

DomPrep Journal



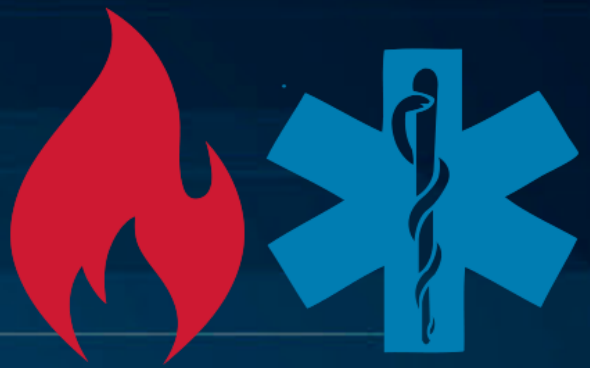
[Subscribe](#)

Volume 19, Issue 7, July 2023

Planning Strategies

Fire-Rescue International

International Association of Fire Chiefs



August 16-18, 2023

Kansas City Convention Center | Kansas City, MO

CELEBRATING
150

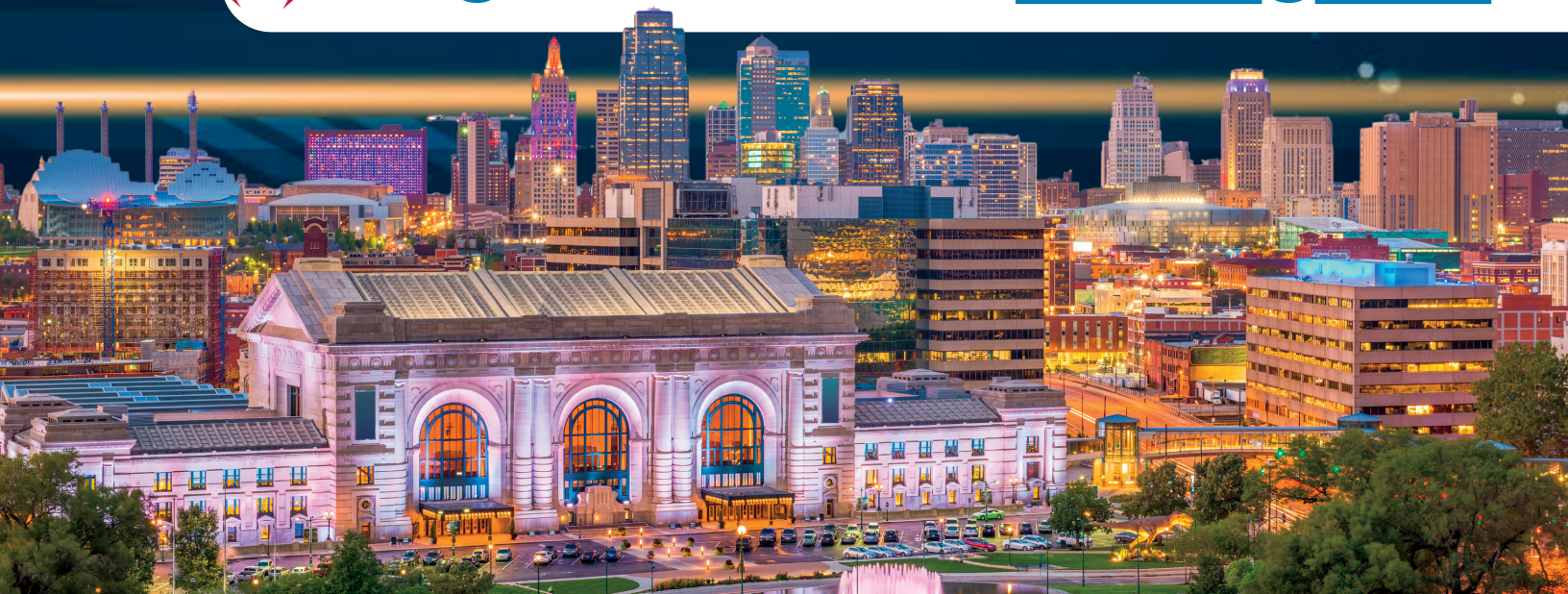
1873 - 2023

INTERNATIONAL ASSOCIATION OF FIRE CHIEFS

HONOR TRADITION **EMBRACE INNOVATION**



Register Now at iafc.org/FRI



Business Office

313 E Anderson Lane
 Suite 300
 Austin, Texas 78752
www.DomesticPreparedness.com

Staff

MacGregor Stephenson
 Publisher
macgregor.stephenson@tdem.texas.gov

Catherine (Cathy) Feinman
 Editor
cfeinman@domprep.com

David "Randy" Vivian
 Business Outreach
randy.vivian@tdem.texas.gov

Bonnie Weidler
 Publications Liaison
bonnie.weidler@tdem.texas.gov

Madison Leeves
 Marketing Manager
madison.leeves@tdem.texas.gov

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

Advertisers in This Issue:

IAFC Fire-Rescue International

TEEX Response
 Leadership Podcast

© Copyright 2023, by the Texas Division of
 Emergency Management. Reproduction of any
 part of this publication without express written
 permission is strictly prohibited.

Domestic Preparedness Journal is electronically
 delivered by the Texas Division of Emergency
 Management, 313 E Anderson Lane Suite 300,
 Austin, Texas 78752 USA; email: subscriber@domprep.com.

The website, www.domesticpreparedness.com,
 the *Domestic Preparedness Journal* and the
 DPJ Weekly Brief include facts, views, opinions,
 and recommendations of individuals and
 organizations deemed of interest. The Texas
 Division of Emergency Management and the
 Texas A&M University System does not guarantee
 the accuracy, completeness, or timeliness of, or
 otherwise endorse, these views, facts, opinions or
 recommendations.

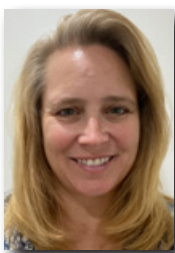
Featured in This Issue

Maintaining Planning Strategies for Evolving Threats <i>By Catherine L. Feinman</i>	4
Creating a New Standard for Evaluating Tabletop Exercises <i>By John Duda and Scott J. Glick</i>	5
Long-Term Care Facilities in Emergency Preparedness Planning <i>By Tanya Scherr & Daniel Scherr</i>	14
Inside the "Boot Camp" for Emergency Managers <i>By Michael Valiente</i>	20
Incident Management – The Whataburger Way <i>By Ron Derrick</i>	24
Three Keys to Life-Saving Hurricane Season Communication <i>By Brian Toolan</i>	29
AI Partners – Filling Law Enforcement Experience Gaps <i>By Jeff Henderson</i>	33
Family Terror Networks 2.0: January 6 <i>By Dean C. Alexander and Huseyin Cinoglu</i>	38

Pictured on the Cover: ©iStock/Sergei Krestinin

Maintaining Planning Strategies for Evolving Threats

By Catherine L. Feinman



Agencies and organizations have different strategies when it comes to planning for emergencies and disasters. However, research and evaluation help emergency preparedness professionals stay current on emerging threats, new technologies, and resource and training gaps. The authors in this July edition of the *Domestic Preparedness Journal* share important research and lessons learned to assist in the planning process for any organization.

Planning for a natural threat like a [hurricane](#) relies on lessons learned from past incidents and can take years to fine-tune the crisis response and communication plans to address the numerous factors involved. This type of threat may not be preventable, but the consequences could be mitigated. Other human-caused threats, like [family terror networks](#), require additional research to identify patterns and key indicators. Planning for these types of incidents includes prevention measures as well as mitigation strategies.

To help plan for and respond to potential risks, threats, and hazards, various technologies exist or are being developed to help build awareness and keep communities safe. These include a range of mobile devices and applications – from those that detect and track threats like hurricanes to [artificial intelligence](#) that can be used by first responders in the field.

Regardless of the type of incident, emergency planners need to consider the whole community and ensure that vulnerable populations like [long-term care facilities](#) are included in the planning process. While each community stakeholder should have an [incident management plan](#), these plans are most effective when they include collaboration with other stakeholders to enhance mutual aid efforts and resource allocation during an incident.

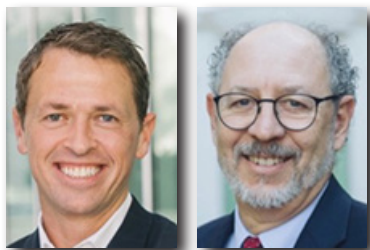
Once a plan is created, it then needs to be exercised to ensure that team members are [trained](#) to perform their roles and responsibilities at the most critical moments. However, preparing the team is also an ongoing process. Being able to [evaluate the exercises](#) and their effectiveness in preparing participants provides essential insight to be able to update the plans accordingly.

The highest priority threat last year may not be the same this year. Ensure that, through research and lessons learned, plans are regularly revisited and evolve with the community's needs.

Catherine L. Feinman, M.A., joined Domestic Preparedness in January 2010. She has more than 30 years of publishing experience and currently serves as Editor of the Domestic Preparedness Journal, www.DomesticPreparedness.com, and the DPJ Weekly Brief, and works with writers and other contributors to build and create new content that is relevant to the emergency preparedness, response, and recovery communities. She received a bachelor's degree in international business from University of Maryland, College Park, and a master's degree in emergency and disaster management from American Military University.

Creating a New Standard for Evaluating Tabletop Exercises

By John Duda and Scott J. Glick



Exercises play a vital role in preparing organizations to respond to critical incidents and have been used by the U.S. government for decades to enhance department and agency understanding of their respective [roles and responsibilities](#) and to help prepare for terrorist threats. Although organizations can develop plans, expand their resources, and add personnel with expertise in responding to different threats and hazards, the planning process cannot move beyond the theoretical if exercises do not validate plans. Having the right equipment and personnel to respond to a critical incident may provide insight into what an organization's response capabilities can accomplish. Still, unless those capabilities are tested in exercises as part of a comprehensive and integrated preparedness program, the organization cannot answer the fundamental question that its leadership needs to know: [Can the organization effectively respond](#) when a threat or hazard arises?

Currently Used Exercise Tools

During operations-based exercises, participants execute functions in a simulated environment to recreate what would happen if the scenario were real. Operations-based exercises, which include drills and full-scale exercises, are easily evaluated with quantitative assessment tools (e.g., whether participants set up a command post, initiate communications, or employ personnel and resources within a specific time). However, rather than demonstrating capabilities, participants in discussion-based exercises such as tabletop exercises (TTX) talk through a response policy, plan, or procedure and discuss what they would be doing. As a result, TTXs do not readily lend themselves to quantitative assessments, nor is there an industry standard for evaluating their effectiveness.

The Federal Emergency Management Agency (FEMA), through its Homeland Security Exercise and Evaluation Program ([HSEEP](#)), has taken essential steps to improve the evaluation of exercises. Beginning nearly a decade ago, FEMA published a sample [Participant Feedback Form – HSEEP-C09](#), which organizations can adapt. In this sample form, FEMA recommended that organizations solicit opinions from exercise participants on eight statements using a [Likert scale](#), including whether participants observed *strengths* during the exercise or areas that needed *improvement*. These statements, however, only solicited general assessments about preparedness, and the feedback was not directly tied to exercise objectives. In January 2020, FEMA updated the [HSEEP guide](#), but has not updated the Participant Feedback Form. Therefore, the current HSEEP exercise evaluation methodology may not solicit sufficient data to assist organizations in accurately measuring a TTX's overall effectiveness in improving organizational preparedness.

Designing and Evaluating Tabletop Exercises

TTXs provide a forum for participants to discuss policies, procedures, or plans that relate to how the organization will respond to a critical incident. During TTXs, facilitators or moderators lead the discussion to keep participants moving toward meeting the exercise objectives. The exercises must have [realistic](#) scenarios to accurately [assess response capabilities](#). They should be well-designed, take into account [how adults learn best](#), and engage participants in ways that build better *muscle memory* and avoid negative training; that is, training that reinforces responses that are not aligned with an organization's policies and procedures, and obstruct or otherwise interfere with future learning. Post-incident analyses repeatedly demonstrate that [experience gained](#) during exercises is one of the best ways “to prepare teams to respond effectively to an emergency.”

After the exercise, it is important to find the best way to evaluate whether the TTX has increased the participants' short-term and long-term knowledge or behaviors and to determine whether the exercise improved organizational preparedness. Researchers and academic scholars have examined different evaluation methodologies. For example, in 2017, nine researchers conducted an extensive study of whether a TTX enhanced the [pediatric emergency preparedness](#) of 26 pediatricians and public health practitioners from four states. After analyzing the data, the researchers published their study in 2019 and concluded that TTXs “increased emergency preparedness knowledge and confidence.”



John Duda facilitating a multi-country exercise in Budapest, Hungary, sponsored by the Departments of State and Energy (Source: Sandia National Labs, April 10, 2018).

Using the wrong evaluation methodology, organizations may not be able to accurately determine whether they are getting a high return on their training investments. However, since a TTX can be conducted cost-effectively in a short time, the method used to evaluate their effectiveness must also be capable of being completed relatively quickly and cost-effectively.

Quantitative Assessments

The driving principle behind [exercise evaluation](#) should be “to determine whether exercise objectives were met and to identify opportunities for program improvement.” The HSEEP’s Participant Feedback Form’s quantitative measurements are limited and primarily focused on exercise *delivery* and asking participants to provide *general and conclusory* statements about whether the exercise improved their preparedness (see Fig. 1).

Please rate, on a scale of 1 to 5, your overall assessment of the exercise relative to the statements provided, with 1 indicating strong disagreement and 5 indicating strong agreement.

Assessment Factor	Strongly Disagree			Strongly Agree	
Pre-exercise briefings were informative and provided the necessary information for my role in the exercise.	1	2	3	4	5
The exercise scenario was plausible and realistic.	1	2	3	4	5
Exercise participants included the right people in terms of level and mix of disciplines.	1	2	3	4	5
Participants were actively involved in the exercise.	1	2	3	4	5
Exercise participation was appropriate for someone in my field with my level of experience/training.	1	2	3	4	5
The exercise increased my understanding about and familiarity with the capabilities and resources of other participating organizations.	1	2	3	4	5
The exercise provided the opportunity to address significant decisions in support of critical mission areas.	1	2	3	4	5
After this exercise, I am better prepared to deal with the capabilities and hazards addressed.	1	2	3	4	5

Fig. 1. HSEEP Participant Form Questions (Source: HSEEP-C09, Participant Feedback Form Template).

The numerical scores that can be aggregated in the HSEEP statements have utility, but will not produce sufficient quantitative data because the questions are limited, are not tied explicitly to exercise objectives, and do not assign different weight values to the answers. Using objective-based and goal-based criteria can help distinguish between evaluative statements focused on exercise delivery and those focused on whether the TTX met a particular objective. Assigning a weighted numerical value for each response is also critical. For example, responses focused on exercise design and delivery should not be weighted as heavily as those focused on how well the TTX met a particular objective and improved the organization’s preparedness. In addition, when scores are averaged and compared over time, they produce a more accurate evaluation of whether the TTX improved the organization’s preparedness.


The following types of statements can be adapted by organizations to their specific TTX. Scoring these exercise factors and assigning them a weighted value creates what the authors call an XF Score.

Please rate, on a scale of 1 to 5, your response to the following statements, with 1 indicating that you strongly disagree, a 2 indicating that you disagree, a 3 indicating that you are undecided or neutral, a 4 indicating that you agree, and a 5 indicating that you strongly agree.

- The TTX improved my understanding of my organization's critical incident response capabilities [to the specific scenario being tested] (multiply this response by 2);
- The TTX improved my understanding of other organization's response capabilities, plans, policies, and procedures and how they integrate with my organization's critical incident response plans, policies, and procedures (multiply this response by 2);
- TTX objective 1 was to ... [repeat for each objective] was aligned with assessing my organization's preparedness to respond to this type of critical incident (multiply this response by 3). (This should be the main TTX objective.);
- TTX objective 2 was to ... [repeat for each objective] was met (multiply this response by 3);
- The TTX revealed a gap in my organization's critical incident response capabilities, plans, policies, and procedures (multiply this response by 2);
- The TTX revealed areas where my organization can improve its preparedness to respond to this or other critical incidents (multiply this response by 2);
- As a result of the TTX, I or my organization will be changing the way that I or we respond to critical incidents (multiply this response by 3). (This helps to measure behavioral change.); and
- As a result of the TTX, my organization has improved its ability to respond to this type of incident (multiply this response by 2).

Participant responses that are anonymous tend to produce more reliable quantitative data to analyze objectively. In addition, a scoring system that assigns the highest value to questions aligning with exercise objectives and goals (e.g., tasks and issues with the greatest importance to the organization's preparedness), and a scoring system that assigns the lowest value to exercise delivery, would produce more meaningful results about the exercise's effectiveness than HSEEP's Participant Feedback Form. For example, median score increases over time could be used to measure the degree to which the TTX transferred learning to participants and participants changed their behavior.

Organizations, however, must avoid exclusive reliance on quantitative assessments. For example, HSSEP's Participant Feedback Form does include qualitative information, which provides some degree of categorization for the information sought regarding core capabilities. However, that qualitative data does not appear to be tied to exercise objectives, as the Department of Homeland Security's Cybersecurity and Infrastructure Agency ([CISA](https://www.cisa.gov)) illustrates in its use of HSEEP's form (see Fig. 2).



CISA Tabletop Exercise Package (CTEP)
Participant Feedback Form

Part III: Participant Feedback

1. I observed the following strengths during this exercise (please select the corresponding capability and applicable element related to the strength):

Strengths	Core Capability	Element
	[list core capabilities for this exercise]	Planning <input type="checkbox"/> Organization <input type="checkbox"/> Equipment <input type="checkbox"/> Training <input type="checkbox"/> Exercise <input type="checkbox"/>
	[list core capabilities for this exercise]	Planning <input type="checkbox"/> Organization <input type="checkbox"/> Equipment <input type="checkbox"/> Training <input type="checkbox"/> Exercise <input type="checkbox"/>
	[list core capabilities for this exercise]	Planning <input type="checkbox"/> Organization <input type="checkbox"/> Equipment <input type="checkbox"/> Training <input type="checkbox"/> Exercise <input type="checkbox"/>

Fig. 2. CISA Participant Feedback Form.

Integrating Quantitative Scores With Qualitative Assessments

Organizations must also collect qualitative data to evaluate their TTX's effectiveness. Consider, for example, using the Likert scale to assess customer satisfaction for a restaurant. In the same way that a low score would not, by itself, reveal *why* the customer was dissatisfied (e.g., poor food quality or poor service), exclusive reliance on the numeric values of the quantitative score would not provide an organization with the insight needed to understand *why* the TTXs may or may not have improved its preparedness. By directly linking and integrating the quantitative data with the qualitative data, evaluators obtain more accurate and comprehensive [insight](#) regarding effectiveness.

Qualitative assessments must focus on exercise objectives during the “[hot wash](#)” and subsequent participant feedback. While facilitators can ask “open-ended” questions during the hot wash, exercise participants should focus their immediate comments on their organization’s preparedness. Hot wash participants providing comments on organizational preparedness – strengths and areas for improvement – rather than on the exercise’s execution or logistics in written post-exercise questionnaires, enables the immediate discussion to focus on more important preparedness questions.

Effective exercise evaluation requires careful planning from the beginning of the exercise design phase and when observing and collecting data, including comparing exercise objectives to how participants performed during the exercise. For example, asking questions such as “How was exercise objective #1 accomplished?” will provide important data regarding improving the response and organizational preparedness for the exercise. To further the qualitative data collection process, evaluators should ask the following key questions:

- Were the participants exercised on the specific plan, policy, and procedure the organization intended to assess?
- Did the participants understand the specific plan, policy, and procedure discussed during the exercise?
- Did the participants understand how to execute the plan, policy, and procedure?
- Did the participants follow their organization’s plans, policies, and procedures, or were gaps identified (e.g., actions not stated in plans), indicating the need to reassess a particular plan, policy, or procedure?
- What were the consequences of the decisions made?

Responses to the above questions should help exercise evaluators reach several important conclusions about the TTX’s effectiveness. For example, suppose participants did not demonstrate an understanding of a policy, plan, or procedure during the TTX. In that case, evaluators may need to conduct a root-cause analysis to better understand why that happened. Using qualitative assessments as part of a root-cause analysis can provide key data for an [after-action report and improvement plan](#). When compiling this information, however, evaluators must consider the direct relationship among several factors that can affect the evaluators’ conclusions about the data they collected, including:

- Whether there were well-considered and developed exercise goals and objectives;
- The quality of the data collected;

- Whether there were experienced and skilled exercise facilitators;
- Whether appropriate exercise participants were present; and
- Whether exercise participants were assured that the TTX was “no-fault” and “non-attributional” after-action report and improvement plan data collection would occur.

When participants receive “no-fault” and “non-attributional” assurances about the answers they will be providing to the TTX evaluation questions, better qualitative data will be collected because participants will have less reluctance to admit a lack of understanding, a shortfall in a policy, plan, or procedure, or the fact that the appropriate individuals and agencies did not participate. The collected data can then enable evaluators to reach conclusions about whether the TTX contributed to the following:

- Team building, agency coordination, and enhancing familiarity among response assets and leadership;
- Participants’ increased knowledge of their roles and responsibilities and how they would be applied during a particular scenario;
- Participants’ increased knowledge of others’ roles and responsibilities;
- Participants’ increased identification of any gaps in policies, plans, or procedures; and
- Participants’ increasing knowledge of potential threats, vulnerabilities, or consequences, if those subjects were covered during the exercise.

The collected qualitative information plays a significant role in evaluating organizational change and whether TTXs have improved the organization’s preparedness. However, separate briefings with exercise evaluators, controllers, and facilitators would produce the most complete and accurate assessment.

Testing Future Preparedness Efforts

Testing response capabilities in exercises prepares personnel and organizations for all types of threats, hazards, and incidents, and ensures that [plans are current and effective](#). TTXs are a cost-effective way for the government, private companies, and non-government organizations to test their preparedness. Following a [checklist](#) to create a well-designed TTX will maximize an organization’s chances for a successful TTX. When a TTX is well-designed, engages participants, and is conducted effectively, participants’ written responses to post-exercise questionnaires can provide important indicators of whether the TTX improved organizational preparedness. Yet, no industry standard exists for evaluating this effectiveness over time.

Tabletop exercises are vital in preparing organizations to respond to critical incidents, but an industry standard is needed to evaluate their effectiveness.

There is a need for a new industry standard for a reliable, objective, and cost-effective way to evaluate TTX effectiveness. The new standard should be based on quantitative and qualitative data that is tied to exercise objectives and that assigns weighted values to the most important exercise factors to better understand the TTX's impact on organizational preparedness. However, care must be taken regarding the scoring statements, exercise design, and delivery. Moreover, conducting TTXs alone is not enough to ensure organizational preparedness. When a comprehensive and integrated preparedness program has senior leaders' support and the exercises are appropriately resourced, organizations can maximize the return on investment in their training investments and pursue multi-year exercise plans and priorities through effective program management.

Author note: Since 2012, one of the authors of this article has noted the [lack of an industry standard](#) for quantitative assessments of TTXs, which prompted him to develop a rubric that included various factors for analyzing and measuring exercise effectiveness. Based on their extensive exercise experience in both the government and the private sector, the authors of this article have further refined the rubric into what we call the XF Score™. Building on and improving the eight questions included in the sample HSEEP Participant Feedback Form, the XF Score, along with integrated qualitative assessments, provides a practical, easy-to-use, and cost-effective method for organizations to evaluate the effectiveness of TTXs objectively and reliably. This approach could lead to a new industry standard that helps organizations maximize their return on investment and use their limited exercise budgets wisely to enhance organizational preparedness.

The views expressed in this article are solely those of the authors and do not necessarily represent the views of any government department or agency or private sector organization. This article contains no classified, confidential, or otherwise sensitive government information. The authors wish to thank Holly Hardin, Christine Moore, Jessica Mielec, and Chris Norris for their prior review and comments, and Mart Stewart-Smith for his review, comments, and contributions, to an earlier draft of the article. Mr. Duda and Mr. Glick can be reached [here](#).

John R. Duda is the chief executive officer of [Summit Exercises and Training LLC](#) (SummitET®), a veteran-owned small business that specializes in providing proven full spectrum preparedness solutions to systematically address all threats and hazards through a wide-range of services. Mr. Duda has led and supported multiple domestic and international exercise and training programs for numerous government and non-government organizations. Mr. Duda has also co-authored a research study involving defense-based sensor technology and has been certified as a senior professional in Human Resources and as a Business Continuity Professional. Prior to forming SummitET, Mr. Duda served many organizations including the U.S. Department of Energy/[National Nuclear Security Administration](#), Publix Super Markets, and the Jacksonville Port Authority. Mr. Duda is also a member of the Advisory Board for the University of North Florida's School for International Business and the cybersecurity and compliance company, RISCPoint.

Scott J. Glick, SummitET's General Counsel, has more than four decades of experience in law enforcement, counterterrorism, critical incident response, and emergency preparedness, as well as extensive exercise experience with federal government departments and agencies, including in the design and facilitation of tabletop exercises. Mr. Glick previously served as the Director of Preparedness and Response and Senior Counsel in the National Security at the U.S. Department of Justice (DOJ), where he led DOJ's national preparedness policy and planning efforts and represented DOJ during senior official exercises. He has investigated and prosecuted international terrorism cases as a federal prosecutor, and organized crime cases as a state prosecutor in New York.



Long-Term Care Facilities in Emergency Preparedness Planning

By Tanya Scherr & Daniel Scherr



An important part of community emergency preparedness planning includes long-term care facilities such as nursing homes, dialysis, home care centers, or hospice facilities. Older adults and those with disabilities have increased vulnerability during emergencies. This population may have more [limitations](#), require additional support, and may experience health emergencies sooner than others when faced with limited food, drink, rest, or access to electricity.

Concerns include the need for large-scale transportation for patients, which may require continuous care during transport, along with the ability to be moved in a nontraditional manner (i.e., patients may not be able to sit up). Complications may include: (1) the need to reach and communicate with individuals that can make decisions for any impaired patient population, (2) the need for electricity for durable medical equipment to keep patients healthy, and (3) temperature requirements for necessary medications. Based on the type of care these facilities provide, preparing for emergencies is simply not as high a priority as others they face daily.

During impending emergencies, when there is time to plan (e.g., hurricanes), each facility decides to evacuate its residents or shelter in place. Whichever action it chooses, each decision comes with unique challenges due to the complex care that most residents require. Sheltering in place means that providers need training and skills to manage the post-event complications that can occur. Evacuation requires strong planning and community coordination to ensure the safety of the residents before, during, and after transport.

In 2016, the Centers for Medicare & Medicaid Services (CMS) published the “[Emergency Preparedness Requirements](#) for Medicare and Medicaid Participating Providers and Suppliers.” The rule impacted [17](#) different types of providers and suppliers.

However, in 2017, the U.S. Senate Committee on Finance published a [report](#) showing critical safety failures on behalf of nursing homes in Texas and Florida during and after Hurricanes Harvey and Irma. The report also notes that one county medical examiner ruled the deaths of 12 seniors in Florida as homicide, as they died due to heat-related complications when plans were not in place to accommodate the loss of their air conditioner for several days. The report additionally discusses the flooding in Texas due to Hurricane Harvey and the struggles at two nursing homes. One nursing home was evacuated only after pictures of the residents in [waist-deep water](#) circulated on social media. Another nursing home was evacuated only when someone held the director at [gunpoint](#). The director was later arrested when he refused to assist with the evacuation.

In 2020, CMS released updated [guidance](#) to the 2016 rule, which included revisions due to the recent COVID-19 pandemic. The rule has requirements for both human-caused and natural disasters. Each provider requires four elements of emergency preparedness:

- Risk assessment and emergency planning,
- Policies and procedures,
- Communication plan, and
- Training and testing.

In 2021, CMS again released [additional guidance](#) to the 2016 rule, reducing the frequency of some emergency preparedness activity requirements and revising timelines for certain providers and suppliers. Emergency programs were decreased to a biennial review (from annually) for certain facilities, but this does not apply to long-term care facilities. While the training requirement decreased from yearly to every two years for certain providers, nursing homes are still required to keep the annual training.

In February 2022 – in response to the COVID-19 pandemic, [climate change](#), and specific instances where long-term care struggled to manage an emergency – the White House released its [reform fact sheet](#), which notes protecting seniors through strengthening emergency preparedness initiatives. Increasing emergency preparedness efforts in long-term care facilities can help minimize injury, illness, and preventable deaths.

Risk Assessment and Emergency Planning

Taken directly from its website, CMS requires that all risk assessment and emergency planning for long-term care facilities include the following [elements](#):

- Hazards likely in a geographic area;
- Care-related emergencies;
- Equipment and power failures;
- Interruption in communications, including cyberattacks;
- Loss of all or a portion of a facility;
- Loss of all or a portion of supplies; and
- The plan should be reviewed and updated at least annually.

Plans should follow the industry standard of using the all-hazards approach, including building plans to address a broad spectrum of emergency events or disasters. Consideration should be given to natural and human-caused emergencies, including hurricanes, tornadoes, earthquakes, cyberattacks, loss of essential supplies such as food and water, equipment/power failures, and loss of portions of the facility.

The National Association for Home Care & Hospice (NAHC) published an [emergency preparedness packet](#) in 2008 for home health agencies. This document provides a detailed analysis for facilities to identify areas that need to be addressed within their emergency plans. This packet has a template that facilities can use for their assessment, beginning with identifying the probability of specific emergencies such as ice, flooding, terrorist

attacks, and electrical failures. For a higher-level overview, facilities can also use a [Hazard Vulnerability Analysis](#) (HVA) tool, such as the one created by Kaiser Permanente, to assess areas of risk that need to be considered in emergency planning. This tool helps each facility identify considerations, including probability, human impact, property impact, business impact, preparedness, internal response, and external response. Due to the age of the NAHC document (and the lack of an updated one on its website), it is important for facilities to think about cyberattacks and whether or not they are prepared. While not specifically noted in the packet, this scenario could be considered under vulnerability in terms of the terrorism section of the HVA.

The Federal Emergency Management Agency (FEMA) also provides a [Comprehensive Preparedness Guide](#), which reminds facilities of the need to engage the entire community in planning so that decisions reflect the actual community population. Risks should

Critical safety failures on behalf of nursing homes during and after Hurricanes Harvey and Irma exposed planning gaps for long-term care facilities.

be analyzed using the question, “What could go wrong?” when building contingencies. Supplies and resources should be noted, along with any gaps that must be addressed before an emergency. The Centers for Disease Control (CDC) published a [COVID-19 preparedness checklist](#) for nursing homes and other long-term care facilities. This checklist includes several areas, including staffing

contingency plans, communication protocols for interfacility transfers, and post-mortem care. CMS also published a [State Operations Manual](#) that provides emergency preparedness information for several types of providers and suppliers.

Building and Communicating a Strong Plan, Policies, and Procedures

Each facility needs to have a dedicated owner of the emergency plan. While this position is not dictated by federal law, it is a necessary step in setting up each facility for success in minimizing loss of life and property during an event. Evacuation plans should be posted on all floors in a prominent location to assist employees and residents with learning exit routes in an emergency. A minimum of quarterly communication should occur to help keep the plan’s location and the exit routes fresh in each person’s mind.

To prepare the residents, the Department of Health & Human Services & CMS published the [Emergency Planning Checklist](#) for long-term care residents, their families, friends, guardians, and caregivers. Understanding this, each long-term care facility should ensure that this information is regularly communicated without the residents or their families having to specifically request it. When all involved parties are informed and aware, it builds a stronger coalition of resources and helps to ensure a smoother approach to emergency preparedness.

Each state website provides a wealth of resources for long-term facilities to build policies, procedures, and plans for emergency preparedness. Facility administration should familiarize themselves with all available resources. Reviewing neighboring state websites can also provide additional resources and considerations that may not be included in current planning. The following state websites have guidance that is similar from state to state.

Missouri lists specific requirements for emergency plans in [19 CSR 30-85.022\(33\)](#), giving the following structure:

- A phased response ranging from relocation within the facility to complete evacuation;
- Written instructions for evacuation of each floor, including:
 - Evacuation to areas of refuge, and
 - Floor plans showing the location of exits, fire alarm pull stations, fire extinguishers, and any areas of refuge;
- Evacuating residents from an internal area of refuge to outside the building;
- Location of additional water sources on the property;
- Procedures for the safety/comfort of residents during and after evacuation;
- Staffing;
- Staff instructions for initiating emergency services resources;
- Staff instructions for contacting alternative housing for residents;
- Responsibilities for administrative staff; and
- Understanding of who is responsible for accounting for all residents' locations.

[Colorado](#) includes additional information within their website, like Missouri but notes additional information such as:

- Accounting for food, water, supplies, and medications for staff and residents for both evacuating or sheltering in space;
- Determining alternate sources of energy to ensure continuity of necessities such as temperatures, lighting, sewage and waste disposal, and fire detection and extinguishment;
- Systems to track the physical location of staff and residents;
- Establishing a primary and secondary way of communication outside the facility; and
- Medical documentation plans that continue to secure resident information in compliance with HIPAA.

Several state websites also include resources specific to the probable events within their geographical location, such as hurricanes, tornadoes, earthquakes, and flooding. In recent years planning should also incorporate cyberattacks, as they are a [growing and persistent threat](#) to long-term facilities specifically and healthcare organizations overall. Dozens of long-term care facilities have been targeted by these attacks, with a [\\$14-million dollar ransomware](#) attack in 2019 serving as a case study. That attack impacted over 100 facilities and led to a halt in a number of critical business functions. Many long-term care facilities leave this scenario out of emergency planning due to either lack of resources and/or expertise in this area, which can result in critical loss to the facility and its residents.

Understanding the unique risks of each facility is critical for building a strong and reasonable plan. For example, if residents require communication with designated decision-makers for care, provisions should be implemented for emergencies if a decision-maker cannot be reached or it is not reasonably feasible to attempt to contact the person during the emergency event. Considerations also need to be made to address the fact that most long-term care facilities do not have a staff member specifically for cybersecurity or emergency management tasks. These duties generally fall to the administrator or their representative, placing them in a position to decide where to allocate resources: managing cases and today's patient needs or planning for future events.

Training and Testing

Training and testing must comply with both federal and state laws and need to occur annually. Long-term care facilities are included in the [National Preparedness Goal](#), which stresses whole community readiness for emergency events. The Homeland Security Exercise and Evaluation Program provides [guidance](#) for programs, including emergency preparedness exercises. They recommend establishing Training and Exercise Planning Workshops to engage elected and appointed officials in the emergency planning process to set appropriate priorities for each community.

The American Health Care Association created the [Nursing Home Incident Command System](#) (NCHICS) Guidebook, which can serve as a training and educational tool to better understand the organization and incident command process as it applies to each long-term care facility. The following criteria must be met for the exercise to be considered a formal drill:

- An overview of the scenario has been documented and communicated;
- The emergency preparedness plan has been activated;
- Evaluation has occurred for all areas/departments and participants;
- An after-action review/critique occurs; and
- Follow-up items/training/areas of improvement are identified, and documents and corrections are planned to close the gap.

Considerations for weather and time of year should occur when conducting trainings. Training should not be set during impending weather issues such as excessive heat, excessive cold, or the likelihood of storms. Long-term care facilities should engage community resources during exercises and drills to ensure smooth operations and continuity of care during an emergency.

Emergency Response to Long-Term Care Facilities

There are several things that first responders and emergency preparedness professionals can do to help the facilities within each community plan and prepare for emergencies. Suggestions include:

- Inviting and actively including facility leadership in community preparedness meetings;
- Collaborating with facilities on training and testing days;
- Offering to attend after-action reviews at the facility;
- Offering to review plans and assess areas of weakness;
- Asking for a tour of the facility to help identify areas of opportunity and to familiarize responders with the overall layout;
- Ensuring up-to-date plans are on file for each location with the local emergency management director; and
- Having local fire departments provide annual assistance to review fire and evacuation plans.

A review of all state websites produced a wealth of resources, including a checklist from [Arizona](#) that assists with surveying long-term care facilities. The document mentions that it is not comprehensive in developing the actual emergency plan but should be used more for researching long-term care facilities and ensuring they have adequate documentation to support emergency events.

When responding to long-term care facilities during emergencies, consideration should be given to the unique challenges that the facilities face. Having a dedicated person to own the emergency plan, as well as having a plan in place to assist with multiple limited mobility patients and understanding the increased need to monitor older people for temperature-related events, is necessary.

CMS's Quality, Safety, and Oversight group also publishes a [Special Focus Facility](#) list, summarizing facilities with a previous history of serious quality issues. If one of these facilities is within the local community, it is important to understand the deficiencies noted and be ready to accommodate the additional issues within that population in an emergency. It is strongly suggested that these entities are actively included in community emergency preparedness coalitions and training. Engaging high-risk populations empowers local communities to build strong emergency preparedness and response capabilities while minimizing the risk of preventable injuries, illnesses, and death.

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

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

Inside the “Boot Camp” for Emergency Managers

By Michael Valiente



Monday, August 1, 2022, was a typical San Antonio, Texas, summer day, with clouds hanging low and humidity increasing as the sun rose. But nothing was ordinary to the 20 individuals who would become cadets in the first [Emergency Management Academy](#) developed by the Texas Division of Emergency Management (TDEM). Looking around, the cadets appeared apprehensive but excited that they had been selected to become the future of emergency management in the Lone Star State. TDEM Chief Nim Kidd spoke to the class and shared his expectations of The Academy. He indicated that the cadet demographics were intentionally diverse: military veterans, college graduates, recent high school graduates, and practitioners from fire, emergency medical services (EMS), and law enforcement backgrounds. The purpose was to garner different perspectives inherent to the cooperative and collaborative nature of the emergency management field.

Emergency Medical Technician – Basic

After onboarding into The Texas A&M University System, the cadets moved to a different location from its roots in the [Texas A&M–San Antonio](#) campus to the Schertz EMS Academy in Guadalupe County. There, the cadets underwent a rigorous, condensed eight-week training (from the standard 16-week course) in emergency medical response, undergoing testing in academics and skills. Also, the practical application portion of the training was supplemented by clinical familiarity through ambulance duty on weekends, in which the cadets had to complete 40 hours of assisting ambulance crews. The final test was the [National Registry](#) exam, in which the nationally recognized EMS certification was awarded. The emergency medical response certification would enhance the cadet’s ability to augment EMS in their jurisdictions after graduating from the Academy.

Preparedness – Planning During “Blue Sky” Days

The cadets went back to the Texas A&M–San Antonio campus for the duration of The Academy. Before diving into the Preparedness training module, the cadets received a week-long series of classes on leadership development, team building, and stress management. Then, they took courses on the Foundations of Emergency Management, Science of Disasters, Emergency Planning, Homeland Security Exercise and Evaluation Program, Threat and Hazard Identification and Risk Assessment, and Continuity of Operations. The cadets also became intimate with the federal laws governing emergency management, specifically the [Stafford Act](#) and the [Texas Government Code Chapter 418](#), the state’s statutory authority on disaster management. Additionally, the cadets were introduced to [the State of Texas Emergency Assistance Registry](#), a program administered locally for citizens with access and functional needs, and the [Emergency Tracking Network](#), where they learned to track evacuees and pets.

Hazard Mitigation Training – State and Federal Perspectives

The complexity of hazard mitigation was navigating through the idiosyncrasies of the various federal hazard mitigation programs and the processes from applying for the grant programs at the local level to the programmatic closeout between TDEM and the Federal Emergency Management Agency ([FEMA](#)). The instructors hailed from TDEM, giving the cadets the state-level perspectives, and FEMA Region 6, headquartered in Denton, Texas, providing the federal-level views. Also, the cadets observed that other state agencies, such as the [General Land Office](#) and the [Texas Water Development Board](#), were instrumental in providing additional funding assistance for hazard mitigation. The classes familiarized the cadets with the various funding assistance programs and their applications, conducting benefit-cost analyses, and grant application reviews and evaluations.

Response – “How Big Is Big? How Bad Is Bad?”

The cadets welcomed the New Year in 2023 with two weeks of the Incident Command System (ICS) for Expanding Incidents (G-300 and G-400), followed by Public Information Basics, in which TDEM’s own Media and Communications team interviewed the cadets who subsequently conducted press conferences fielding questions from the “press.” The cadets were then introduced to various Geographic Information System platforms such as Survey 123, Individual (Assistance) State of Texas Assessment Tool ([iSTAT](#)), Public (Assistance) State of Texas Assessment Tool ([pSTAT](#)), State of Texas Assistance Request ([STAR](#)), and [WebEOC](#), the resource request tracking tool from local jurisdictions to the Texas State Operations Center (SOC). The data collected from the iSTAT and pSTAT digital surveys give an overview of the initial damage assessment for the Disaster Summary Outline ([DSO](#)). The DSO is transmitted to the SOC to assist in evaluating the extent of the damage within a jurisdiction.

“Every Day Is Recovery Day” Training

The recovery training module started with grant management for both Individual Assistance and Public Assistance programs. Emergency declarations and disaster declarations were also covered, starting with requests from the local level up to the president’s approval. Further, there was an emphasis on the importance of a debris management plan, as well as the roles of community leaders in disaster declarations, sheltering and feeding operations, engaging [Volunteer Organizations Active in Disasters](#) and [Community Organizations Active in Disasters](#), establishing a [Long-Term Recovery Group](#), and choosing a fiduciary agent (a third-party entity to assist in processing monetary donations during disasters). An added feature was education in Disaster Finance, taught by a team from TDEM that manages and allocates federal and state funds to individual jurisdictions.

The cadet demographics were intentionally diverse to garner different perspectives inherent to the cooperative and collaborative nature of emergency management.



The inaugural cadet class of the Texas Emergency Management Academy stands with Texas Emergency Management Chief Nim Kidd and Academy leadership during a graduation ceremony in the Texas Capitol Auditorium (Source: Texas Division of Emergency Management/Marcus Clark, March 24, 2023).

Off-Site Training

Although most of the training took place on the Texas A&M–San Antonio campus, the cadets had the opportunity to train off-site. The first field experience was on Sunday, November 20, 2022, attending the Texas EMS Conference in Austin, Texas, where they were introduced to the various [Emergency Medical Task Force \(EMTF\)](#) teams throughout the state and the different types of assets, including mobile medical units. They also explored various technological advances in emergency response by talking to the vendors in the exhibit hall. A great event was experienced by all when the Emergency Operations Center (EOC) Operations and Planning class met in the Bexar County/City of San Antonio EOC to conduct scenario-based training in an actual EOC. Instructors from the Texas A&M Engineering Extension Service ([TEEX](#)) guided the cadets in operating an EOC by filling the roles in an ICS framework. The cadets also had the opportunity to tour the SOC in Austin, where they were introduced to the various emergency support functions (ESFs) and how the SOC would operate during activations. Moreover, during the recovery

training phase, the cadets visited the San Antonio Food Bank to acclimate to its mission, capabilities, and valuable role in disaster resource assistance.

Job Fair – “The Academy Mixer”

To fully understand the uniqueness of each region and functional area within TDEM, and before applying for employment, cadets participated in a job fair organized by the TDEM Administration Division and the Human Resources team. To prepare for the job fair, cadets took classes on resume building, cover letter drafting, and job interview techniques.

Capstone – The Final Phase of the Emergency Management “[Boot Camp](#)”

The Academy Capstone took place over three days in late March at [Disaster City](#) in College Station. Hosted by TEEEX, the multi-day exercise consisted of filling the roles of the ICS functions within the EOC. The simulation was divided into multiple operational periods wherein cadets switched roles. This “final project” enhanced the exercise’s realism and gave the cadets confidence in performing the essential tasks during disaster operations.

Reflections

The challenging yet fulfilling experience culminated at 4 p.m. on Friday, March 24, 2023, when 17 cadets walked across the stage to receive their diplomas, FEMA certificates, and badges – part of their reward for completing the 8-month “basic training” in emergency management. The keynote speaker was Governor Greg Abbott. Texas A&M University System Chancellor John Sharp, Texas Emergency Management Chief Nim Kidd, FEMA Region 6 Administrator Tony Robinson, and TDEM Academy Division Chief David Covington also delivered remarks. This academy cohort was unique for two reasons: This was a new and unique emergency management academy and this was the first cadet class to go through the training – an opportunity of a lifetime! Familiarization with the four phases of emergency management, receiving FEMA and EMS certifications, networking opportunities, and, most of all, performing the skills requirements of the emergency management field was a tremendous experience! The 17 cadets that completed the training became family, dedicated and eager to respond to assist the citizens of Texas as the next generation of emergency managers.

The author would like to especially thank TDEM Division Chief David Covington, Unit Chief Kade Long, and Unit Chief Angela Shook for their leadership and academic acumen in sustaining The Academy.

Michael Valiente currently serves as the Senior Training Officer – Preparedness Division at the Texas Division of Emergency Management. He is a retired U.S. Marine with 23 years of active-duty service. His initial emergency management experience came from participating in Operational Unified Assistance, the U.S. military humanitarian relief efforts during the December 2004 tsunami in Southeast Asia. After retiring in 2005, he taught at the University of Phoenix and Alamo Colleges in San Antonio, Texas. He has a master’s degree in international relations from Troy University and a Doctor of Emergency Management degree from Capella University.

Incident Management – The Whataburger Way

By Ron Derrick



A community's level of resilience during a disaster often relies on the preparedness efforts of its private sector partners. Companies that invest in preparing for and responding to large-scale events are protecting much more than just company profits. For example, the thought and design that went into one hamburger restaurant led to a companywide culture of safety and community service.

Whataburger was born from one man's dream in 1950 when Harmon Dobson opened a small building selling burgers for just 25 cents in Corpus Christi, Texas. His idea was for someone to hold up the burger and think, "Wow, What-A-Burger." The name has stuck, and the company has gone from one little shack to over 950 restaurants across 14 states. The orange and white colors and the iconic "A-frame" building came from the founder's passion. Dobson was a pilot, and he wanted to be able to see his buildings as he flew overhead. The orange and white colors come from aviation; most airports use these colors to signify obstructions and buildings. The "A-frame" shape is also iconic, and a version of it is used in all new construction along with the flying "W." In 2001, the 77th Texas Legislature officially designated Whataburger as a "Texas Treasure."

Whataburger restaurants grew rapidly into many southern states, and most restaurants are open 24 hours. Executive leadership knew that issues and incidents would need to be handled through an elite team with emergency management and crisis response experience and expertise. In response, the company formed the Whataburger Command Center, which initially consisted of four individuals dedicated to identifying potential threats and incidents that could impact or threaten employees, customers, restaurants, or brand reputation. After COVID-19 emerged in the U.S. in March 2020 and several company re-organizations between 2020 and 2023, the team now has one senior manager and one professional running a *high-level* Command Center at the San Antonio, Texas, home office. This team uses multiple vendors and applications to help identify, analyze, and verify incoming information.

The Command Center uses a hybrid form of the Incident Command System, and its mission is to prepare for, identify, respond to, and recover from a crisis or an unexpected event that threatens the stability, reputation, or operations of the company's employees, buildings, franchisees, and support departments. It involves a wide range of activities and strategies designed to mitigate the impact of the crisis and protect the interests of the company and its stakeholders. The main goal of the Command Center is to minimize damages and ensure the company's survival and quick recovery after a planned or unplanned incident.

Prepare

The Command Center's preparedness initiative is to not only ensure each restaurant and operator is prepared to respond to a myriad of emergent incidents but also to ensure its staff and the Core team are educated on incidents around the U.S. that may or may not have an impact on the entire footprint. The Core team is comprised of key stakeholders from each support department and Operations. These individuals are empowered to represent their departments, make "on-the-spot" decisions, provide knowledge from their areas of expertise, and make or influence decisions that impact Operations and brand reputation. The team is dynamic, and not all members are used for every incident. The Command Center will determine which of the Core team members it will take to respond and recover from the incident.

The Command Center ensures that all restaurant management, field support teams, and each Core team member are prepared to deal with the myriad of incidents in the following ways:

- Operational and field teams are prepared through various platforms, including videos produced at the home office and provided to operators and field staff.
- Virtual training is offered to the regions that find it difficult and cost-prohibited to bring their entire team to one location.
- Quarterly training is available on a Teams call or provided by in-person training to restaurant teams as much as possible.
- Restaurant Operations and field support teams are kept abreast on all important information and updates through numerous daily email and text communications concerning upcoming severe weather, heat preparedness, hurricane preparedness, personal severe weather preparedness, and other issues that could impact the business or employees.
- A mass communication program is used daily, making it much easier to send multiple messages rapidly to the same group through templates.

Identify

Most threats to company restaurants across the 14-state layout come from mother nature. Torrential spring rains and tornados, severe winter storms, active tropical seasons, and other weather phenomena keep the Command Center team busy year-round. To help identify severe weather threats, the Command Center team uses two weather vendors – one for severe weather on land and one for tropical weather during hurricane season. Extreme weather impacts one or more restaurants across its 14-state enterprise every day, so getting that information out expeditiously to restaurants and field leaders is imperative.



Tulsa, Oklahoma, tornado damage (*Source: Whataburger social photo, 2018*).

Receiving severe weather reports from weather vendors through texts, emails, and vendor applications, the Command Center verifies the information before sending on to restaurants and field personnel. In the case of tornado warnings, restaurants go through a specific process, closing and securing the building for at least 30 minutes or until the threat no longer impacts the facility. If the threat is winter weather, the Command Center will send this information to restaurants as soon as possible so they can begin staff planning and product needs if roads are closed. Many lessons were learned from Winter Storm Uri in February 2021, but the most notable was to get information out early and often.

The Command Center also uses a tropical system weather vendor for threats from the Atlantic Ocean, Caribbean, and Gulf of Mexico during hurricane season. This vendor assists in identifying, analyzing, responding to, and recovering from tropical events that potentially impact coastal restaurants and employees. The tropical weather vendor provides the Command Center with daily assessments and forecasts of storms moving through the Atlantic, Caribbean, and Gulf. When it is evident a storm is going to make landfall near a Whataburger restaurant, the vendor provides the team with tropical meteorologists on all conference calls to give all engaged departments and franchisees the latest information and forecast so preparations and proper closures can take place. This information is used to make the best company and restaurant safety decisions.

Weather is not the only potential threat or activity the Command Center monitors and assesses. Other activities include power and water outages, boil water advisories, technology outages, fires, protests, demonstrations, social media, employee health, vehicle strikes, drive-thru issues, robberies, employee safety/injuries, fights, food safety, and new restaurant openings. The company is also currently opening an average of one new restaurant per week. There is an enormous amount of time taken each day identifying and assessing each of these events to see how it will impact the safety of employees and customers and potentially impact the company's brand reputation. Identifying threats across a wide area takes extraordinary threat intelligence.

The Command Center uses two threat intelligence vendors to receive clear vision and analysis of what occurs in and around restaurants, offices, learning centers, and Tier-1 suppliers. A quarter-mile circle is drawn around each of these locations. If any of these threats emerge in one of these circles, a notification is sent to the Command Center by email, text, app notification, and dashboard post. The information provided includes a brief description of the threat, the distance from the monitored location, the severity of the danger, when it occurred, and the ability to speak to an analyst to garner additional information about the incident. The team can then make decisions based on playbooks on who to engage, by what means, and how urgent this incident is to the business. It is imperative to be able to send the right information to the right people by the right means at the right time.

The Whataburger Command Center team has 24 incident playbooks, providing step-by-step plans of tasks and procedures each team performs in response to specific incidents.

Respond

Strong leadership, clear and concise communication, and the ability to adapt to rapidly changing circumstances when responding to escalated incidents is what the Command Center provides on a daily basis. This concept depends most on trust and understanding from the restaurants and field support departments. These field teams know when they receive direction from the Command Center, it is the "Voice of Truth," and they feel comfortable following the directions.

The Command Center has 24 incident playbooks, which are step-by-step plans that outline the tasks and procedures each department will perform when responding to a specific incident. The tasks and procedures are updated annually and after each incident. Along with the playbooks is a communications matrix that outlines who the team communicates with, by what means, and how often. Response teams also use lists, checklists, and logs. Most major responses, such as hurricanes, are divided into phases, and procedures performed by each team depend on which phase of the incident.

Recover

The priority once the incident has concluded is employee and customer safety. Whataburger goes to great lengths to ensure all employees have time to recover personally. Once the Command Center team knows the staff is ready, they use the recovery process to restore restaurants and the business to normal operations and hours, address



Command Center preparedness training
(Source: Whataburger, 2022).

residual restaurant or field team issues and unmet needs, and ensure all employees are recovering. The Whataburger Family Foundation addresses any employees' needs. The quicker the restaurant can recover, the sooner the company and its resources can assist the community in recovery.

Through it all, Whataburger remains committed to investing in the communities they serve. Its marketing and public relations teams will infiltrate the impacted area to assess how the company can fill voids or feed recovery teams and first responders after

a critical event and meet the community's needs. Whataburger uses its food truck and volunteers to help communities in need by raising money for the community or feeding families in their time of need.

As the final recovery process, after all employees, customers, and communities fully recover, the Command Center will facilitate an after-action review, including lessons learned, best practices, and opportunities for improvement. These ideas and concepts are used to update all playbooks and task lists each department uses when responding to an escalated incident. This learned information is sent out again months later to ensure each team has addressed all issues.

Ron Derrick serves as the senior emergency manager at the Whataburger Command Center and oversees the daily operation of the Command Center and its staff. Ron spent over 30 years in fire and emergency medical services (EMS) and has been in emergency management since 1993. He has a bachelor's degree in emergency management from Jacksonville State University. Ron spent more than 20 years in the Kerrville Fire Department and Fredericksburg Fire and EMS and another six years as the operations manager for South-Central Texas for Acadian Ambulance Service. After a long fire and EMS career, he spent five years as the regional director of safety and emergency management for the Baptist Health System in San Antonio and six years as a senior controller in the USAA Command Center before taking his current position at Whataburger over five years ago. Ron is a Certified Business Continuity Professional and a certified State of Texas Pyrotechnic Operator. He has been a speaker at numerous conferences, including the TEEX Leadership Development Symposium and the Texas Division of Emergency Management Conference.

Three Keys to Life-Saving Hurricane Season Communication

By Brian Toolan



In 2022, hurricanes and floods displaced nearly [3 million](#) people. As the frequency and severity of natural disasters continue to evolve due to climate change, how citizens, enterprises, and government organizations approach safety and resilience must change with it. More critically, this means updating public safety plans to strategically address the specific needs of different groups and areas under one's care.

However, hurricane response plans are not one-size-fits-all. How certain sections of a city or area must prepare for disaster response may differ from another (think mobile home neighborhoods vs. new home developments) and will require different foresight and resources. Also, vulnerable communities, like persons with physical disabilities, may require additional care, planning, and resource allocation.

It is often misconceived that government agencies have every resource and available piece of knowledge to deploy resources immediately [when hurricanes hit](#). As technology advances, this becomes easier, but it will never be a perfect system. Years of strategy and planning go into crisis response and developing a communication plan that keeps people safe, clearly outlines the situation, and empowers them to act. There are three key factors to a successful communications plan during hurricane season:

- Primary and secondary methods of communication,
- Understanding and acknowledging community members' needs and diversity, and
- Thoughtful and well-structured templated messages.

Having Primary and Secondary Methods of Communication

Government entities should have two forms of mass communication services to ensure notification of all citizens when there is impending danger. The primary solution should consist of a multi-modal, multi-lingual system that provides outreach to the community through the devices they request to receive alerts on and in the language they will understand. The secondary would be the Integrated Public Alert & Warning System ([IPAWS](#)), which provides emergency response agencies the capability to reach all active cellphones in an area while also delivering alerts through the emergency alert system to televisions and radios.

When developing communication best practices, government agencies must also understand the messages they are pushing out and when. Ahead of storms, messages may guide people to websites or include hyperlinks, which work well to provide complete details. As the storm approaches and makes landfall, citizens will have limited service and bandwidth. At this point, communication systems must account for downed power lines and a lack of Wi-Fi and cellular data. Recovery details should be direct and actionable, avoiding the need to click on hyperlinks or view web-posted information, often unavailable to those with limited data connectivity.

Understanding the Diversity of Needs in the Community

In addition to a strategic communications plan, government agencies must survey citizens' needs and adequately prepare to meet them once a hurricane strikes. Government agencies should clearly communicate systems where citizens should input necessary life-saving details ahead of hurricane season, including state databases, website forms, physical locations, etc. Information to input include but is not limited to:

- *Essential medications* – For example, are you reliant on oxygen, insulin, or other medications? Do these medications need to be refrigerated?
- *Evacuation aide* – For example, are you bariatric or blind? Will you need help evacuating your home?
- *Accessibility issues* – For example, do you have language barriers?

Understanding diversity in the community is also where governments must empower self-advocacy in their citizens. Officials can only know as much as their citizens are willing to disclose – the more they know, the better they can serve the public's needs. Of course,

There is a delicate balance between the efficiency of sending mass notifications and ensuring that the appropriate people receive the most relevant information.

there will always be challenges in getting citizens to willingly disclose personal information about themselves to government organizations. To work through this as best they can, government officials must *clearly* explain why they are asking for information and list potential consequences for citizens in an emergency if they do not disclose accessibility issues, such as an inability to receive live-saving resources. It is essential to have an alerting system to inform citizens of critical resources, such as where they can voluntarily register assistance needs ahead of hurricane season. They must also have information available to them year-round to put as much control of their safety in their own hands as possible, which includes:



Source: Robert D. Barnes/Moment via Getty Images.

- Regularly scheduled community preparedness events;
- The ability to register to receive safety alerts;
- Easily navigable government websites for up-to-date information;
- Understandable and clearly communicated evacuation routes; and
- [Home preparedness](#) (e.g., preparing to be in isolation for a minimum of 72 hours before assistance may be available, depending on storm severity).

Prepare Thoughtful and Well-Structured Templated Messages to Get Attention

There is a delicate balance between the efficiency of sending out mass notifications and ensuring that the appropriate areas are getting the information most relevant to them. All communication must provide precise details of the specific (or anticipated) impact on each local community with actionable next steps. When they feel that a message was meant for them specifically and will impact them directly, citizens will demonstrate [higher action rates](#). Starting a statement with, “Your residence is in evacuation zone A

and under mandatory evacuation. You must evacuate now,” is a simple, highly effective way to get citizens to comply. In addition, since vulnerable populations or those with disabilities may need more time to prepare for evacuation than others, those messages may start with, “You are receiving this message because you identified as someone needing additional assistance for evacuation.”

The timing of these messages matters as well – vulnerable areas or populations may receive communications as early as 72 hours before the anticipated landfall of a hurricane, while others may receive 24-48 hours’ notice depending on their ability to evacuate. Critical considerations for evacuations are to be initiated during daytime hours and completed before nightfall. Evacuations during darkness can lead to significant challenges for the public.

An essential piece of effective messaging is establishing government or official entities as the primary source for all evacuation and preparedness information. For example, this can mean sending a disclaimer to all citizens of the *only* places to seek out correct information from these organizations (government social media handles, government websites, etc.). Fear and panic can create misinformation. So, in addition to proactively sending out needed information, officials must be prepared to be *reactive* to narratives of misinformation spreading through social media, online forums, and local groups such as homeowner associations. These sites must be monitored and rumors addressed ahead of detrimental impact. This occurred throughout COVID where government websites developed webpages that directly spoke against misinformation. Building trust and reducing fear and panic requires that people be consistently guided to a source where the most up-to-date information is readily available.

Key Takeaways

While a hurricane’s physical impact is unavoidable, government officials have every ability to communicate with their citizens to minimize loss of life and enhance public safety. Governments must prioritize community resilience and establish strategic communication plans consisting of multiple methods of communication, an acknowledgment of community members’ diverse needs, and actionable messages. These three tactics foster clear channels of communication and empower self-advocacy and action from citizens to ensure everyone is doing their part during every hurricane season.

Brian Toolan is the vice president of global public safety at [Everbridge](#) and works with government and private sector organizations to ensure safety and resilience in the face of emergencies and crises. With 25 years of public safety experience, Brian draws from his domain expertise and background in public safety, having previously served as vice president of life and safety at Intrado and an operation chief at the Connecticut Division of Emergency Management and Homeland Security.

AI Partners – Filling Law Enforcement Experience Gaps

By Jeff Henderson



The Marshall Project, a nonprofit, nonpartisan news organization about criminal justice, states that Americans are choosing to opt out of policing and other government jobs. According to [their analysis](#), many officers resign or retire early after incidents such as the Floyd Protests in 2020-2021. Senior police officers are leaving the law enforcement profession. Imagine retaining most of the department's experiences and wisdom, even deploying that institutional knowledge with every officer in the field. This ability could soon be as simple as using a device like the one used to read this article. Artificial intelligence (AI), though, could offer much more expertise to any contact in the field, which supports law enforcement efforts to implement AI and machine learning (ML) into the daily lives of officers on duty for better and safer communities. It is imperative to look at how improvements in policing involving AI would benefit citizens in the short term and move forward.

Over time, law enforcement agencies often lose officers due to a change in staffing or retirement. As agencies continue hiring new officers, they can replace the presence in the community, but there is a gap in knowledge and experience. Research suggests that using AI and ML in policing has already begun to [bridge the gap](#), with facial recognition being one example. Inexperienced officers may make rash decisions, escalating a situation into a violent encounter, which might be avoided with the insight and experience AI could provide.

Many officers are turning to jobs in the private sector, where there is potentially [more pay and flexibility](#). Many opt for jobs where they [do not have to interact with the public](#). The departure of these senior employees, though, leaves experience gaps. According to [The Marshall Project](#), "The problems may seem more severe because the sharpest declines have been in cities with more than 1 million residents, such as New York, Los Angeles and Chicago, where the number of sworn officers dropped twice as fast as the national average."

This article discusses how creating a database of police experience to be accessed and used by newer officers can lessen the impact of losing senior and experienced officers. Using a mobile device, officers could access the expertise of the officers leaving the profession, resulting in better field performance by younger and newer officers. It would also slow the experience gap that is widening.

The Exodus

According to the [U.S. Bureau of Labor Statistics](#), there was a [steady decline](#) in law enforcement and local government jobs during the pandemic. "From March 2020 to August 2022, the number of government workers dropped by 5%, while the number of local law enforcement employees decreased by 4%, the most recent data shows. The Census Bureau's government payroll survey shows similar trends."

[Turnover](#) in a law enforcement agency is an important topic to review because replacing an officer can be time-consuming and expensive. Direct costs to the agency include background checks, uniforms and equipment, psychological assessments, medical assessments, overtime, training, and administrative costs. Indirect costs include quality of services, productivity, accumulated institutional, and a loss of professional knowledge and skills. CNN news reported [shortages](#) in 2022 of new police applicants and current officers resigning or retiring. Due to these factors and increasing community concerns, law enforcement agencies are predicted to increase police and detective jobs [by 3%](#) between 2021 and 2031, so stemming the flow of losses and reducing turnover should be a priority for the police. If cops began gathering the experience of veteran officers (many of whom are leaving), they could prevent the loss of institutional knowledge and use AI technology to address the most critical aspects of community confidence.

A Catalyst

In Minneapolis, Minnesota, in 2020, George Floyd was arrested in front of a grocery store and died as a result of the arrest by Minneapolis Police Department officers. Two of the arresting officers were employed for [less than a week](#), with no prior police experience other than Basic Academy Training. Floyd's death was international news, part of protests and legislation leading to nationwide changes in law enforcement policies and procedures.

The community demands professional policing that is free of bias and relies on fairness and [de-escalation tactics](#) to offer alternative solutions. As a result, they may be relying on their limited training and peers for guidance. AI, though, could offer much more expertise to any contact in the field, which supports law enforcement efforts to implement AI and machine learning (ML) into the daily lives of officers on duty for better and safer communities.

AI and the Police – Change the Approach

In "[Flash Foresight](#)," Daniel Burrus offers a different lens to examine the problem of losing senior staffing. All places of employment will face impactful losses as employees exit the agency. Burrus suggests that there are seven triggers for generating foresight, two of which are "transform" (i.e., using technology to build competitive advantage) and "go opposite." Going opposite suggests going the opposite direction from where everyone else is looking, which results in seeing things nobody else is seeing – for example, solutions that no one could see because no one was looking for them or considering hidden opportunities, unnoticed resources and overlooked possibilities.

Considering the loss of senior officers and the slow addition of newer officers, law enforcement can use technology to retain officers' wisdom, allowing newer officers to become more efficient. To hire and retain officers, some agencies are already using AI systems. For example, the [Austin Police Department](#) uses Versaterm Public Safety's Case Service to take non-emergency police reports. That AI software instantaneously communicates with the public through voice, mobile, web, and text messaging to ask questions and fill out reports like those typically provided by officers.

The Austin Police Department is an example of going opposite and putting its energy into building up its AI system instead of trying to hire itself out of this situation. Researching AI technology, scientists and engineers at Pacific Northwest National Laboratory are working in the field of human-machine teaming to bridge the gap

between today's tools and the machine teammates of the future. The Digital Police Officer (D-PO) "is a vision of machine teammates: an artificial intelligence-based partner that can be reached through multiple devices including the patrol car's on-board computer and officers' mobile devices." The interface between the officer and D-PO can be as simple as the officer's smartwatch.

How AI Will Be the Solution

If an AI system were available to [offer alternative solutions](#) in the Floyd incident, it could have suggested alternative tactics, and the new officers' actions may have [changed the outcome](#). According to a [Police Executive Research Forum Report](#), agencies in 2020-2021 typically filled only 93% of the available positions. Overall, responding agencies hired 5% fewer officers and saw an 18% increase in resignations and a 45% increase in retirements compared to the previous year. As these trends continue, more police departments will employ inexperienced officers. Inexperience may increase the potential for [excessive-force issues](#), "No matter how well they are trained or what level of professionalism is instilled in them, many new officers lack the maturity and in groups may do things that are more emotional than wise."

To understand the future of AI, look at how law enforcement and others have implemented it in the past. [John McCarthy](#) defined AI in the mid-1950s as "The science and engineering of making intelligent machines." During that period, AI research focused on creating machines that could independently perceive and respond to their environment and perform tasks that would typically require human intelligence and decision-making without human intervention. AI has [often replaced human tasks](#), and it is now widely accepted to have AI running many industries, such as the auto industry assembly lines, and replacing the human worker. Those AI machines weld parts and paint the exteriors of cars at a level of precision that humans cannot match. In this example, the intricate detail the vehicle assembly requires could directly translate into machines performing the complex functions of police officers. An example would be giving officers step-by-step guidance on what questions to ask and what steps to take on an investigation. Additionally, AI can go through hours of video and audio evidence much faster than an officer can and determine the next leads to investigate or point the officer toward valuable suspect information.

An AI system would be like "[Siri](#)" on an iPhone in these evidence searches. The system would use [machine learning](#) to guide the officer, like partnering with a 25-year veteran officer. Currently, AI systems are used for booking flights, monitoring travelers in airports, and assisting pilots flying airplanes. This technology can take a 911 call, find the location on closed-circuit television surveillance, watch the real-time actions of the subjects involved, and drive or navigate the officer to the scene. AI that learns from all the available video footage, radio traffic, and court outcomes could use that database to guide a newer officer to make decisions similar to a seasoned officer by suggesting senior-level strategies for handling that type of call. [Pacific Northwest National Laboratory](#) believes that, in time, D-POs will be deployed in law enforcement agencies. The outcomes can be remarkably different when it and other similar technologies enter the field.

How the New "Digital Police Officer" Would Help New Officers

A wearable, field-deployed AI for an officer will capture all the experiences, strategies, and techniques senior officers use to navigate citizen or internal interactions. Through



each occasion, the AI system will learn positive or negative outcomes and then deploy guidance to field personnel that veteran officers provided in the past. For example, AI now assists pilots while flying planes; a mobile AI would assist officers on calls by giving them forecasted challenges.

Using AI technology to identify where shots may have been fired so officers can respond more efficiently and effectively to [shooting calls](#). Officers can respond to areas where current trends suggest a specific type of crime may occur (e.g., a burglary and the most likely times for that to happen). An officer can then be on the scene at or around that time and [may deter or catch a suspect](#). Knowing where a crime is happening is a skill that takes experience in the field. AI-powered predictive policing could direct new officers to areas they would otherwise know only with the experience of responding to numerous calls and crimes in that specific area. AI takes the need for personal expertise out and uses the data to suggest where the officer should be to [prevent crime](#). However, AI technology does not come without risk of bias becoming a factor.

AI may provide the officer with real-time camera information that would guide new officers by directing who and where involved parties are and if there are any weapons. The interface could be seamless, like having a veteran officer working right next to the new officer and giving guidance.

In the near future, a mobile AI will be deployed and offer the officer and public more confidence in the information to be processed and presented before deciding. AI will provide a superior component to policing because it removes the emotional or human element from a decision, which is heightened during an incident. It will remove any “caught up in the moment” or “I got pissed” feelings of an officer, which could potentially

impact the decision-making. Like in every community, this research could also affect those who engage in criminal activity and would be aware that officers have more accurate information. AI could lower all involved parties' stress, creating a calmer community. At a time when communities are looking at ways to re-imagine policing, AI and ML research could fulfill that expectation.

The Challenges

The introduction of AI was only 70 years ago; the next 70 years could see AI systems replacing officers entirely to better society. With all the advantages that mobile systems would offer, there are potential conflicts to consider when relying on AI in community

Implementing artificial intelligence into the daily lives of officers on duty could promote better and safer communities.

settings. In previous studies, AI was utilized in differing applications, and it has exhibited decision-making bias, which would be a crucial factor in policing. For example, AI systems have shown bias in credit allocations in the banking industry and [shades of racial bias](#) in criminal sentencing trials. The community and agencies alike will want to know how the technology could reduce bias implications and potential ethical issues.

AI will be evaluated on the testing outcomes and real-world examples. Research may also reveal a history of fairness. However, if the AI predicts incorrectly and an innocent person is unnecessarily affected, there is little accountability. The public is not fully exposed to the capabilities of AI yet, so there needs to be a greater understanding of how a decision would help create validity in the next decade. As they do, and as the police become more effective with far fewer adverse actions and decisions using AI, what now seems like science fiction will become the norm.

One path to solving the problem of losing experienced law enforcement officers is using AI in the community. With the high rate of advancement and development coupled with the potential need, AI could be the most sought-after solution in law enforcement. AI fills the gaps for non-biased policing and is becoming a more widely accepted standard in law enforcement. Law enforcement leadership should be prepared for their organizations, communities, budgets, and legal teams to integrate and adapt to that future reality. As a result, AI partners could make the current and new generation of officers more efficient, safer, and able to provide a high-quality law enforcement service from the first day an officer starts.

Police Commander Jeff Henderson started his law enforcement career in 1998 with the Woodland Police Department in Woodland, California. During his time at the Woodland Police Department, he worked many different assignments, which included: patrol, bicycle patrol, D.A.R.E., and Honor Guard. He was a firearms instructor for 13 years and on the SWAT team for 14 years. He was a field training officer for 12 years and a school resource officer for five years. In November 2013, he lateralled to the Suisun City Police Department, where he was promoted to the rank of sergeant. During his time at the Suisun City Police Department, he worked patrol and was the department range master and Glock armorer. Additionally, he was the Preliminary Alcohol Screening device coordinator, taught building search tactics, and was the cadet coordinator. He lateralled and was promoted to lieutenant for the Oakdale Police Department in 2019. He served as the support service division commander, managing dispatch, investigations, property and evidence, and animal control. He returned to the Suisun City Police Department in May 2021 with a promotion to the position of police commander. He has a bachelor's degree in criminal justice administration.

Family Terror Networks 2.0: January 6

By Dean C. Alexander and Huseyin Cinoglu



The storming of the U.S. Capitol on January 6, 2021, was a [momentous event](#) politically, socially, and most importantly, in terms of the evolution of [domestic extremism](#) in the United States. The multifaceted consequences of January 6, mired by misinformation and disinformation, continue today. [As of June 2023](#), over 1,043 people have been arrested for their purported roles on January 6, with defendants from nearly 50 states. Within that grouping, “338 defendants have links to more than [50 extremist groups and movements](#),” including (in order of highest representation): QAnon, Proud Boys, Oath Keepers, Three Percenters, White Nationalists, and Sovereign Citizens. Among the anti-statist extremists present on January 6 were [accelerationists](#):

Individuals with disparate beliefs are united in the goal of hastening the cataclysmic end of economic, political, and social systems so as to more rapidly bring about what is seen as an inevitable end-times collapse and subsequent rebirth into a utopian afterworld.

Interestingly, however, about two-thirds of all defendants were [not affiliated](#) with such groups, meaning they were self-radicalized, “individual believers,” and their ranks were peppered with a host of personal grievances waiting for an outlet to trigger them into action. Ultimately, this fusion of factors contributed observably to the dynamic of [mass radicalization](#) becoming mass mobilization.

Further inquiry into the January 6 defendants – the largest criminal prosecution in U.S. history – shows 180 had [military backgrounds](#). Among the states with the most defendants [by state residency](#) were: Florida (112, Pennsylvania (84, Texas (83, California and New York (71), Ohio (56), and Virginia (54). According to the Office of the U.S. Attorney for the District of Columbia, between [1,600 and 2,100 additional people](#) are expected to be charged in relation to the January 6 attack. In that case, 2,600-3,100 could be charged for their conduct on January 6, accentuating the inordinate number of extremists mobilized into action that day. [As of May 2023](#), over 30 Proud Boys and Oath Keeper members have pleaded guilty or been convicted in relation to their activities on January 6. The Oath Keepers founder, Stewart Rhodes, was sentenced to [18 years](#).

According to the U.S. Attorney’s Office for the District of Columbia, [as of June 2023](#), the January 6 prosecutions include:

- 347 defendants charged with assaulting or impeding officers, including 109 with deadly weapons or serious bodily injury.
- 909 defendants charged with entering restricted federal buildings, 103 while carrying deadly and/or dangerous weapons.
- 310 defendants charged with obstructing or influencing official proceedings.

- 55 defendants charged with conspiracy related to obstructing congressional proceedings, law enforcement, or injuring officers.
- 587 individuals pleaded guilty to federal charges, many facing or expected to face incarceration.

This article discusses the phenomenon of family-affiliated extremism among the January 6 siege participants. In particular, it highlights the 177 persons prosecuted with family members on January 6 comprising 90 familial relationships among them. Then, the piece compares this set of January 6 extremists with family terror networks observed in primarily violent jihadist operatives covered in a 2019 study involving 138 kin affiliations among 281 extremists. In total, this record demonstrates the dangers arising from kin-connected extremism. Also, the work discusses law enforcement responses to terrorism and efforts against family-affiliated extremism. Lastly, the article addresses selected law enforcement responses on January 6 and lessons learned therein.

Radicalization and Family Terror Networks/Family-Affiliated Terrorism

The [reasons](#) for an individual supporting an extremist movement or terrorist group include:

- Belief that the ideology is correct and merits support;
- Revenge for real or perceived victimization;
- Socioeconomic marginalization and alienation;
- Political marginalization and alienation;
- Protection against perceived oppressors;
- Acceptance, respect, or status;
- Pressure from family, friends, and community;
- Expunging dishonor due to moral indiscretion;
- Seeking purpose or excitement in life;
- Mental disability; and
- Alternative to failures or setbacks.

Radicalization is an identity formation process. Its intended result is the acceptance of violent extremism. Family's importance and its unique role in providing an identity during childhood and adolescence have already been [accepted in literature](#). However, as the January 6 events proved one more time, some families also radicalized and accelerated the radicalization processes of their members. There is a need to delve deeper into how familial connections catalyze radicalization and extremism.

Families can instill radical beliefs, values, worldviews, and ideologies. Those new inputs are often met with unfiltered acceptance, especially when familial ties intersect with extremist worldviews. The [familial backdrop as a nurturing environment](#) has continuously provided unique opportunities for terrorist groups.

Families are a significant source of emotional bonding. Families, by design, have the potential to fulfill the innate desire for belonging. Emotional support and validation in families may also lead people into a radicalization pathway. This will also strengthen

one's budding commitment to family-approved radical worldviews. In selected families, members are exposed to preselected information and narratives that would establish and reinforce ties with radical groups.

Confirmation bias in families has also proven to be a significant catalyst for radicalization. Fact-checking and further investigation to establish the truth are disproportionately low compared to other social settings. Sadly, particular family members tend to believe even an illogical and baseless view proffered by other kin. These January 6 siege cases attest that a growing number of people (the authors' research has identified 177 individuals) entered the U.S. Capitol with a family member. Subsequently, they faced legal prosecution for engaging in criminal activities associated with the events.

Analogously, families provide transgenerational transmission of radical beliefs. Parents are essential agents in passing down their extremist ideologies to their children. Moreover, they may restrict their children's mainstream values and significantly limit their exposure to diverse perspectives. Under the influence of groupthink, children are unlikely to have the opportunity to question and accept what is presented to them without resistance. That creates a vicious cycle of radicalization. Family structures facilitate higher rates of radical belief conversion due to the credibility and trust conferred within the family unit, in contrast to unaffiliated networks. Breaking free from that spell is complicated, time-consuming, and sometimes ineffectual.

In sum, family-affiliated extremism (or alternatively, family terror networks) involves two or more people from the same family unit who support the threat or use of political violence. "[Kin terrorism](#) has appeared across diverse views, from religiously motivated precepts to national liberation movements, and from hate-based ideologies to other extremist viewpoints." The mix of radical tenets embraced by kin-connected insurrectionists on January 6 and their conduct merit attention.

Family-Affiliated Extremism Among the January 6 Rioters

The authors' research thus far has found that 177 people were arrested with other family members in connection with their criminal offenses while entering the U.S. Capitol on January 6. The different family relationships encompassed 90 occurrences of kin relationships (e.g., husbands and wives, siblings, and parents and children) involved in January 6 events.

Collectively viewed, the January 6 suspects frequently show a pattern of embracing varied conspiracy theories and fringe perspectives (e.g., QAnon precepts, support for Stop the Steal movement, antigovernment and various militia ideologies, white nationalism, opposition to government COVID-19 restrictions, etc.) or other personal grievances. In total, these participants were primarily tied that day to an apparent unifying practical objective: interfering with the congressional certification of the Electoral College results tied with the 2020 presidential elections.

- [Illinois husband](#) with QAnon references on Twitter, expressed [interest in being in D.C.](#) on January 6.

- [Texas son](#) charged with father, claimed he entered Capitol against father's wishes during mob action.
- [Georgia mother and Tennessee son](#) referred to Capitol breach as support for revolution, mother expressed willingness to die fighting oppression.

The family-linked U.S. Capitol defendants resided in several dozen states, comprised a breadth of ages ranging from a 20-year-old daughter to a 70-year-old husband, and held varied occupations/stages in life (e.g., real estate broker, doctoral student, retired, etc.). Some families entered the U.S. Capitol with their minor children, who are not included in this analysis as they were not prosecuted. Likewise, the convictions per family members sometimes comprised a few, relatively “minor” charges (e.g., entering or remaining in a restricted building as well as disorderly conduct therein). In contrast, others were charged with up to nine counts individually, and, for some, serious offenses (e.g., seditious conspiracy, conspiracy, obstruction of an official proceeding, and assaulting a federal officer). Convictions of family-affiliated extremists were marked by weighty offenses and resulted in prison sentences of 14 years and two months. Many of the offenders pleaded guilty or were found guilty at trial. Others are awaiting adjudication.

Two [Montana brothers](#), for instance, are alleged to have been among the first ten rioters to climb through a window into the Capitol. The pair, and others, then pursued U.S. Capitol Police Officer Eugene Goodman, before ultimately entering the Senate floor, sitting in “Senators’ chairs, opened Senators’ desks, and reviewed sensitive material stored therein.” A [Tennessee-based man](#) and his mother from Georgia are on video surveillance on U.S. Capitol grounds and walking in the U.S. Capitol with other rioters. Both of them had flex cuffs while there. A [Missouri-based niece and uncle](#) faced multiple charges, including two connected to the theft of an engraved wooden nameplate of the Speaker of the House Nancy Pelosi.

A pair of male [cousins](#) – one from Louisiana and one from Texas – were charged with the same five crimes including assaulting a federal officer. The pair created and disseminated incriminating photos and videos of themselves at the U.S. Capitol, such as one where the Louisiana cousin told a contact on Facebook, “I have more videos of us breaching the Capitol but not gonna [sic] post them. We will be back and it will be a lot worse than yesterday!” In other social media posts, the [Texas cousin](#) stated “4 of us breached the cops blockade and us same 4 breached the Capitol.” Days after the event, [some family members](#) charged with U.S. Capitol connected crimes asserted they were merely exercising their free speech or predicted the FBI would “see some pics but no militia.”

Although often family members were charged with the same crimes, in other instances – as with an [Iowa-linked mother and son](#) – overlapping and distinct charges have been filed. In the case of [two sets of spouses](#), they were charged similarly on four charges (including conspiracy whose goal “was to stop, delay, and hinder Congress’s certification of the Electoral College vote”), along with five others, some of whom are purportedly members of the Oath Keepers.

After attending a pro-Trump rally in Washington, D.C., a [pair of male cousins](#), one from Kentucky and the other from Virginia, marched toward the U.S. Capitol “because” – according to the former – “President Trump said to do so.” One later shouted, “stop the

steal,” once they were both inside the Capitol. Authorities intend to use a [photo of the smiling pair](#) wearing “‘Trump 2020’ baseball hats” and each “holding up their middle fingers” while inside the Capitol building as proof of their presence there. A [North Carolina husband, with his wife](#) nearby, remarked in a video, at Statuary Hall, “Who would’ve knew the first time I ever come would be to storm.” The same man, in concert with other rioters, referred to police as “F***ing traitor[s]” and, in unison with other protesters, screamed, “Where’s Nancy’s [Pelosi] office?” At an earlier point, the man repeatedly chanted with a crowd in the Capitol’s crypt, “Who’s House? Our house?” and “Stop the steal!”

Selected [family members](#) approached the U.S. Capitol as part of a larger block of group-linked rioters (e.g., Oath Keepers) in a “stack or line formation” in order to maintain “direct physical contact with one another” as it enhanced communication, “especially in crowded or noisy areas.” This appears to have taken place with two sets of spouses (from Ohio and Florida) and a brother and sister (from Arizona). [Communications within distinctive cabals](#) included text messages, phone calls, leveraging social media, and through a Zello (a push-to-talk application that operates like a walkie-talkie on a cellular telephone) channel called “Stop the Steal J6.” Other coordination between kin and individuals supposedly tied to formal groups has been proffered by accounts alleging they communicated together beforehand, stayed at the same hotels, and met there early on the morning of January 6. A [North Carolina couple](#) drove to Washington, D.C. in their own car, but joined a car caravan organized by a Twitter personality.

Sentencing for a [North Carolina-based husband and wife](#) who were convicted of “assaulting, resisting, or impeding law enforcement officers and obstruction of an official proceeding” and “for obstruction of an official proceeding,” respectively, resulted in the prison sentences of 41 months, for the former, and 8 months, for the latter. A [Pennsylvania couple](#) who pepper sprayed law enforcement on January 6, and conducted other criminal acts, was sentenced to two years (wife) and 14 years and two months (husband).

While approximately two-thirds of arrestees were unaffiliated with a particular group, some claimed or had connections to such entities as Proud Boys or Oath Keepers. According to an FBI affidavit, “[Oath Keepers](#) are a large but loosely organized collection of militia who believe that the federal government has been coopted by a shadowy conspiracy that is trying to strip American citizens of their rights.” A Florida couple, and another one from Ohio, were charged in unison with several suspected Oath Keepers members. Also, one such family member was listed by a purported co-conspirator as an “Ohio State Regular Militia” recruit. An Arizona brother and sister were charged with conspiracy with three supposed Kansas City Proud Boy members. The sister bragged she was invited to join the group’s chapter and displayed a challenge coin she claimed to have received from them. According to an FBI affidavit, [Proud Boys](#) “is a nationalist organization” that describes itself as a “‘pro-Western fraternal organization for men who refuse to apologize for creating the modern world; aka Western Chauvinists.’”

Among [three female Oath Keeper members](#) found guilty of conspiracy to obstruct an official proceeding included two wives and a sister. Kelly Meggs, the husband of one of the aforementioned spouses and [leader of the Florida Oath Keepers](#), was convicted of seditious conspiracy and other charges. He was sentenced to 14 years in prison. Other

notable defendants were a Florida Proud Boys [father and son duo](#) who formerly served as police officers. Two [Oregon brothers](#), including a self-identified Proud Boy, were indicted on six federal counts, including conspiracy, obstruction of an official proceeding, and destruction of government property.

Family Extremism Networks 2.0: Insights From January 6

From an analysis of the 177 family members authorities have linked with January 6-related family extremism, there were 90 occurrences of kin relationships (e.g., spouses, siblings, and parents and children). In some instances, family relationships involve individuals who were counted more than once (because multiple family members were present). For example, in the case of a father and two sons: they are listed once as “father-son” and again as “brothers.” While this may appear repetitive, the reality is two different forms of relationships were present. Ten percent of the 90 family-affiliated extremism cases (9) involved multiple counting. The fact that 17.1% (177/1,033) of the people who breached the U.S. Capitol did so with other family members exemplifies the effects of radicalization among kin.

In aggregate, the types of family relationships (90), among the 177 persons charged with other family members for their alleged federal crimes at the U.S. Capitol on January 6, included:

<i>TYPE OF KINSHIP</i>	<i>N (out of 90)</i>	<i>%</i>
<i>Husbands/Wives</i>	28	31.1
<i>Parents/Children</i>	27	30.0
<i>Siblings</i>	25	27.8
<i>Cousins</i>	5	5.6
<i>Uncle/Nephew</i>	1	1.1
<i>Aunt/Nephew</i>	1	1.1
<i>Uncle/Niece</i>	1	1.1
<i>Brothers-in-law</i>	1	1.1
<i>Stepmother-in-law/Stepson-in-law</i>	1	1.1
<i>TOTAL</i>	90	100

The results above show 88.9% of the 90 families comprising the family-affiliated extremists of January 6 involved fairly equal amounts of husbands/wives (28/90 or 31.1%) parents/children (27/90 or 30%), and siblings (25/90 or 27.8%). As such, these case studies suggest that family-affiliated terrorism occurs most readily in husbands/wives, parents/children, and siblings than in other family relationships.

Here is a further breakdown of parent(s)/child(ren) relationships.

PARENT(S)/CHILD(REN) RELATIONSHIPS	N (out of 27)	Overall % (of 90 cases)
<i>Father/son(s)</i>	19	21.10
<i>Mother/son(s)</i>	5	5.60
<i>Father/daughter</i>	1	1.10
<i>Mother/daughter</i>	1	1.10
<i>Parents/children</i>	1	1.10
TOTAL	27	30

Here are more details of sibling relationships.

TYPES OF SIBLINGS	N (out of 25)	Overall % (of 90 cases)
<i>Brothers</i>	14	15.60
<i>Brother/sister(s)</i>	9	10.00
<i>Sisters</i>	2	2.20
TOTAL	25	27.80

These results are attributable to the bonds that coalesce during courtship and marriage as well as the influence parents can have on their children. The frequency of siblings in this study underscores the potency of sibling relationships. Six other sources of January 6 family-extremist connections contributed 11.1% of such instances, namely: cousins (5/90 cases or 5.6%) while uncle/nephew, aunt/nephew, uncle/niece, brothers-in-law, and stepmother-in-law/stepson accounted for 1/90 cases or 1.1% individually. The case studies chosen for this study arose principally through a systematic review of the U.S. Attorney's Office for the District of Columbia list of U.S. [Capitol breach cases](#), supplemented by media sources of January 6 prosecutions.

Family Terror Networks 1.0

"Although of a different strain and less serious offenses – none specifically terrorism nor involving murder" – [kin-connected radicalism](#) witnessed on January 6 "is neither a new phenomenon nor one unique to the United States or elsewhere." In fact, in Alexander's 2019 book, "[Family Terror Networks](#)," he "[analyzed 118 global cases](#) of family terror networks, including some 50 instances involving U.S.-based jihadists, sovereign citizens, militia, and white supremacy adherents. Illustrations of such family terror networks encompassed: multiple brothers" (e.g., two sets of brother hijackers on 9/11, a set of brothers in ISIS attack in Paris in 2015, and 2013 Boston Marathon bombers), husbands and wives (e.g., participants in the 2015 San Bernardino attack, 2014 killing of two police officers in Las Vegas, and FBI translator marrying an ISIS leader), fathers and sons (e.g.,

2010 murders of two police officers in Arkansas, 2008 murder of two police officers in Oregon, and 2004 killing of a bank security guard in Oklahoma), cousins (e.g., 9/11 mastermind Khalid Sheikh Mohammed and 1993 World Trade Center bomb-maker Ramzi Yusef, three 9/11 hijackers, and a subverted attack at an armory in Illinois in 2015), and many more.

The findings from “[Family Terror Networks](#)” showed 118 case studies of family participation in terrorism encompassing 138 occurrences of kin relationships (e.g., husband and wives, brothers, and fathers and sons) and comprising 281 individual family members. Similar to the January 6 cases, a family may have more than two persons involved in extremist activities. In aggregate, these many instances of family relationships involved in terrorism were exhibited, in the main, accordingly: siblings (48 out of 138 or 34.78%), husbands/wives (43 out of 138 or 31.16%), fathers/sons (15 out of 138 or 10.87%), and cousins (11 out of 138 or 7.97%). Those findings also found:

Overwhelmingly, violent jihadism was the ideology connected to the 118 instances of families affiliated with terrorism that were reviewed. This type of extremism was found in [87%] of the cases with other precepts occurring comparatively fairly rarely [(13%)]. Among the non-jihadists associated with kin terrorism, they were affiliated with mostly right-wing extremism (e.g., sovereign citizens, militia, and white supremacy).

Law Enforcement Combating Extremism

One can delineate potent police counterterror efforts and countermeasures focused on family-affiliated extremism between those activities effectuated internally to the police department and those focused on the public. Attention to these distinct responses can prove helpful when management crafts steps to undermine radicalism in the United States. Subsequently, law enforcement’s experience with January 6 extremism and the investigation of criminal conduct by rioters that day are addressed.

Police Countermeasures Internal to the Department

Foremost and foundationally, police management must recognize that terrorism merits organizational concern. The administration should allocate personnel and other resources to undermine radicalism. Also, management should raise awareness of the threat and its negative implications for “[police officers](#) and the community. Acknowledgment that common crimes can be associated with extremism” should buttress police awareness of radicals in their jurisdictions.

Threats to officer safety stemming from these nontraditional criminals must be emphasized with personnel. [Attacks on officers](#) “by terrorists of varied ideological affiliations encompass spontaneous and pre-planned incidents across varied means of attack” (e.g., gunfire, vehicle, and edged weapons) in diverse settings (e.g., while on the street, in a vehicle, and at a precinct). In May 2020, for example, [Boogaloo member Steven Carrillo shot and killed](#) a Federal Protective Service officer in Oakland, California. The following month, [Carrillo killed a sheriff’s deputy](#) in Santa Cruz, California. Subsequently, he was later captured and faces federal and state charges surrounding these deaths and

other counts. Also, [risk to police](#) arises while countering a kinetic “incident by a sovereign citizen, militia member, hate-affiliated operative, a jihadist, or another culprit.”

“[Multiple state statutes](#) can be engaged to prosecute persons suspected of extremism. This is so even as federal prosecutions are often the mainstay of terrorism cases. Both federal and state laws may have applicability relative to an accused terrorist or” hate-crime perpetrator, among others. The following [criminal activities](#) may have relevance “in prosecuting radicals: terrorism, sedition, gang membership, organized crime, hate crimes, arson, possession of unregistered explosives, and stalking. As sometimes such fanatics are involved in precursor crimes or other criminality, their unlawful actions may” also include money laundering, weapons or drug offenses, fraud, extortion, identity theft, human trafficking/smuggling, and sex crimes.

It is [critical for police agencies](#) to “use existing federal, regional, state, local, and tribal counterterrorism organizations and resources in their efforts to subvert terrorism locally. For instance, over 100 Joint Terrorism Task Forces, some 80 regional and state fusion centers, multiple drug and other specialized task forces, as well as anti-money laundering and” counterterror finance groups, should be engaged as relevant. [Likewise](#), the use of classified and nonclassified “intelligence databases, along with submission to and accessing national suspicious activity reports and suspicious transaction reports (via the Department of Treasury’s Financial Crimes Enforcement Network), are [utile instruments.] Of note, the National Crime Information Center ([NCIC](#)) database contains information about [known or suspected terrorists](#). Daily some [55 traffic stops](#) that get an NCIC hit on a suspected terrorist, meriting appropriate follow-up by police.”

Obstacles to police department success in taking steps internally to undermine extremism are manifold but may rest on faulty assumptions, inaction, or other circumstances. “Some departments are of the [incorrect mindset](#) that extremist threats will never happen in their town. The lack of kinetic attacks, reported hate crimes, and silent terror fundraising and money laundering efforts are not indicative of the lack of radicalism in one’s community. Other jurisdictions may project terrorism as a concern nationally but not so locally.”

“Along with such thinking is the belief that while an acquaintance has characteristics otherwise meriting concern, the person is perceived as innocuous. Elsewhere, a suspect may engender the modes of radicalization, indicators of mobilization, and other attributes of extremism that are unrecognized. Preconceived perspectives of who might be a radical – even stereotyping – may cause wrong determinations, such as false negatives and positives. Still, a police department may face multiple” [pressing challenges to their limited resources](#) straining their ability to monitor and counter rising “extremism. In that setting, the issue is not a lack an awareness of the threat but a capacity to assuage it.”

Police Responses Centered on the Public

Police departments may craft multiple, distinct counterterrorism efforts that center on the public. They should fixate on endeavors that detect and counter radicalization and terror recruitment efforts. [Police should become](#) “skilled at ferreting out individuals who have become mobilized (radicalized persons who support the use of violence in their

efforts and intend to do so). Although not foolproof, it is imperative that criminal analysts assess questionable behaviors that are dangerous” independently of other considerations (e.g., declaring one is seeking martyrdom) and warrant immediate countermeasures (e.g., impending travel to a conflict zone).

“Paying attention to the prospect of family terror network-centered suspects is worthwhile, as this type of terrorism has become prominent globally. By understanding the influences of families on the creation of terrorists, incapacitating the likelihood of their involvement in terrorism is enhanced. Multiple family members have taken part in prominent U.S. extremist incidents,” [for example](#):

- 2010 killing of two police officers during a traffic stop in Arkansas by the father and son ([Kanes](#); son did the shooting at the father’s behest);
- 2013 Boston Marathon attacks by [Tsarnaev brothers](#);
- 2014 assassination of two Las Vegas police officers by husband and wife ([Millers](#)); and
- 2015 San Bernardino shooting ([spouses Farook/Malik](#)).

“Other successful countermeasures include pursuing [traditional policing efforts](#) like conducting traffic stops and responding to calls for service. These bread-and-butter policing functions should be carried out against a cognizance of well-known signs of terrorism: surveillance of and eliciting about a target, testing the security of an asset, acquiring supplies, fundraising, impersonation, conducting a dry run, and getting into position for an attack. Using informants and undercover agents in building a case has relevancy as in other investigations. Informants and undercover agents are used in many extremist cases across all ideological spheres. In [the fall of] 2020, [an undercover FBI employee posed as a member of Hamas](#) while interacting with two anti-government operatives (Boogaloo Bois) in relation to the latter offering themselves as mercenaries” for [Hamas](#), a designated Foreign Terrorist Organization. “The pair were [accused of](#) conspiring to provide material support to Hamas.”

[Police](#) can [leverage technologies](#) “in their quest to combat terrorism. For example, they can monitor social media, use commercial and proprietary monitoring tools, and get search warrants for electronic devices, including phones and computers. Also, license plate readers, stingrays, infrared cameras, and explosive and metal detectors are among those technologies that can aid in disrupting radicalism. Still, [terrorists are skillful](#) at diverse technologies to communicate, conduct” command-and-control “measures, and raise funds. Heightened capabilities with encryption and emerging technological developments often force authorities to play catch up. The [lack of cooperation by some companies](#) in certain instances makes accessibility to terrorist data – even once a warrant has been issued – quite difficult.” Also, the insufficient training on social media technology within agencies and limited human resources for specialization make the necessary cooperation all the more complicated.

Next, [efforts should be centered](#) “on preventing the acquisition of [extremist funding](#) and other material support, such as the provision of weapons, safe houses, fake”

identifications, training, and expert advice. Besides undermining fundraising, [focus needs to be paid](#) to “the movement of these monies and interdicting money laundering efforts (when monies derive from illicit actions). Consideration should also rest on stopping the next strike. It is imperative to initiate risk and vulnerability assessments so that damage from attack is limited. Such security assessments examine the assets requiring protection, their vulnerability, and criticality. It is paramount for jurisdictions to generate a list of the most prone government, private sector, nonprofit, and nongovernmental organization targets and encourage them to harden their sites.”

Several variables are relevant when responding to a terrorist attack. Initially, one must weigh the form of attack the police may face: bombing, active shooter, vehicle attack, a combination of them, or others. Upon arriving at the location, police must detain or otherwise neutralize the perpetrator(s). Terror incidents may not prove static as an active shooter situation can evolve into a hostage scenario, the converse, or multiple attacks at disparate locations. [New York Police](#) Department’s Critical Response Command has heeded this concern by training its members to detect and impede attacks such as chemical, biological, radiological, nuclear, explosives, and the like.

The [police department](#) “should encourage the [public’s involvement](#) in combating terrorism. The public can recognize the signs of terrorism, inform police of their concern, and aid them in preventing attacks. In particular, [the] industry can facilitate identifying suspicious behaviors, transactions, and persons (employees and customers) that have a nexus with terrorism. Likewise, sustained, trust-infused, and impactful community policing efforts have a role in undermining and uncovering extremism, especially in otherwise alienated and marginalized populations. Fostering engagements with well-known, credible community leaders can contribute to increasing public vigilance and resilience to infiltration by radicals. Neighborhood policing can help develop sources, gain insights [into] suspicious persons and activities, and pinpoint where to use informants and undercover agents in future sting operations.”

[High-profile](#) “involvement in communities can deter [hate crimes and other extremism](#) in the area, including through de-radicalization efforts. Additionally, once police cement ties with a neighborhood, they can build up bonds with particular households. In doing so, police can detect a family terror cell, encourage activities within the family to expunge radicalism that may exist, or prevent infiltration of extremism within a home.”

Law Enforcement and January 6

Law enforcement identified U.S. Capitol breach suspects from various sources, such as tipsters, coworkers, friends, (other) family members, informants, social media accounts of suspects and their incriminating remarks or poses on videos and photos, news media stories, cell site records, interviews with suspects and others, video surveillance footage, and revelations arising from execution of search warrants. Distinctive clothing (“camouflaged-combat attire”), headgear (baseball caps to tactical helmets affixed with stickers), goggles, group patches/logos/insignia, backpacks, a Confederate Battle Flag, and prominent tattoos aided in their discovery during

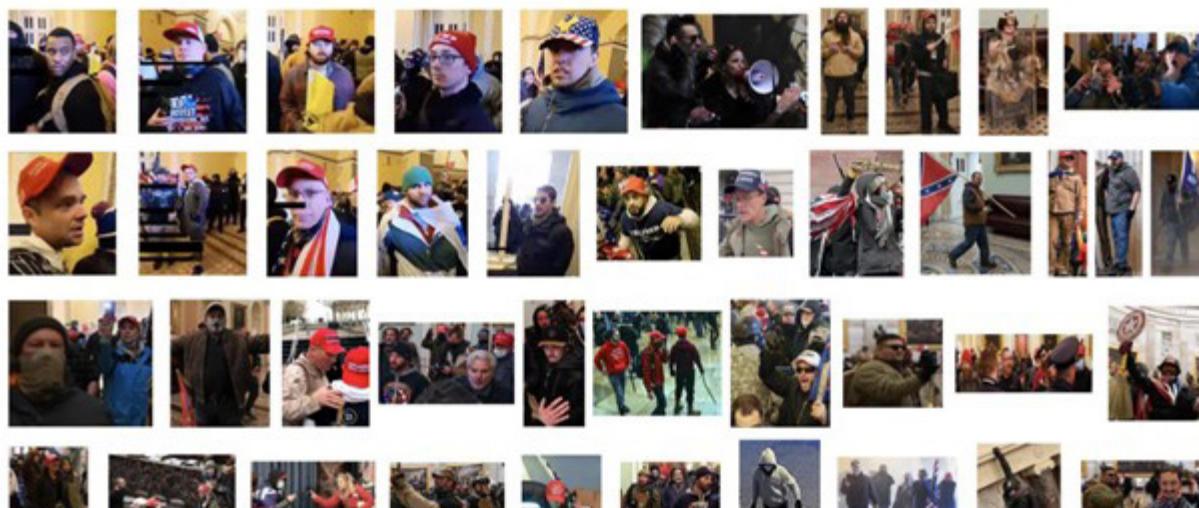
preliminary investigations. Other evidence has been garnered through troves of cached Parler (“conservative alternative to Twitter and Facebook”) accounts and insights from communications on Telegram channels.

Law enforcement responses to the Capitol Hill siege on January 6 represented a watershed point in the challenge of domestic extremism threatening the peaceful transfer of political power. Law enforcement authorities had the enormous challenge of restoring order and defending the seat of American democracy as the world watched in shock. The incident showed flaws in intelligence gathering, communication, training, readiness, management, and political calculations, among other failings. More broadly, the [June 2021 U.S. Senate bipartisan report](#), “Examining the U.S. Capitol Attack: A Review of the Security, Planning, and Response Failures on January 6,” (Report) found:

- The [federal intelligence community](#) – led by FBI and DHS – did “not issue a threat assessment warning of potential violence targeting the Capitol on January 6.” [FBI denies](#) this allegation, and they claim that prior to the U.S. Capitol riot, they provided a cautionary alert concerning the potential for violence.
- USCP’s [U.S. Capitol Police] intelligence components failed to convey the full scope of threat information they possessed.
- USCP was not adequately prepared to prevent or respond to the January 6 security threats, which contributed to the breach of the Capitol.
- Opaque processes and a lack of emergency authority delayed requests for National Guard assistance.
- The intelligence failures, coupled with the Capitol Police Board’s failure to request National Guard assistance prior to January 6, meant District of Columbia National Guard was not activated, staged, and prepared to quickly respond to an attack on the Capitol. As the attack unfolded, DOD required time to approve the request and gather, equip, and instruct its personnel on the mission, which resulted in additional delays.

The report also published [21 findings of facts](#) showing there were multiple deficiencies across various agencies and departments that contributed to the security, planning, and response failures on January 6. Among [crucial lessons](#) from the Capitol breach incident are for law enforcement to elevate communication, coordination, training, staffing, and intelligence sharing capabilities and expand security funding. Additionally, there is a need to reassess the existing security standards. In addition, law enforcement personnel also displayed incredible bravery and perseverance while significantly outnumbered on January 6 in the face of hours-long onslaughts by rioters, as of June 2023, 109 of whom are accused of using “a [deadly or dangerous weapon](#) or causing serious bodily injury to an officer.” Hopefully, this study shows the need for law enforcement and the intelligence community to consider family-affiliated extremism as an enduring feature in 21st-century terror threats.

SEEKING INFORMATION



Source: Federal Bureau of Investigation Facebook post (January 8, 2021).

Conclusion

The 90 kin-connected prosecutions representing 177 persons involved in extremist activity on January 6 demonstrates the importance and ubiquity of family-affiliated extremism worldwide. The reality that 17.1% (177/1,033) of the people prosecuted in the siege at the U.S. Capitol participated in the onslaughts with other family members epitomizes the dangers of radicalization within a family unit. Also, the existence of family terror networks across ideologies was confirmed in 281 individuals in the 2019 book [Family Terror Networks](#). While the impetus for a person becoming an extremist can be multi-dimensional, family relationships are not the sole factor affecting radicalization. Still, given its frequency globally and so prominently on January 6, this terror phenomenon merits closer attention.

Law enforcement's broad efforts in combating terrorism will concurrently undermine a subset of this political violence, namely, family-affiliated extremism. This is especially so once law enforcement fully appreciates the pervasiveness and negative effects of family terrorism networks. Police efforts in combating terrorism need to be at the forefront of their activities. After all, the U.S. Department of Homeland Security's [May 24, 2023](#), National Terrorism Advisory System projected:

In the coming months, factors that could mobilize individuals to commit violence include their perceptions of the 2024 general election cycle and legislative or judicial decisions pertaining to sociopolitical issues. Likely targets of potential violence include U.S. critical infrastructure, faith-based institutions, individuals or events associated with the LGBTQIA+ community, schools, racial and ethnic minorities, and government facilities and personnel, including law enforcement.

Against this backdrop, it is probable that extremist activity in the United States will continue to be prevalent in 2023 and beyond, represented, at times, by participants whose radicalization has emerged within a family unit, and whose mobilization to violence occurs in unison with other family members. Indeed, these scenarios were seen on January 6 and in numerous instances beforehand in the United States and abroad. In the face of such foreboding political violence, U.S. federal district judge Amit Mehta aptly stated during the May 2023 [sentencing of Oath Keepers founder Stewart Rhodes](#), “What we absolutely cannot have is a group of citizens who – because they did not like the outcome of an election, who did not believe the law was followed as it should be – foment revolution.” This is true whether the person acts as such alone or in concert with others, irrespective if they are kin or otherwise, particularly in presidential elections.

Retrospectively, January 6 was a watershed moment for law enforcement and the country. Some sought to explain this phenomenon through the lens of [contagion theory](#), while others preferred non-theoretical explanations for the violence. What was witnessed that day was not “sightseeing” by pacific actors, but rather, violently inclined individuals who wreaked havoc on the country’s institutions and processes. Today, the irrefutable January 6 belligerency is characterized by some (e.g., particular politicians and media figures) as meritorious, patriotic actions. Such a perspective is wrong and undermines the foundations of democracy. Instead, the threat or use of political violence by anyone – irrespective of one’s political viewpoint or grievance – should be viewed as untenable. Otherwise, prospectively, political power will be transferred chaotically, led by individuals blinded by the aphorism “might is right.”

Prof. Dean C. Alexander JD, LLM, is the director of the Homeland Security Research Program and professor of Homeland Security at the School of Law Enforcement and Justice Administration at Western Illinois University. In addition to numerous peer-reviewed publications, he has authored several books on terrorism, including: Family Terror Networks (2019); The Islamic State: Combating the Caliphate Without Borders (Lexington, 2015); Business Confronts Terrorism: Risks and Responses (University of Wisconsin Press, 2004); and Terrorism and Business: The Impact of September 11, 2001 (Transnational, 2002). In addition, he is frequently interviewed by domestic and international media, such as the Washington Post, Boston Globe, Atlanta Journal-Constitution, Chicago Tribune, Dallas Morning News, Orlando Sentinel, Associated Press, Voice of America, Security Management, El Mercurio, Tribune de Genève, and NHK. He has provided on-air commentary for television and radio stations, including CBS Radio, Voice of America, Wisconsin Public Radio, and CBC Business. dc-alexander@wiu.edu

Dr. Huseyin Cinoglu is an associate professor of Criminal Justice in the Department of Social Sciences at Texas A&M International University (TAMU). Dr. Cinoglu published and presented extensively in the areas of (countering) violent extremism, (countering) terrorism, (de)radicalization, immigration, crime and criminality, identity formation, and terrorist identity formation. He authored or co-authored several books. His publications appeared in respected journals such as International Journal on Criminology, European Scientific Journal (ESJ), International Journal of Human Sciences, and IOS Press. Dr. Cinoglu was interviewed by Newsweek and Laredo Morning Times. huseyin.cinoglu@tamiu.edu

RESPONSE LEADERSHIP



LISTEN WHEREVER YOU GET YOUR PODCASTS:

Apple Podcast

iHeartRadio

Spotify

Or listen online at: teex.org/podcast