-career emergency management professionals with five or more years of experience and who led teams. The curriculum outcomes were designed to develop individual and team leadership skills and improve the EM profession by teaching students to use current research to create new and innovative best practices, leading the profession forward using the program's "Research, Synthesize, Apply" model.

The cohort's students were leaders in various private and public EM specialties, including university, transportation, hospital, military, first response, voluntary agencies, and traditional county and state government EM. Three faculty members were assigned and remained with the cohort for all four sessions. Faculty assigned students to groups, and faculty members changed the membership of those groups for each course. Observation during the first session showed some groups were finishing work much earlier than others. As faculty observed the first three sessions, they identified specific individuals as common denominators in groups that consistently finished more quickly and had more focused products during activity reports. Upon analysis, the difference was their use of AI.

Faculty observations were that, while the final products were more focused and the content was created more quickly, not everyone in the group had fully participated. Using AI allowed some students to craft their products from a more extensive research dataset and to hone in on the most relevant facts more quickly, moving them from the research to the synthesis stage before their peers. The result was that the "analog students" (i.e., those using traditional online search engines and reading the entirety of the material to glean the pertinent points) disengaged to avoid holding back the process. It was observed that they were unprepared to engage in the synthesis portion without the time to read the materials. They only began re-engaging with the group in the final product's editing and presentation stages. Faculty recognized that AI was both a problem for some learners and a solution for others.

INNOVATING LEARNING WITH AI

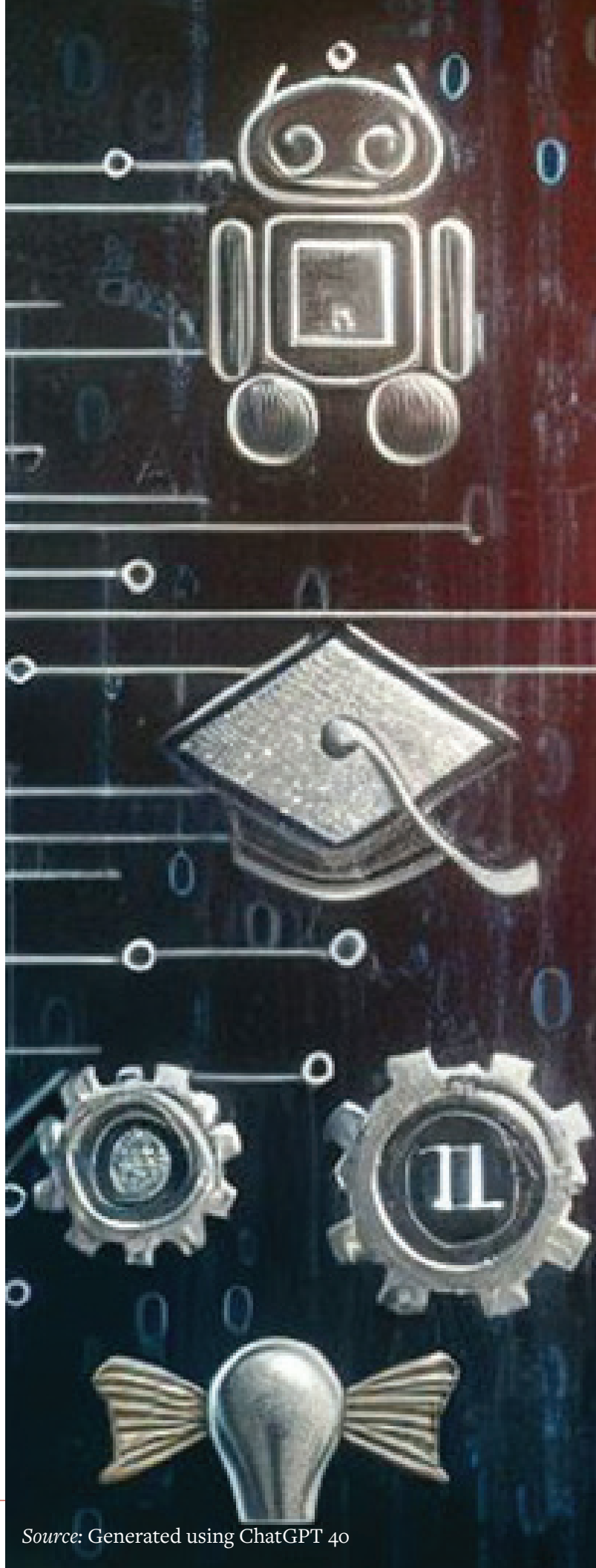
The faculty introduced a learning activity in Week 4 to address this. The standard module content was designed around "leading up" (i.e., influencing those at higher organizational levels). The activity was AI-focused, using ChatGPT's GPT-4o to reinforce the module topic and thread other leadership themes from the previous three weeks.

The lesson plan was that first, one student who had been particularly active in using AI to complete assignments was asked to lead a whole-class session on what AI could do and how to use it for researching EM problems. He had been observed consistently throughout the three weeks, providing AI-generated information to his groups, which proved its value. However, others had not learned to do the work themselves; they "drafted" off his expertise. In this activity, he introduced his classmates to the processes behind his work. Faculty supported his authority on the topic by wholly distributing the activity's leadership (i.e., content, design, and presentation) to him and only minimally engaged to ensure learning objectives were met within the allotted time.

Other students were animated in their questioning and excited about the opportunity to try AI. Research by Miller and Rockabrand has shown that exposing people to AI technology can make them more inclined to use it, which is also evident here. The student leader demonstrated "prompt engineering," which is designing and refining precise and effective instructions or questions to guide the tool in generating accurate and relevant responses. Prompt engineering is a foundational skill for people learning to use AI tools, and poor prompting is often a frustrating barrier for new users because poor prompts lead to poor results. After the demonstration, students practiced designing and refining prompts in a participatory large-group activity using ChatGPT's GPT-4o to comprehensively summarize the introduction to Niccolo Machiavelli's *The Prince*.

Aside from practicing iterative prompt engineering, the goal of this activity was to understand this work's full historical and socio-political context in natural language. *The Prince* was chosen because it is a short book and a foundational text in leadership studies. One of Machiavelli's purposes in writing was to "lead up," which aligned with the module content. It is translated from Renaissance Italian, making the text more difficult, as the language, even in translation, is formal and somewhat convoluted for the modern English reader.

Once the introduction was completed, the groups were shown how to limit the AI client's results to a specific body of knowledge (i.e., instead of the whole internet) by putting the entire book into the ChatGPT interface. This is one way to limit "hallucinations" or false, biased, or misleading information presented as facts. This occurs because the software cannot distinguish the quality of the information; it can only repackage and present the



Source: Generated using ChatGPT 4o

Source: Generated using ChatGPT 40

information it finds in the training data. If the training data is restricted to factual or relevant data, the output reflects that.

The students were then tasked with using ChatGPT to find discussions about "leading up" within the text (i.e., research). Groups were directed to read the original text for context and see the point Machiavelli made in those sections contextualized for his time (i.e., synthesize) using the information from the first activity. Finally, they were asked to apply those points to modern EM problems, negative or positive, and to share what they learned.

After this exercise, analog students understood how to use the technology that enabled them to search an entire book quickly to find relevant portions. Having the material presented in natural language allowed them to grasp "plain English" meaning and context before re-reading the original language to get subtle nuances. An additional bonus of this exercise was that the avid AI users had typically not returned to the original text, and this lesson provided a model to help them expand their comprehension by finding nuances in an author's original writing.

Additionally, the whole group became more effective as they more evenly distributed the workload for fuller participation. The analog students in this case study generally had more professional experience than the AI users. Because of the speed of AI, their practical experience was often not incorporated because the AI users had moved on to the synthesis stage before the analog readers had comprehended the base content. By teaching a structured use of AI, speeding up the analog readers, and slowing down the AI readers, groups worked more cohesively, blending technology and experience to complete the assignment in a novel way that helped each group learn more collaboratively. This became

evident when the final product (i.e., apply) reflected more of the professional experiences of the analog learners.

In post-activity reviews, students appreciated the opportunity to learn about AI. Many had heard negatives about it and were unsure how it worked and whether it was worth the effort. The reviews of the activity were generally positive in post-activity discussions and anonymous written evaluations. Similar results were achieved in additional small-scale tests of this curriculum in other learning environments.

AI COMPETENCY IN EM

This type of AI use in training is foundational to building competency and comfort around AI technology for the existing EM workforce. The barriers to entry are minimal and consist mainly of instructional design time. Professional EM educators and trainers see a near future in which AI will build from these basic activities into more advanced and innovative uses, enabling individualized content and increasingly sophisticated user experiences. Users will engage with AI using natural language communication, simulations, gamification, etc., to assess areas where each learner is strong or struggling. This allows training and education to be tailored to the needs of each learner (i.e., competency-based education), which is reemerging as a leading model for future educational initiatives, possible now because of the technology's ability to assess students and deliver individually-tailored content at a speed that human teachers cannot duplicate.

AI can also be paired with other educational initiatives to increase their effectiveness, as seen when paired with open education resources that use open content licenses to create individualized content, as was done with this assignment. (The age of *The Prince* means that copyright laws do not restrict it, and it is therefore considered open source.) Regardless of future applications, the result is that AI will create competency and outcomes-based learning tailored to each learner's unique needs and learning style preferences while being more efficient for the learner and their employer.

BONUS: If you would like to use this activity, download the lesson plan.

Lenora G. Borchardt, MBA, CEM, MEP, is a seasoned emergency management professional with over 30 years of experience and nearly 25 years in education. Inspired by her family's experience during Hurricane Eloise, she has dedicated her career to advancing preparedness, response, and recovery in diverse settings. Her career spans roles at Meriter Hospital, Wisconsin Emergency Management, and as the emergency management director for Adams County (Wisconsin). Since 2003, she has consulted domestically and internationally with EPTEC, Inc., across all mission areas. Lenora is an instructor at the National Disaster Preparedness Training Center and FEMA's National Disaster Emergency Management University and an adjunct assistant Professor at Pierce College (Washington). She also chairs the training caucus for the International Association of Emergency Managers. She holds a B.A. in geography from the University of Wisconsin–Madison and an M.B.A. from Colorado State University. Currently pursuing a Ph.D. in educational leadership at the University of the Cumberlands, her research focuses on instructional design and adult learning. Note: The project described in this article was not done at Pierce College.

Source: Texas Department of Public Safety, 2024 Cadet Class

A Data-Driven Approach to Police Recruitment and Retention

By Glenn Fueston and Michael Breslin

One growing threat to public safety across the United States is the crisis of recruitment and retention of police personnel. According to a study by the International Association of Chiefs of Police (IACP), *The State of Recruitment: A Crisis for Law Enforcement*, many police agencies face the challenge of recruiting and hiring qualified new police officers to replace those retiring and leaving the profession. The report stated that "[25%] of the responding agencies reported having to reduce or eliminate certain agency services, units, or positions because of staffing difficulties." In addition, a fact sheet by the America First Policy Institute shared that "a 2019 survey of law enforcement executives found that 78% of responding agencies had difficulty recruiting qualified candidates." This nationwide challenge has intensified with societal shifts and recent events. Officers confront evolving daily demands and unique obstacles within their communities, as departments face more challenges in attracting and retaining workforce levels needed to address them.

The complexities of modern policing further compound these challenges. From the rise of advanced criminal networks and borderless crimes to the persistent hurdles of limited resources, inadequate training, and outdated tools, departments navigate an increasingly demanding landscape. Although specifics vary by region, the critical need for comprehensive data-sharing and collaboration is growing across agencies to address these challenges. Awareness of national trends and localized dynamics is essential for addressing increasing pressures.

Challenges in Police Recruitment, Hiring, and Retention

Harnessing the power of data offers a tangible path forward. By leveraging insights and fostering interagency collaboration (e.g., the Federal Bureau of Investigation's InfraGard, the Global Shield Network, and NYPD Shield), law enforcement can begin to counteract the strain caused by recruitment and retention shortfalls. The underlying causes of this crisis are complex and multifaceted, but departments can better adapt to and mitigate these pressing challenges by strategically using information and resources.

Building and retaining the police workforce is a significant challenge. The long and rigorous application process can deter potential candidates. With low unemployment rates and a strong job market, potential recruits have more career options in a competitive job market. This makes it more difficult for law enforcement agencies to attract and retain new officers. Then there are generational differences. Millennials and Gen Z candidates often prioritize work-life balance and job satisfaction over traditional benefits. As a result, the appeal of long-term careers in law enforcement lessens.

Once hired, police officers are less incentivized to stay. Negative public perception of law enforcement resulting from highly publicized incidents coupled with the demanding nature of the job have contributed to application declines. In addition, high-profile incidents and negative media coverage have increased critical opinions of law enforcement agencies. One of the key takeaways from the Council on Criminal Justice's 2020 survey *Public Perceptions of the Police* was that "the percentage of Americans who say they have a great deal or quite a lot of confidence in the police has dipped below 50%.... It's never been below 50%." Officers working during the COVID-19 pandemic experienced higher stress and health risks. Burnout is one contributing factor to early retirement and resignations by some police officers. Earlier-than-expected departures reduce workforce numbers and decrease the wealth of experience acquired throughout long careers.

Key Findings From an IACP Report

IACP recently released the results of a comprehensive survey that sheds light on ongoing challenges in police recruitment and retention across the United States. This survey, conducted in the summer of 2024, gathered responses from over 1,100 police agencies nationwide. Findings underscore the urgent need for comprehensive strategies to address the recruitment and retention crisis in policing. Factors to consider include widespread recruitment difficulties, high resignation rates, and innovative recruitment and retention strategies.

More than 70% of responding agencies reported increased difficulty in recruiting new officers compared to five years ago. This trend is pronounced in the midwestern and northeastern United States, where 81% and 77% of agencies, respectively, noted heightened recruitment challenges. Smaller agencies also reported greater difficulties, with 72% indicating struggles attracting new candidates.

The report highlights a troubling increase in officer resignations. Many agencies are experiencing significant staffing shortages, which increase pressure on remaining officers, leading to burnout and further resignations.

The IACP report also found that approximately 75% of agencies have implemented changes to enhance recruitment and retention. Strategies include loosening restrictions on tattoos and grooming, increasing starting salaries, and developing wellness programs. Despite these efforts, many agencies report mixed results, indicating the need for continued innovation and support.

Leveraging Referential Data and Social Determinants of Health Data

Although police recruiting and retention can be challenging, standards must be maintained to avoid additional problems. For example, dropping or lowering standards arbitrarily can result in subpar performance and unintended consequences impacting the community. However, leveraging new data sets can help.

To address challenges, law enforcement and public safety agencies can leverage referential

data and social determinants of health (SDOH) data to better understand the profiles of their officers. This approach can help agencies place officers more effectively within the organization, hire candidates who are more likely to stay, and reduce turnover within the first five years. Referential data includes information that can be used to compare and analyze various aspects of an officer's profile. This data can encompass demographic information (e.g., age, gender, ethnicity, educational background), professional experience (e.g., previous job roles, years of service, specialized training), and performance metrics (e.g., evaluations, commendations, disciplinary records). The 2023 U.S. Department of Justice report *Recruitment and Retention for the Modern Law Enforcement Agency* cites the efforts of some departments across the country.

By analyzing this data, agencies can identify patterns and trends that correlate with successful long-term employment – for example, the likelihood of officers with certain educational or training backgrounds staying with the department. SDOH data include factors that influence an individual's health and well-being, such as economic stability (e.g., income level, employment status, job security), education (e.g., access to quality education and educational attainment), social and community context (e.g., relationships with family, friends, and the community), health and healthcare (e.g., access to healthcare services and overall health status), and neighborhood and built environments (e.g., quality of housing, neighborhood safety, access to transportation).

By integrating SDOH data with referential data, agencies can gain a holistic view of officers' lives. This comprehensive understanding can inform strategies to improve job satisfaction, work-life balance, and overall well-being, which are critical retention factors. Practical applications for law enforcement agencies to consider include the following:

- *Targeted recruitment* – Using data analytics, agencies can identify the characteristics of officers who have successfully integrated and remained with the department. This information can guide recruitment efforts to target candidates with similar profiles, increasing the likelihood of long-term retention.
- *Personalized placement* – By understanding officers' strengths, preferences, and backgrounds of officers, agencies can make more informed decisions about placements within the department. For example, an officer with a strong community background might be well-suited for community policing roles.
- *Enhanced support programs* – Data on social determinants of health can highlight areas where officers may need additional support. Agencies can develop programs to address these needs, such as financial planning assistance, mental health services, and family support initiatives.
- *Continuous monitoring and feedback* – Implementing systems to continuously monitor officer well-being and job satisfaction can help agencies identify issues early and take appropriate measures. Regular feedback can ensure that officers feel heard and valued, which may improve morale and retention.

Even though agencies may not use the term SDOH, some indicate the overall use of social factors such as health, socioeconomic status, and others in police recruitment and retention. For example, a 2021 Institute for Excellence in Government report shares its research-based recommendations for law enforcement recruiting.

Source: Texas Department of Public Safety, 2024 Cadet Class

Next Steps for Agencies

Overcoming recruitment and retention challenges in law enforcement demands innovative, forward-thinking solutions. Modernizing recruitment processes, prioritizing officer wellness, and fostering stronger community relationships are essential steps to rebuild trust and attract a broad, qualified candidate pool. These strategies address immediate staffing needs and lay the foundation for sustainable growth and operational resilience.

The IACP's report underscores the urgency and complexity of these challenges, offering actionable insights to guide law enforcement agencies nationwide. By integrating referential and social determinants of health data, agencies can craft targeted strategies that better understand officers' needs, optimize placement decisions, and enhance support systems. This data-driven approach is vital for cultivating a stable and engaged workforce.

Ultimately, these efforts fill vacancies and transform law enforcement's culture and capacity. By investing in personnel and adapting to the evolving demands of public safety, agencies can reduce turnover, build stronger teams, and ensure they are equipped to serve their communities effectively and sustainably.

V. Glenn Fueston, Jr., is a seasoned senior solutions architect at LexisNexis Risk Solutions. With over two decades of experience in the criminal justice field, he possesses a deep understanding of data analytics, policy development, and process improvement. Fueston's expertise extends to the collection and analysis of large datasets, having led initiatives that leveraged data to enhance public safety and security. His previous role as a senior advisor to Governor Larry Hogan provided him with the opportunity to oversee grant funds totaling more than $300 million annually. These grants were strategically allocated to entities across the state to reduce and prevent crime through a multidisciplinary approach. As a deputy director at the Washington/Baltimore HIDTA, Fueston was responsible for the collection, analysis, and dissemination of intelligence and information within the region. He oversaw a team that developed, maintained, and implemented nationally recognized tools to disrupt and dismantle drug trafficking operations. These experiences demonstrate his ability to coordinate complex projects and drive positive changes. As a solutions architect at LexisNexis Risk Solutions, Fueston leverages his extensive knowledge of criminal justice challenges to develop innovative data-driven solutions for partners. His unwavering commitment to making a positive impact on society through technology and data is evident in his career accomplishments.

Michael Breslin is a retired federal law enforcement senior executive with 24 years of law enforcement and homeland security experience. He served as the deputy assistant director in the Health and Human Services Office of the Inspector General Office of Investigations focusing on the integrated mission of investigations and protection with oversight of 162 domestic and foreign field offices. He served as the event coordinator for the National Special Security Event papal visit to Philadelphia in September 2015 and was appointed by the secretary of Homeland Security to serve as the federal coordinator for the papal visit to the Mexico–U.S. Border in 2016. He is a member of the Senior Executive Service and is a published author of numerous articles on homeland security, defense, and threat mitigation methods. He serves on the Cyber Investigations Advisory Board of the U.S. Secret Service and is a board member of the National Center for Missing and Exploited Children. He also serves on the Preparedness Leadership Council. He has a B.A. from Saint John's University, an M.S. in national security strategy, and a graduate certificate in business transformation and decision-making from the Industrial College of the Armed Forces, and an M.P.A. from John Jay College of Criminal Justice.

Source: AI-generated by Milos/Adobe Stock

From Today to Tomorrow: The Emergency Operations Center of the Future

By Nick Betzsold and Grant Tietje

Imagine a future world where an emergency operations center (EOC) has tools like artificial intelligence (AI) already in place, both vetted and verified to be trustworthy, and the EOC team is skilled in using those tools. Consider this scenario:

The earthquake struck Metro City at 0746 during the peak of the morning commute. Molly, the Metro City's Class IV AI, had just seconds to act before shaking commenced, based on data from the state's earthquake early warning system. Fortunately, mere seconds are a lifetime to an AI, and Molly didn't waste any time.

While the state system automatically warned residents to drop, cover, and hold, Molly issued an EOC activation notification to all EOC personnel and senior elected and appointed officials. The advent of commercial, low-cost satellite service as a redundant, resilient communication system increased the probability most would receive the message. Using the location of each phone combined with damage assessment information, Molly safely routed personnel to the EOC. Officials even began to immediately get to work on the situation at hand while on their way to the EOC, thanks to Molly's assistance.

Simultaneously, Molly engaged the community. It contacted classrooms, day cares, and long-term care facilities with audience-appropriate warnings and assurances immediately after the earthquake, translated as necessary. The AI was already well-known to the students, having built trust through participation in emergency drills and other school events. In fact, a contest among third-grade students years ago is how the AI got its name.

Following detailed instructions, Molly began streaming damage assessment

information that relied on thousands of sensors – public and private – spread throughout the city and augmented by information from calls to the public safety answering point (911), by public safety radio traffic, and by social media posts. After notifying the Federal Aviation Administration that it was activating pre-disaster authorization for flight, Molly launched its unmanned aerial systems as mobile sensor platforms and initially assigned them to fill in reporting gaps caused by damage.

Meanwhile, the EOC director verbally confirmed the activation decision and instructed Molly to initiate Protocol 1. This triggered a series of scripted actions for Molly to accomplish before the EOC team arrived. It included arranging meetings for the director with the mayor and department heads, sending an emergency declaration to the mayor for approval, releasing previously approved standard public-safety messaging to multiple communications platforms, and more. Most importantly, it authorized Molly to function as the common platform for data, information, and intelligence sharing and collaboration between the city and supporting agencies at all levels, non-governmental organizations, and volunteers, as designated in the city plan and in support of disaster information transparency goals. Molly is capable of filtering and presenting data, information, and intelligence based on EOC personnel roles, responsibilities, and learning preferences.

Under Protocol 1, an automated request for mutual aid was sent to EOCs outside the impact area via the interstate Emergency Management Assistance Compact. These were designated partner agencies that had agreed ahead of time to respond when needed. Within minutes, the staffing of the Metro City EOC was augmented by virtual responders equipped with tools like augmented reality and virtual reality technology and capable of maintaining the requisite level of staffing for weeks if necessary. Similar arrangements were in place between city department operations centers and their counterparts in other jurisdictions. The extensive training, planning, simulations, and exercises with these partners now paid off. Had the Metro City EOC been rendered inoperable, these same EOCs were authorized to step in and take over with support by Molly.

For responders in the field, Molly created a human-impact analysis based on patterns of life, cell phone location data, building permits, and other inputs to guide responders to the most likely areas where casualties and people trapped could be found. This was only possible through a public records act that established a local, nonprofit, government-funded data security company operated by and for the public to protect private data while ensuring responders had the information they needed during emergencies. This AI-operated system authorized the release of private data and then monitored how it was used by government officials. When the emergency was over, it ensured all data was erased.

Much of the technology in this story either already exists or is on the near horizon. Augmented and virtual reality, digital twins (virtual models of real-world objects or

places), large language models, virtual mutual aid, sensors, analytics, modeling, unmanned autonomous systems, and a common AI platform (e.g., Molly) are just some examples of tools that are beginning to transform how disasters are managed.

This next-generation EOC concept does not promise perfect disaster management, but it does mean responders at all levels will have better situational awareness, plan more efficiently, and act faster. EOC team members will have time to collaborate, focus on solutions, and work at a pace that is sustainable. The revolution of EM-capabilities powered by AI is only just beginning. Currently, many technologies have the potential to transform emergency management. What is needed is a commitment to a rapid, coordinated design process that can transition technology to the EOC. This will involve fundamental changes in how disasters are managed.

What Is Next for the Next-Generation EOC?

To assess the feasibility of this vision for the "EOC of the Future," an in-depth landscape assessment, stakeholder outreach, and a series of tabletop exercises explored how the rapid and accelerating pace of advancements in science and technology can be highly disruptive to emergency services.

In moving the needle toward the EOC of the Future, an assessment of the history of EOCs, a review of current emergency management research and development (R&D) and EOC operations, and feedback from EOC team members identified recurring foundational concepts for the future reflected in Metro City:

- Next-generation data management
- Continuous, real-time situational awareness
- AI automation and human-machine teaming
- Human-centered design of workspaces
- Hybrid EOC operations
- Resilient system design

Source: AI-generated by Milos/Adobe Stock

- Whole community approach
- Forward-leaning workforce development

However, every new technology comes with new challenges – particularly funding, interoperability, and policy barriers. For such futuristic concepts, fostering trust and buy-in from end-user communities is a formidable obstacle, particularly as tasks AI is permitted to take on increase in complexity and consequence. Trust can be built through a collaborative and iterative process of research and development, transparency, processes for validating information, commitment to safety, and experience. Most important is the need for an AI that is specifically developed for responders at all levels, including EOC operations, instead of adapting existing systems. All of this will need a foundation of ethical guidelines and best practices developed in partnership with the community.

The Future Is Now

Returning to the EOC of the Future scenario, a next-generation combination of tools has enabled efficient, integrated response:

> *Although it might seem to be almost sentient, Molly represents a relatively simple system that depends on several*

plans, protocols, and instructions developed beforehand by the emergency management team.

Gone are written situation reports that are out of date before they were published. Sensor-enabled continuous situational awareness coupled with modeling and simulation describes the current state and possible future changes in status and outcomes. This has the potential to change how planning is done as well. With all personnel drawing from the same well, resource conflicts are reduced and operational timing, sequencing, and coordination improved. Planners can quickly model options and, to some degree, identify second- and third-order effects.

Such improvements may also turn the vision of a whole community response into reality. Molly provides the means for registering volunteers, assigning them to appropriate missions and tasks, monitoring their activity, and coordinating with responders.

It sounds futuristic, but in today's era of AI-enabled transformation and productivity, the EOC of the Future is feasible. By bringing together the right mix of end-user-informed vision building, testing, and evaluation and by adapting policy and standard operating procedures, a more resilient emergency management system can emerge that stands ready to face the challenges of tomorrow. The next-generation EOC will blend operators and optimal tooling to forge a path toward a safer, more secure future. Getting there will take not only continued research and development of emerging technology but also engagement from EOC personnel within the R&D community to discern how it can best meet their needs today and in the future.

Nick Betzsold is a data scientist at Pacific Northwest National Laboratory (PNNL) where he has led project tasks devoted to AI and machine learning, statistical computer programming, and risk tool concept of operations development. He joined PNNL as an undergraduate intern within the Applied Statistics and Computational Modeling group and conducted research in national security and infrastructure risk analysis, power grid data analytics, R Shiny web app development, and various data/statistical analysis projects. He obtained his master's degree in data science at Northwestern University. Today, his work is primarily within PNNL's National Security Directorate, and he serves as the Aviation Security and Soft Targets Homeland Security Subsector Lead.

Grant Tietje is a former paramedic, police officer, and emergency manager. He was a program manager at Pacific Northwest National Laboratory (PNNL) and led research and development of technology solutions for first responders. He is now president of Front Range Planning, a company dedicated to supporting first responders through training, exercises, and planning.

Source: AI-generated by Maxim/Adobe Stock.

Protecting Critical Infrastructure From Weaponized Drones

By David Winks, Steve Chill, Frederick Ferrer, Michael "Apollo" Lovell, Mike Swearingen, and Mary Lasky

In November 2024, the Federal Bureau of Investigation (FBI) thwarted an attack on the Nashville power grid by a man attempting to use an explosive-laden drone. The FBI indicated that the defendant had ordered the explosive C4 from undercover agents. In the U.S., most critical infrastructure was designed and built in a relatively low-threat environment, designed to survive weather events, minimize accidents, and prevent theft, rather than built to protect against attack or sabotage. The idea that people would intentionally destroy infrastructure was generally not considered. For instance, in the energy sector, most substations were simply protected by chain link fences and signage indicating the dangers of high voltage. The reason for fencing was to deter theft and protect the public. In response to the 2013 Metcalf substation attack, utilities – the North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC) – began to improve transmission substation security. While ballistic walls are effective at protecting transmission substations against rifle fire, this protection still leaves property vulnerable to weaponized drones attacking from above.

Wars in Ukraine and Israel have shown how drones can be used to destroy civilian infrastructure. In a similar fashion, transnational crime organizations embrace weaponized drones to combat rivals and police, as the use of weaponized drones is spreading beyond war zones. In 2020, a drone was used in an attempt to disrupt the U.S. power grid by attacking a substation in Pennsylvania by dropping a metal cable across high-voltage lines. Fortunately, the attack was unsuccessful. However, it is only a matter of time before a drone attack disables or destroys critical infrastructure.

Several technologies can be used to protect infrastructure from drones, including large nets, net guns, radio frequency (RF) and global navigation satellite system (GNSS) jamming, and cyber spoofing. Using other technologies – such as "frangible" ammunition that becomes tiny pellets when fired from conventional firearms, ground-based and aerial lasers, and RF weapons – will need additional legislation and regulation.

Currently in the U.S., critical infrastructure protection is the responsibility of infrastructure owners. Protection options are limited by Federal Aviation Administration (FAA) regulations that prevent shooting down drones. Defenders can use RF jamming, GPS spoofing, and net guns for non-destructive removal of drones as long as they comply with federal regulations. As counter-drone systems have been deployed in Ukraine and Russia, drone technologies have also changed. Drones are now being controlled by a spool of very fine fiber-optic cables up to six miles. Using fiber-optic control overcomes radio frequency detection, RF and GNSS jamming, and cyber-spoofing defenses.

In Ukraine, drones with Thermite spray – a combination of aluminum and iron oxide powder – act as flying flame throwers, igniting the tree lines where Russian forces are hiding. When ignited, Thermite spray produces molten metal at about 4,000 degrees Fahrenheit, which can melt through the steel armor of tanks and trucks to ignite the fuel and weapons inside them. Adversaries can use the same type of drones to overcome fixed netting at substations. Thermite spray can be used to ignite the oil used in substation transformers. Napalm and white phosphorus can also be dropped from drones as incendiary weapons. Similarly, highly conductive graphene powder can be dispersed over a substation. The graphene powder short-circuits equipment, causing arcing across bushings, which can damage transformers.

The Threat Mitigation Process

A process the military uses for countering drones can be adapted for the protection of critical infrastructure. It consists of shaping, sensing, warning, intercepting, responding, protecting, commanding, and controlling:

- Shaping reduces attack options and forces attackers into more easily defended approaches.
- Sensing tracks drones and helps identify friends from foes.
- The warning allows site workers and responders to seek protection.
- Intercepting captures or destroys incoming drones in flight.
- Responding enables law enforcement or the military to apprehend attackers.
- Protecting closes off weaknesses and further protects critical assets.
- Commanding and controlling occur throughout the process to coordinate defensive actions and record tactics, techniques, and procedures to inform other vulnerable sites.

Several techniques can be used to detect and identify drones as they approach critical infrastructure. These include acoustic detection, optical and infrared sensing, radio frequency sensing of control channels, light detection and ranging (LiDAR), and radar. Each approach has advantages and limitations. Ukraine uses a network of several thousand pole-mounted cell phones as sensors to inexpensively track incoming drones acoustically:

- Acoustic sensing can be limited by noisy environments and quiet drones.
- Optical and infrared sensing can be effective but requires a line of sight, which may be affected by dust and fog environments. Attackers may pick an approach with the sun behind them to limit optical sensor effectiveness. The infrared signature of a drone may be quite small, leading to false positives.
- Radio frequency direction-finding can provide accurate direction but may have issues with range accuracy for rapidly moving drones.
- LiDAR can provide precise characterizations of an incoming drone but may be affected by dust, rain, and heavy fog.
- Compact radar systems offer the advantages of all-weather, all-time detection. Unfortunately, radar emissions can also be used as homing signals for drones.

Active and Passive Defense

Several technologies can actively capture or disable drones. Net guns launch nets that tangle the propellers of incoming drones, causing them to crash. These can be ground-launched or launched by defensive drones. The U.S. Army has developed an expanding net that can be launched from a standard grenade launcher.

Frangible ammunition can be used from rifles or radar-controlled guns to disable drones. Frangible ammo breaks into small pieces to minimize any collateral damage beyond the target. The effect is similar to skeet shooting.

The U.S. Army is deploying radar-controlled guns along with laser weapons for counter-drone protection. As technology advances and costs come down, lasers or radar-controlled guns with frangible ammunition could be viable solutions to protect critical infrastructure sites.

In addition to lasers and radar-controlled guns, it is possible to defeat drones using phased array high-power microwave systems. These systems use radiated electromagnetic pulses at microwave frequencies to destroy the drone's control electronics. The sudden change in voltage on control circuitry damages the chips in the drone control system, and the drone loses control and crashes.

One concern with active-defense measures is the potential for collateral damage beyond the target. Bullets, lasers, and high-power microwave weapons require coordination with the FAA to avoid affecting aircraft. Therefore, protecting critical infrastructure in urban areas may be difficult with active-defense solutions.

With the increasing sophistication of drone attacks, infrastructure owners may need to rethink how to design and build facilities. Adding concrete walls and a roof may not be suitable for many existing substations with limited space.

Figure 1. The DragonFire laser shooting at an aerial target (*Source:* UK Ministry of Defence).

Concrete walls require a significant below-grade foundation. One option is to use composite panels for ballistic protection.

It may be necessary to consider building new underground structures in parallel to existing facilities to counter the threat of weaponized, fiber-optically controlled drones equipped with Thermite spray, incendiaries, munitions, and graphene powder.

Command and Control

Many critical infrastructure owners have network operation centers and security operation centers. These are connected to infrastructure sites by fiber, cellular, and satellite links. In the Metcalf substation attack, fiber-optic cables in two communication vaults belonging to AT&T and Level 3 were cut. This action disabled some of the area's landline, cellular, and internet communications, as well as the 911 center. Once the communications were disabled, attackers shot holes in transformers, causing millions of dollars of damage. These tactics emphasize the need for multiple communication technologies at critical sites.

Satellite communication companies provide flat-panel antennas and electronics that can be used for remote alerting at relatively low costs. Their low profile and small size make them difficult for attackers to destroy. While

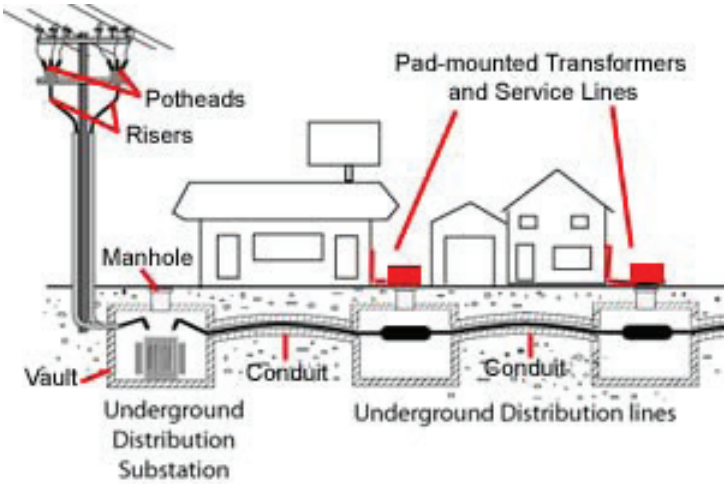


Figure 2. Underground distribution substation (*Source:* Occupational Safety and Health Administration).

the data rate is fairly low, it is sufficient for alerting and control. To relay high-speed data, such as images from cameras and Forward Looking Infrared (FLIR) systems or data from Identification Friend or Foe systems, Low Earth Orbit satellite internet data Starlink terminals can provide excellent connectivity. Both solutions provide diverse paths that operate in addition to terrestrial connections.

Next Steps

An analysis is needed to determine which critical infrastructure sites should be protected first. The analysis could consider the possible approaches for defending each site and then recommend the most effective means of protection against emerging drone threats.

Legislation is needed to define exclusion zones for specific activities around critical infrastructure. The legislation should allow critical infrastructure owners to intercept, disable, or destroy drones within the exclusion zone. The legislation may need to address the placement of acoustic, optical, LiDAR, and miniature radar systems, drone identification systems, drone capture systems using net guns, or drone disablement using frangible bullets from human-in-the-loop automated systems, lasers, or high-power microwave systems.

Given the challenges of legislative approval for active-defense measures by utilities and private companies, critical infrastructure owners may need to consider passive protection by fully enclosing above-ground infrastructures using ballistic panels or reinforced concrete roof and walls or by building underground infrastructure for existing facilities.

Congressional action is needed to protect critical infrastructure from the clear and present danger posed by weaponized drones. Congress must provide guidance and funding to install counter-drone systems, encasement, or undergrounding of critical sites. FAA regulations need to be amended to provide exclusion zones around critical infrastructure sites and rules by which critical infrastructure security teams can shoot down weaponized drones before they destroy the infrastructure.

David Winks is the senior advisor for Advanced Technology. He currently serves as a subject matter expert for the Foundation for Infrastructure Resilience and as part of the U.S. Department of Homeland Security (DHS) Resilient Power Working Group. He has been a subject matter expert in the U.S. Department of Defense's Electromagnetic Defense Task Force and the North American Electric Reliability Corporation EMP Task Force. He is co-author and co-editor of the book Powering Through – Building Critical Infrastructure Resilience, *author of the report* Protecting the U.S. Electric Grid Communications from EMP, *and a contributor to the DHS Cybersecurity & Infrastructure Security Agency report* Resilient Power Best Practices for Critical Facilities and Sites. *Currently working on advanced data centers using immersion cooling for secure environments, David has developed cyber defense architectures utilizing binary hardening, software-defined perimeters, zero-trust access, artificial intelligence, automated orchestration, and restoral for information and operational technology networks. His work includes EMP-shielded natural gas turbines, fuel cells, Stirling engines, solar thermal systems, wind, geothermal, and hydropower generation. He is a co-inventor of a patented, rugged, ground-conformal solar thermal system. David has a degree in physics (cum laude) with additional coursework in electrical and mechanical engineering.*

Steve Chill is a retired Marine with decades of security experience in domestic and overseas environments. He has executed or created U.S. Department of Defense/Service policy for the security of special weapons, ships, and bases of all types and units ranging in size from combatant commands down to the individual Marine. He was recently an author/editor of both Joint Base San Antonio's guide titled Domestic Electromagnetic Spectrum Operations *and Infragard's* Powering Through: Building Critical Infrastructure Resilience.

Frederick Ferrer is a national intelligence professional, homeland security expert, and educator. He is a 20-year military intelligence veteran who worked with the upper echelons of the U.S. intelligence community before retiring and returning to his home state to complete a PhD program of studies in American history, with minors in Russian and European history. Mr. Ferrer's last posting was at the Idaho National Lab's National Security Division. He held top secret security clearances across a half-dozen agencies over four decades. Mr. Ferrer currently teaches topics like counterintelligence, cyber- and anti-terrorism for various universities across the nation.

Brigadier General Michael J. "Apollo" Lovell, USAF (Ret.), served as the United States Strategic Command Mobilization Assistant to the Director of Intelligence and flew 212 mission-hours as the Airborne emergency action officer on the E-6B Looking Glass Airborne Nuclear Command Post. General Lovell is an intelligence, surveillance and reconnaissance, and cyber senior leader who served the Texas Air National Guard as the director of intelligence. He is an ISR mission commander with over 1,800 mission hours in the MQ-1, MQ-9, MC-12, RQ-4, RQ-170, and U-2. He has a master of science in executive leadership and is a graduate of the Maxwell School's National Security Studies at Syracuse University and Kenan-Flagler's Executive Development program at the University of North Carolina.

Mike Swearingen is a retired electric cooperative power systems engineer with 20+ years of experience. He has worked in every aspect of power systems operation, including control systems, protection systems, transmission design, substation design, distribution design, and NERC compliance as well as regulatory matters. He represented his cooperative as a member of the Transmission Working Group, Market Operations and Policy Committee, and Market Working Group at the Southwest Power Pool. He served as an analyst and independent merit reviewer on several projects at the Department of Energy, was a technical advisor for the National Electric Energy Testing Research and Applications Center, and is an IEEE senior member.

Mary Lasky, a Certified Business Continuity Professional, serves as the program manager for business continuity planning for the Johns Hopkins University Applied Physics Laboratory, where she coordinated the APL Incident Command System Team. She also is a member of InfraGard, where she is the vice chair for the InfraGard EMP-SIG. In Howard County, Maryland, she served as president of the Community Emergency Response Network Inc.; president of the board of directors of Grassroots Crisis Intervention Center; and for Leadership Howard County is co-chair of the steering committee for the Leadership Premier Program. For many years, she has been adjunct faculty at the Johns Hopkins University Whiting School of Engineering. She is the immediate past president of the Central Maryland Chapter of the Association of Contingency Planners and has held a variety of supervisory positions in information technology and in business services. Her consulting work has included helping nonprofit organizations create and implement their business continuity plans.

Advisor Spotlight: Interview With Caroline Agarabi

Caroline Agarabi, Ph.D., discussed her professional journey into domestic preparedness with *Domestic Preparedness Journal*'s Nicolette Casey. Dr. Agarabi is a medicinal chemist who now regulates medical countermeasures in response to CBRN incidents. In this interview, she shares her passion about domestic preparedness and the *Journal* and her intrigue with new developments in crisis communications.

Nicolette: So happy we get to talk this morning. I really am.

Caroline: Me, too! Thank you so much for rescheduling. I know it was, you know, coordinating schedules and stuff, and time zone, so thank you for making it work. I really appreciate it. Yeah.

Nicolette: I appreciate you taking the time to sit with me and just chat a little bit about domestic preparedness. So cheers to our first cup of coffee, or maybe you're second or third. I'm not sure, but I'm right behind you. So, how are you doing this morning?

Caroline: I'm doing great. I have to say, I really like the series that you're doing on the board members because it's such a wealth of talent and you know, breadth of experience. It's a lot of different people, and I'm, you know, I get to see the people I see in my work sphere, but it's so nice to have that zoom-out perspective and to see, you know, the expertise that the

whole board brings to bear. So I really like the spotlights you're doing. And I think it's a really nice way to showcase, you know, what's going on at the *Domestic Preparedness Journal*.

Nicolette: Absolutely. It's one of those things that we looked at. And it's like, wow, look at who we have backing this journal. Look at who we have backing this publication. We need to push it to the forefront because we're really proud of who we have working with us.

You know, the articles that are written, are written by people with lots of experience and lots of knowledge and a whole lot of heart, you know, within this field. So, people like you. So, I'm really excited to get into this, because just as you are, you know, excited and proud to be a part of the board, our subscribers, our listeners, our readers, are excited to hear what you have to say about it, as well.

Caroline: Well, thank you. Yeah.

Nicolette: Let's jump right in. So what inspired you to join the Domestic Preparedness board?

Caroline: Yeah. Well, for a long time I was a reader of the *Journal*, and I met Cathy at a conference for the International Fire Chiefs Association and hazardous materials, and I went up to her, and I was really excited to meet her because I really enjoyed reading the *Journal*. And I just wanted to know more about the *Journal* and who was behind it and if there were ways I could get involved. And I knew from my scientific background that sometimes a good way to get involved in a new sphere is to offer to read manuscripts.

And so I expressed my interest in that, and Cathy called me a few months later and said, "Hey, do you want to help?" And I said I would love to. And then she offered me a job on the board, or a position on the board, and I gratefully accepted. So I was so happy about that. But essentially I started as a reader who just found that the Domestic Preparedness Journal was a really great resource for someone coming from another field into the domestic preparedness space. And then my interest grew from there.

Nicolette: Wonderful. I didn't know that's how that worked with you and Cathy. That's wonderful.

Caroline: Yeah.

Nicolette: Okay, excellent. Can you share a bit more about your background and how it ties into emergency preparedness?

Caroline: Sure. I don't have a typical emergency preparedness background, and I think that the moral of the story is that, you know, it takes all kinds of people. It takes all sorts of people, and that, you know, I think the message I want to convey is that whatever your skill set is, it can come to bear to help people in the domestic preparedness space if you have a mind to do that. My background is I'm a medicinal chemist of natural products and a pharmaceutical scientist by training. I hold a PhD. In biomedical and pharmaceutical science. And I spent several years at the FDA regulating drugs, medical devices, tobacco products. And, being a person who's curious, inquisitive, willing to take on stretch assignments, I ended up regulating medical countermeasures or medical drugs and devices intended for the response to chemical, biological, radiological, and nuclear incidents.

Nicolette: Wow!

Caroline: Yeah, I did not expect, you know, to take that left turn at Albuquerque. I had no idea I would end up in the preparedness space. But I think what's very attractive to me about it is that it is so multidisciplinary and that you do meet so many different people with so many different types of expertise. I like being a scientist, but I also like getting out of that bubble and hearing from first responders and hearing from people who are, you know, using these medicines, deploying them on the frontlines, etc. And so completing that circle really brings me a lot of fulfillment, to

know that I'm not just pushing paper in an office, that I'm actually helping, you know, make sure that medicines that are needed get to the people that they need to get to, and the time they need to get to. So that's how my background ended up letting me in the domestic preparedness space. I currently work at, as you can see, the Administration for Strategic Preparedness and Response in the Department of Health and Human Services, and there I help develop capabilities and requirements that would be needed to respond to a civilian mass casualty event of a chem/bio/rad/nuke nature.

Nicolette: Wow! Important work! That sounds that sounds exciting. That sounds powerful. That sounds...wow! I'm sure you have a lot to write about. I'm sure you have a lot to write about for sure. Now, as far as your articles go, I'm assuming you've already contribute to Domestic Preparedness.

Caroline: I have not. You know, yeah. And so I do enjoy writing. But I will say that the majority of my support has come in the form of reviewing articles, and that's in large part, because, you know, we have a press office, and things have to go through clearance, and it just takes a long time. But that doesn't mean that I haven't been thinking about potential articles or listening closely on the board member calls about your upcoming issues and your themes, and how I might be able to support and help in a timely way. But again, it's the slowdown of like I don't know how fast I can turn around written copy, get it cleared through my organization, and then to you guys on time.

Nicolette: Right. Oh, it would be amazing to have you contribute, because you bring such a beautiful energy, and you seem very excited about what you're talking about, very knowledgeable, and fresh. You sound like you have a very fresh perspective on it. And I think that would really attract our listeners. So we definitely have to circle back and talk to Cathy about maybe, you know, the next year and what those topics are, because I feel like we've got to have you in there. We've got to have you. Next year we've got to have you in there.

Okay, so that leads me to my next question, which is, what do you see as the biggest challenges or opportunities that we have in preparedness right now?

Caroline: Yeah, yeah, challenges. It's never just one thing. It seems like it's, you know, we're in an age of poly-crisis or multiple things going wrong at the same time. So you can't just assume it's a biological, infectious disease event. There's also a hurricane or a large-scale power outage or some other, you know, a pipeline goes down or a bridge goes down. The Francis Scott Key Bridge is very close to where I live, etc. So I think the challenges include, you know, first of all, this is not a single-player sport. This is not a single event.

This is, how do you marshal the resources? How do you, you know, build your networks and your teams in different, you know, agencies inside of government, outside of government, at the state and local levels, tribal territorial levels, internationally? How do you build your coalitions quickly to respond to these multi-pronged events, which are very rarely, you know, as anticipated or as planned? So that adaptation to poly-crises – and having good people around you, I see as the challenge and also the opportunity, because I think, you know, there are so many people in the preparedness space who are dedicated and who care and want to help, and they don't all look like someone who has a PhD in chemistry. They don't all look like a law enforcement officer, but they look like a lot of different people. They include those people. They look like a lot of different people. They're also, you know, I see a lot of young people in my neighborhood, teenagers who want to get involved in firefighting and their communities and helping in ways that they aren't really sure of what that will lead to. But I see a lot of people willing to help, wanting to help,

engaging those people before the poly-crises happen, activating them to, you know, mount a response. I think those are the opportunities and challenges that exist in the space.

Nicolette: Thank you. That's very true. Now, what would be one key takeaway you'd like to share with our readers about staying prepared?

Caroline: Wow! Okay, staying prepared, you know. I think it's like fitness. You have to, you know, just a little bit every day, you know. Don't go crazy, a little bit every day.

Prepare for Tuesday. You know I am a big believer in, like, do things that are going to be good for you anyway. Is it a good idea to, I don't know, have a little extra water on hand? Sure, it's always a good idea. It's not, you know, ever going to be a negative thing.

It's always a good idea to know who your neighbors are. Who would you call? Who can you help? Who might call you if they need some help? And I think just some simple steps, like, you know, going to the gym several times a week, or, you know, just preparing for Tuesday, as I mentioned, those small things that are good for your life anyway. Help people stay prepared. But also, you know, knowing what is going on in your community, knowing about your helpers in your community. Knowing, you know, do you have the number for the fire department other than 9-1-1, do you have, you know, a plan if those people are delayed? Do you have fire extinguishers in your house? Stuff like that I think is important, just good practice, but also helps people from getting burnt out or afraid or frozen. Don't be frozen. There's always a way to move forward. I'm a strong believer that there's always another way forward, and so just find the way to move forward and find the people who are willing to move forward with you.

Nicolette: That's a very good piece of advice. Now, do you have any advice for someone new to the field, maybe new to your field, maybe new to the preparedness field in general?

Caroline: Yeah, I consider myself new. I never thought that I, you know, would have, that my professional, you know, experience would be of value in the preparedness field. But I saw this job opportunity, and I applied, and it's turned out to be an amazing fit.

I would just say that the preparedness field is so – for people who don't like doing the same thing every day, there will always be something new or different for you to do in the preparedness space. And there's job security. I mean, I wish for a peaceful and calm world, but I think that what can be guaranteed is that we are going to have to continue to, you know, respond to crises and to emergencies, and think about how to recover and how to, you know, support communities that have undergone, you know, severe tragedies. It does not just, you know, the response doesn't end after a few months.

So, what I have been surprised by, and what I would share with anyone considering this field, or who haven't considered this field before, that it is broad – there is a great need for people to help, and I think a lot of people have that helping heart. And they want to, you know, know how to do that. And just know that there are other good people out there, too, who want to do the same thing. You might disagree about how that gets done. But the sentiment is a positive one, and building on that is key and just staying interested, staying inquisitive, staying open, staying open to other people, new ideas and new experiences, and not being afraid to get your hands dirty.

Nicolette: Love that. Now what do you see is on the horizon in emergency preparedness. Is there anything else you want to leave us with before I let you go today?

Caroline: Yeah. Leaving with, okay. You know, there are a couple things. I do think that communication – I do not know how exactly, but I've been thinking a lot – I took this great class in communication, crisis

communications. I am going to give a little plug to the teacher Dev Heilman, who runs the Institute of Crisis Management, and she runs a great crisis communications course. She would be a great person for an article. So maybe I'll hit her up, yeah.

Nicolette: Yes, I am writing her name down.

Caroline: Yes, but the way we communicate during crises and after crises, restoring, you know, a sense of community or a sense of authenticity or credibility, I think, in communications, is really important. How people get their news today is very different from how people got their news in 2004, and so I imagine another 20 years, it will also change. But just finding a way to make those communications authentic, sincere. She would often say, Deb, no one cares what you have to say until they know that you care about them and their situation, and that is really true, and we have this ability to connect with anyone around the world in multiple, real-time Internet exchanges. And yet there is a feeling of being disconnected or unclear about, you know, who's trustworthy and what messages are trustworthy. And so some sort of innovation in communication in the preparedness space, I think, is warranted. I do not know how that would happen. I do not know what that looks like.

But I will say, after taking this class on crisis communications, I have a great respect, and I want to know more about how the communications professionals do their job because they, you know, it can all – all the best laid plans, all the best logistical support can fall by the wayside if people do not know the resources are there, if people don't know where to pick up the water when they are on a boil advisory for a week after a hurricane. You know, so there, there is going to be something with communication. I'm also really interested at this intersection of cyber signaling and maybe I'll save that for another time, but some intersection between, you know, cyber signaling or radio frequency, or some sort of at-a-distance activation of chemistry, because that is my area of interest. That is something I also think we should be, looking into it more. I think, I do not know exactly what that would look like, but I think we have seen some events earlier this year, where we saw cell phones activated for military defense purposes. And I think that that's a very powerful thing as well, the fact that we all carry around cell phones. We all have smart devices all around us. You think about the opportunities present in that. And yeah, it makes me wonder, I would like to know more about that. That is something I, and perhaps the preparedness space as well, you know – it could be new and different for the preparedness space to consider as well.

Nicolette: No, you are absolutely right. We will have to talk about that at a later time. Maybe that's what we ask of you for, you know, next year. I mean, it would be amazing to have you contribute, and I'm sure not the only one that thinks that. So, we'll have to circle back. But I have really appreciated the conversation.

Caroline: Me, too! Thank you so much, Nicolette.

Nicolette: Thank you so much, Caroline. It has been a pleasure talking to you, and I hope we can do this again soon.

Caroline: Great talking to you, too. Yes, absolutely.

Caroline Agarabi, Ph.D., is a biomedical and pharmaceutical scientist with expertise in the medicinal chemistry of natural products. She serves as an interdisciplinary scientist at the United States Department of Health and Human Services Administration for Strategic Preparedness and Response. There she develops requirements for medical countermeasures intended for procurement by the U.S. government and the Strategic National Stockpile. Her work also contributes to the development of capabilities, strategic policy options and alternatives, and operational planning for disaster scenarios, including chemical, biological, radiological, and nuclear (CBRN) threats as well as emerging and infectious diseases.


EST 1998
Domestic Preparedness
Real-World Insights for Safer Communities
We Cover It All
Subscribe Today!
www.domesticpreparedness.com/subscribe