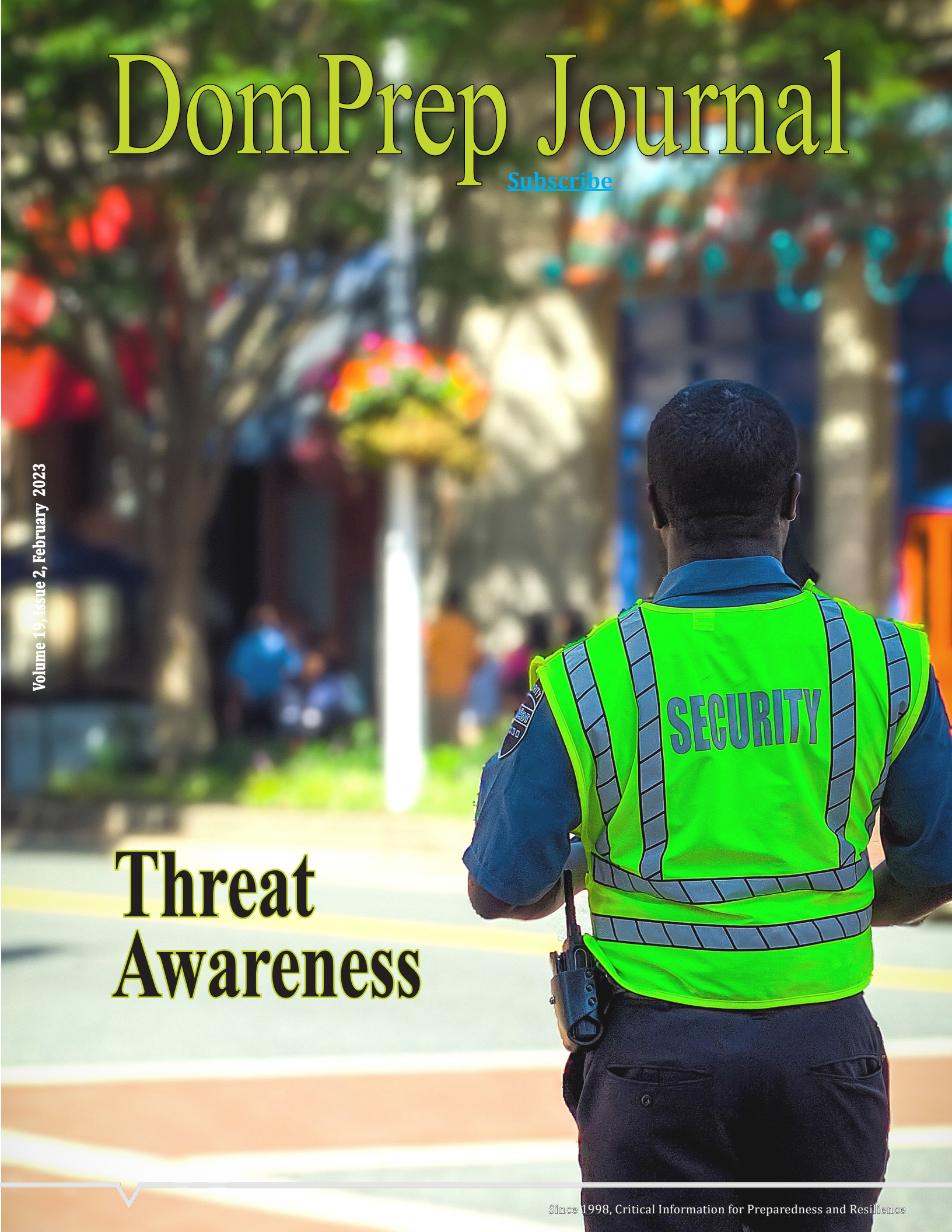
DomPrep Journal

Subscribe

Volume 19, Issue 2, February 2023



Threat Awareness

JOINT CIVIL & DoD CBRN

Symposium and Technology Showcase

March 15-16, 2023 I National Harbor, MD

2023 Speakers Include:

HON Deborah Rosenblum
Assistant Secretary of Defense for Nuclear, Chemical, and Biological Defense Programs
DoD

HON Corey Hinderstein
Principal Associate Administrator for Defense Nonproliferation
NNSA

Gary Rasicot
Acting Assistant Secretary for Countering Weapons of Mass Destruction
DHS

Michael Bailey, SES
Acting Director,
DEVCOM Chemical Biological Center

For Event Details & Registration Please Visit: jointcbrn.dsigroup.org

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

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

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.

Featured in This Issue

Pictured on the Cover: Source: Unsplash/pixel7propix

Threat Awareness – Actions Now Mitigate Disasters Later

By Catherine L. Feinman

Reducing or eliminating the long-term risks associated with natural, human-caused, or technological disasters begins with an awareness that specific threats exist. For example, a Chinese spy balloon crossed the United States and was shot down on February 4, 2023. The exact level of threat that it posed and the amount of information it collected are yet to be determined as intelligence agencies continue to gather information and analyze data. However, what makes that flight different than previous ones is that someone was looking for it after changing monitoring strategies and technologies. In this February edition of the *Domestic Preparedness Journal*, the authors share some strategies and technologies they use to identify, respond to, and recover from threats.

Around the world, statistics show that the number of terrorist attacks has increased. However, by examining effective threat assessment and management practices in various countries, communities can enhance their current threat assessment and management programs to counter evolving threats. Political violence, civil unrest, and mass demonstrations are also rising in many countries. Law enforcement agencies are considering new approaches to address these growing threats, including de-escalation and intervention techniques. Although peaceful protests can escalate to civil disobedience and rioting, U.S. law enforcement and other public safety agencies must be able to recognize the difference and balance their duties of protecting their communities while not infringing on citizens' First Amendment Rights.

At the local and state levels, many communities have been affected by at least one natural disaster in recent years. How leaders handle those events determines how resilient their communities will be for the next. For example, in one state, they adapted their recovery strategy for a first-of-its-kind winter storm event based on established plans for recurring events. In another, they developed a new way to manage recurring hurricane events to ensure that the foundation for business regrowth afterward is stronger than before the storm.

Regardless of the type of incident, technology is a crucial component of emergency response, recovery, and resilience. As such, agencies and organizations must have protections and redundancies in place to ensure the continuity of operations and the continuity of government during a crisis. Organizational leadership should have technological strategies that enable leaders to invest in and implement changes as needed. Many incidents are complex and require innovative solutions to meet the challenges of the evolving threat environment. However, even technology meant to work in a disaster can sometimes fail, so there also needs to be a backup plan. Leaders must be prepared to use their Plan B, Plan C, Plan D, or beyond, whether for the communications systems or other critical emergency response functions. The authors in this issue share a lot of recommendations to consider.

Threat Assessment and Management: Practices Across the World

By Carl Amritt, Eliot Bradshaw & Alyssa Schulenberg



The ever-evolving threat of terrorism continues to impact cities around the world. The Global Terrorism Index shows that in 2021, the number of attacks increased from the previous year by 17 percent to 5,226. As actors adapt and change their tactics and techniques, cities must develop new capabilities to counter these threats. Formalizing threat assessment and management programs can be an effective tool for identifying, gathering, assessing, and responding to risks of targeted violence and terrorism within communities.

Cities experience increasingly diverse and frequent threats targeting people, groups, and public places. The threat of extremism continues to rise; of particular concern are racially or ethnically motivated violent extremism and anti-government extremism, such as militia groups and sovereign citizens interested in plotting attacks against government, racial, religious, and political targets. To address risks of violence, cities may utilize the practices of threat assessment and management to combat targeted violence and terrorism in communities.

This article summarizes a report prepared for the Counter Terrorism Preparedness Network and explores notable global practices to help cities develop or enhance their threat assessment and management programs. The sample included 61 organizations from 50 cities across 11 countries: Austria, Canada, Finland, Germany, South Africa, Spain, Sweden, Switzerland, the Netherlands, the United Kingdom, and the United States. The study used quantitative survey data and qualitative information from interviews with subject matter experts within the field. The survey was disseminated through field-specific entities, including professional associations, professional communities of practice, and international and local intelligence networks.

What Is Threat Assessment?

Establishing a common lexicon is important for building a community of practice and a measurable and replicable program. Threat assessment and management are two functions of a systematic process to evaluate concerning behavioral and thought patterns and determine the context, circumstances, and capability surrounding potential threats. Formalizing threat assessment and management programs can help identify, gather, assess, and respond to risks of violence and extremism. Threat assessments allow cities to move from offender profiling to an evidence-based approach that considers the totality of circumstances. For example, the September 11 attacks (9/11) and Sandy Hook School Shooting both had observable criminal activity or behavioral indicators that, if identified, reported, and acted on appropriately, could have prevented the attacks.

Threat assessments aim to prove the credibility, seriousness, and probability of a potential threat by using facts systematically. These assessments blend information collection and analysis with published research and practitioner experience. They also focus on a person's patterns of behavior and thinking to determine whether, and to what extent, a person of concern is moving toward an attack. Behavioral indicators like leakage, novel aggression, and fixation can indicate that a person is on the pathway to violence. The assessment also considers the context and circumstances – and the interactions between the person of concern, potential targets, and environmental/situational factors – that may influence risk. The companion practice succeeding threat assessment is threat management.

Formalizing threat assessment and management programs helps to identify, gather, assess, and respond to risks of violence and terrorism within communities.

Threat management involves continuously evaluating, managing, and mitigating the risk of harm after identifying a person of concern. Through a coordinated plan of interventions based on current information, threat management is designed to reduce the risk of violence at that time. It all depends on what life stressors (e.g., home and family life, religion or ideology, finances, and workplaces) the person is feeling pressure from and trying to reduce that stress and the associated risk.

The public health approach is a science-based technique that relies on cooperation between diverse disciplines such as health, social services, law enforcement, and correctional services to address underlying factors to increase a person's likelihood of committing an act of violence:

- Primary prevention – approaches aimed at preventing violence before it occurs, such as job programs or bystander awareness;
- Secondary prevention – approaches that focus on the more immediate responses to violence, such as de-radicalization programs or support groups; and
- Tertiary prevention – approaches that focus on long-term care in the wake of violence, such as rehabilitation and reintegration, and attempts to lessen trauma or reduce the long-term disability associated with violence.

The following is an example of threat assessment and management in action:

> *A 2018 federal terrorism investigation involving a 22-year-old male subject with social media posts in support of ISIS, used a local Crisis Intervention Team (CIT) in parallel with the investigation to assess the subject's mental health needs based on a suspected, unidentified mental disorder. The local [Joint Terrorism Task Force] used mental health professionals and other community stakeholders, in conjunction with the CIT and [FBI's Behavioral Threat Assessment Center], to conduct a threat assessment and implement a long-term threat mitigation plan that ensured psychiatric treatment and medication compliance were mandated as conditions of the subject's three-year supervised release.*

Notable Practices

Approaches vary by context. In addition, the feasibility of adopting or expanding threat assessment and management programs rests on the resources and priorities of the city and partner organizations. Based on the 61 organizations in the study sample, nine notable practices emerged.

Approaches vary by context. In addition, the feasibility of adopting or expanding threat assessment and management programs rests on the resources and priorities of the city and partner organizations. Based on the 61 organizations in the study sample, nine notable practices emerged.

Establishing a multidisciplinary team – A multidisciplinary team is central to the public health approach and will enable a well-rounded perspective and effective risk-mitigation strategy development and implementation. Threat assessment and management teams are strengthened through the ability to draw upon multiple perspectives and resources. Most (68.3%, n=43) survey respondents belong to multidisciplinary teams. Of those with only one discipline, 45% (n=9) are law enforcement. While law enforcement serves as a key partner in the threat assessment and management process, consider including mental health, social services, and legal professionals.

Adopting a holistic view – A holistic view enables threat assessment and management teams to consider risk factors, situations, environments, and contexts when evaluating the threat level. By understanding the person's baseline, cities can distinguish deviations from the baseline, identify escalation, and more accurately determine a management and intervention plan best suited to the person.

Developing and adopting a shared language – Cities should consider developing and adopting a language that clearly describes the program goals, minimizes fear and bias, and educates the public on how to utilize its services to foster relationships on transparency and stewardship. When possible, use language and communication mediums (e.g., radio, television, print, and social media) most frequently used in that community to increase understanding and reach.

Performing threat management – Threat assessment achieves little if action is not taken to manage the threat once it is identified. Survey respondents indicated the average number of threats reported annually ranges from 1 to over 500, and the number of cases actively investigated and assessed also ranges widely depending on imminence. Cities should consider following their threat assessments with long-term threat management to reduce the risk of violence from the person of concern. While this practice requires a coordinated plan, continuous monitoring, and implementation of direct or indirect interventions, it is specifically designed to reduce the risk of violence in the given context.

Upholding privacy, civil rights, and civil liberties – The protection of privacy, civil rights, and civil liberties is paramount in the threat assessment space, given that there is not always a nexus to a crime. Safeguarding related protected and sensitive information, especially for juveniles, should be discussed early in team development, ideally with a legal professional.

Applying and layering different types of prevention and intervention strategies – No single method can address and reduce violence alone. Primary prevention strategies like legislation, awareness campaigns, and community training, and secondary prevention strategies like stable housing, mental health counseling, and protective orders are favored globally. However, adding tertiary prevention strategies like victim services, support groups, and restorative justice programs can garner valuable results. Applying layered prevention strategies allows cities to create cascading safety nets and points of intervention for persons of concern before violence occurs. Beyond prevention efforts, local community actions can be particularly effective in bringing about change. Cities should consider what data and resources are needed to inform each strategy and to tailor interventions to fit the needs of the person and community.

Measuring success through data – Measuring the success of targeted violence and terrorism prevention is a challenge. Community surveys where threat assessments are conducted can demonstrate changes in risk level for a person following threat mitigation. Keeping metrics on segments of cases displays a better picture of how a threat assessment and management team's mitigation techniques and methods impact a situation versus comparing before and after a case. For example, if a person comes to the attention of a team as low risk, soon escalates to high and over time is reduced back to low, a before and after will not show change. However, examining that person's path over several identified case segments would highlight the team's work. Finally, tracking the number of reports, tips, and referrals can show the need in a community.


Source: IStock/claudiodivizia

Establishing mechanisms to enhance information sharing – Sharing timely and accurate information is critical to developing threat assessment and management plans. Survey respondents indicated information sharing as a "greatest strength" but also a significant limitation in threat assessment activities. Different city agencies and departments may hold information that can help provide a holistic view of the subject of concern and what resources and services they may require. Health records can illustrate a mental illness diagnosis, and law enforcement records can describe criminal history. However, these records are protected information and can be shared only under certain conditions. Cities may consider legislation to provide threat assessment and management teams with the authority to bypass legal barriers to sharing information.

Lowering the barriers to reporting – People may not be inclined to report potential threats for various reasons. Those barriers may be: emotional, especially if the person

of concern is a loved one; physical, lacking access to a responsible party or system where they can safely and reliably report; or due to a lack of knowledge about available resources. These barriers can be lowered by training the public on reporting methods and threat assessment structures and processes, like the way the "See Something, Say Something" campaign increased public awareness. Socializing threat assessment and management efforts to bring support and resources to those that may not otherwise have access to them can empower community members to uplift those in need.

Outlook

Cities remain attractive targets for targeted violence and terrorism, considering their population density, monuments of significance, and critical infrastructure. These threats must be prevented and mitigated by evidence-based approaches and strategies that further the city's homeland security mission and the safety of the public. Threat assessment and management have long served as an effective method of identifying, gathering, assessing, prioritizing, and responding to various threats.

This article explored the structures, methodologies, and notable practices across different countries to assist cities in developing or enhancing their threat assessment and management program. Through a systematic analysis, one thing is clear – to effectively prevent and mitigate threats, cities must utilize multidisciplinary stakeholders. Bringing these stakeholders together moves professionals closer to having a shared language, which decreases the chances of miscommunication and facilitates collaboration.

No one strategy can prevent violence either. The most successful threat assessment and management programs require a multi-level intervention at the individual, community, and societal levels through the three prevention strategies. To provide these multi-level interventions, cities must develop a strategy to engage the public through education, awareness, and public reporting. This work can be accomplished by building trust with communities and relationships across city government grounded in protecting privacy, civil rights, and civil liberties principles.

Carl Amritt serves as the program manager for the Threat Assessment Center at the Fusion Center within the District of Columbia Homeland Security and Emergency Management Agency (DC HSEMA). In this role, he manages a multidisciplinary threat assessment and management team committed to preventing targeted violence to enhance and community safety and well-being. Before joining DC HSEMA, he served as a senior policy analyst at the National Governors Association, the assistant director of global safety at American University, and held various roles in American University's Police Department.

Eliot Bradshaw serves as the collection analyst for the Threat Assessment Center at the Fusion Center within the District of Columbia Homeland Security and Emergency Management Agency (DC HSEMA). In this role, she monitors open-source information for threats to schools in the District of Columbia and publishes a quarterly bulletin sharing threat information and resources with partners. She also works as a trial consultant, using open-source information to help clients form the best possible jury for their desired outcome.

Alyssa Schulenberg formerly served as an investigative analyst assisting in the creation of the Threat Assessment Center at the Fusion Center within the District of Columbia Homeland Security and Emergency Management Agency (DC HSEMA). In this role, she delivered a targeted violence and terrorism prevention training she developed and worked to adapt it for international audiences. Before joining DC HSEMA as part of a Department of Homeland Security Targeted Violence and Terrorism Prevention grant, she was an investigative support specialist at Louisiana State Analytical and Fusion Exchange and served as a mobile operations coordinator for Louisiana State University's (LSU) National Center for Biomedical Research and Training/Academy of Counter-Terrorist Education.

Trends in Political Violence and Mass Demonstrations

By Richard Schoeberl

More than 400 worldwide antigovernment protests have taken place since 2017. According to the Global Peace Index (GPI), the incidents of civil unrest have doubled across the globe over the past decade. Moreover, the 2022 GPI indicates the world has become "less peaceful for the eleventh time in the last 14 years." By 2020, antigovernment protests (defined as an organized public demonstration of public disapproval of some law, policy, idea, state of affairs, action, or inaction and opposing or resisting governmental policies) rose in North America by nearly 380% compared to a decade earlier, expanding each year at a rate of 17%, which is more than 48% higher than the world average. After reviewing societal safety and security, ongoing domestic and international conflict, and militarization, the 2022 GPI determined that the United States is one of 71 countries that was less peaceful than the previous year. Based on a 1-5 scale, with 5 representing a high degree of violence in a country, the U.S. scored 2.44, which places it in the bottom 25%, with a rank of #129 out of 168 countries.

Reviewing Motivating Factors – Protests Over Time

Since America's early beginnings, people have used protests and demonstrations to advocate for change, starting with the Boston Tea Party in 1773. The right to demonstrate peacefully is at the foundation of democracy. The First Amendment protects the right to assemble and the right to express views through *peaceful* protest. However, it is becoming increasingly more difficult to determine when nonviolent demonstrations may quickly escalate into violent protests. Rioting and violent civil unrest are hardly the best solutions for situations perceived as injustice. However, thousands do not gather in protest for no apparent reason, which was true during the Boston Tea Party in 1773, the 2020 George Floyd Protests, and the 2020 election (including the January 6th attack on the U.S. Capitol).

In recent years, more threats, more armed protests, and more people have resorted to violence against the government. Polarizing events have ignited underlying tensions within American democracy. A study by the Institute for Economics and Peace published in 2020 concluded that roughly 40% of Republicans and Democrats consider political violence somewhat justifiable. Conversely, a joint university study in 2022 concluded that nearly one-quarter of the U.S. population feels it is justified to engage in violent protests against the government – almost 1 in 4 Americans hold an extreme opinion and support violence. This could prove to be a difficult task for law enforcement attempting to identify the unknown triggers that make protestors turn operational, moving from extreme opinion to extreme action, thrusting a peaceful demonstration into a violent protest.

People demonstrate for a myriad of circumstances, including grievances, efficacy, identity, emotions, and social embeddedness, according to a 2013 study by the International Sociological Association. If viewed through the lens of social identity theory, people

separate the movement into *us* versus *them*. For the movement to recruit widespread support for their cause, then the movement is more than likely to be successful if they encourage feelings of shared identity with observers. However, extreme protest behaviors can provoke damaging views of movements because they diminish identification with the actual movement and instead place significant emphasis on the violence of the action itself. While participating in radical protests, actions may help or hurt a movement in certain ways these actions can even undermine widespread support for the movement. More often than not, extreme actions perceived to be immoral can reduce supporters' emotional connection to the movement, this reducing identification with the movement.

Identifying Turning Points – From Peaceful to Violent

Whether a perceived threat from a polarizing incident, or an occupation of public space, demonstrations can quickly jeopardize social order. Because of their role, law enforcement agencies are expected to intercede promptly, ensuring the community's safety and maintaining order. Law enforcement agencies must consider the complexities associated with a proper protest response, like the duality of protecting personal rights guaranteed under the First Amendment while simultaneously ensuring public safety during demonstrations. Sometimes striking the proper balance can prove difficult, particularly since agencies around the U.S. have different levels of familiarity with mass demonstrations and preparedness for such events.

Policing the protests is intrinsically challenging as each mass demonstration has some propensity to evolve into violence. With a society based on group dynamics, peacefully minded protesters may act out violently under certain circumstances. In theory, when group behavior exhibits aggressive tendencies, the larger the organized group, the more propensity for a larger-scale violent eruption. For example, at a football game, patrons typically do not go to a game with the predisposed intention of storming the field and taking down the goalpost. However, it happens many times because of crowd mentality. The contagion theory suggests that crowds employ a "hypnotic influence" on their participants, which results in emotionally and irrationally charged behavior, referred to as *crowd frenzy*.

Sometimes striking the proper law enforcement balance between protecting First Amendment rights and protecting public safety can prove difficult.

Several studies show why demonstrations escalate and become violent and establish early on some of the policing best practices that must be employed in response to organized demonstrations. Certainly, preparedness is paramount, primarily because the environment at mass demonstrations can escalate quickly and get out of control. A Columbia Law School study determined that when law enforcement is viewed as performing procedurally and professionally, protesters are more likely to consider law enforcement as lawful sources of authority and thus exhibit peaceful, lawful behavior. Conversely, when law enforcement is viewed as employing its authority aggressively and oppressively, conflict is more likely to happen with demonstrators.

Preventing Escalation – Facilitation vs. Control

People who are already demonstrating to express a grievance could intensify that sense of grievance and direct it toward the officers who are there to provide public order and safety. A way to diminish this so-called transfer of grievance is to permit demonstrators a chance to express themselves peacefully. Law enforcement can enhance interactions between themselves and demonstrators and lessen the possibility of conflict if it is managed from the perspective of "how to facilitate" versus "how to control" the demonstration.

Preparing for protests ahead of time can be particularly important for law enforcement. Officers must understand their fundamental role before responding and handle their duties in a manner that affords First Amendment rights while protecting public safety. A clear understanding and direction for protecting those rights during demonstrations can benefit the law enforcement community and reduce friction at the event. To every extent, law enforcement should engage in cooperative and strategic planning with community members before, during, and after peaceful demonstrations.

Preparing agencies before a demonstration with raw intelligence is critical. Law enforcement should seek to inform themselves about the general culture and conduct of the protesters. Agencies should gather as much information on the underlying intent of those demonstrating. The information regarding the protest culture of the group then can be an assessment of how to design the operation to facilitate the demonstrators' legitimate intentions while preventing their non-legitimate ones. Analyzing and gathering intelligence on social media platforms the group uses regularly can give law enforcement a better look into not only the intentions of the demonstration but the hostility that may be building up before the event itself. For example, on far-right social media platforms, protesters gave directions on which streets are safe to avoid interaction with the police, and which tools to bring to help pry open doors for the January 6, 2021, Capitol riots. Several dozen social media posts even discussed carrying guns into the halls of Congress.

Consistent psychological research has shown that individual behavior can shift solely on the clothes one wears. Police departments equipping officers in tactical gear can likely affect officer tendencies as well as the point of view for the protesters who perceived tactical gear as intimidating, a tactical mismatch, which is likely to influence escalation that could potentially lead to further unrest. Law enforcement should generally be dressed

in non-tactical uniforms and have an open dialogue to keep the lines of communication open and prevent escalating conflict with the demonstrators unless clear intentions are known ahead of time to deploy officers in riot control gear. Because violence often begets violence, agencies should proportionately adjust police response to the crowd's actions. This measure would evade a snowballing effect of tension that may already be embedded by intensifying and employing more force or equipment than needed to control the current situation. Agencies' demeanor and training will also affect how police are perceived by those demonstrating. Demonstrators are more likely to cooperate when they perceive law enforcement as fair, respectful, and restrained in their interactions and responses to the crowd.

If the possibility of violence is perceived by law enforcement agencies ahead of time, they should adopt a "graded response," where officers in riot control gear can be deployed quickly but staged out of plain view. A mass demonstration observing police officers in riot control gear in plain view of a nonviolent group is an approach that may encourage the very conflict police initially intended to avert.

Recommending Action – Communicate, Train & Review

Effective protest policing starts with effective communication. Communication can be the most important method by which law enforcement can determine the intentions of demonstration coordinators and how best law enforcement can facilitate these goals. It can also be a great way for law enforcement to understand potential public safety concerns better and attempt to counteract them together with organizers and demonstrators. For example, in January 2023, police communicated with Tyre Nichols' family to preserve order and prevent conflict. Nichols' mother urged Americans to "protest in peace" as the Memphis Police Department prepared to release the bodycam footage showing the law enforcement interaction that led to her 29-year-old son's death.

Following years of unparalleled violence that occurred in many cities across America, the Police Executive Research Forum (PERF) released a report in February 2022 providing several recommendations that law enforcement agencies can utilize to plan for and respond to demonstrations or protests in the communities they protect. PERF's nine major recommendations from that report include:

- Invite leaders from the community to participate in agency meetings and trainings about police response to demonstrations. These events better educate all involved on what reactions to expect from both sides and better prepare for those actions.
- Communicate and ensure everyone in the agency has a clear grasp of the goals of policing mass demonstrations. This understanding should include the use of deadly force policy and specific tactics, actions, and tools that appropriately respond to various demonstrator behaviors.
- Train officers and supervisors adequately. Do not lower standards to hire more officers.
- Thoroughly evaluate every type of less-than-lethal device available during the demonstration, its capabilities and limitations, and any known risks it potentially poses to those in its path.

- Warn crowds before deploying less-than-lethal force.
- Avoid mass arrests and using force, if possible. They could create the feeling that law enforcement is prohibiting and punishing First Amendment rights. Therefore, agencies should clearly communicate the thresholds for arrest and warn demonstrators when they violate the law and are subject to arrest.
- Prepare and activate mutual aid agreements. Communicate specific and clear response protocols, particularly when officers from supporting agencies are needed to adhere to the policies of the host agency.
- Protect officers' security and well-being. Establish policies that help prevent fatigue and poor decision-making resulting from sustained exposure to the stress of policing a mass protest.
- Ensure vigorous review of the police response to each demonstration.

Of the above recommendations, law enforcement training is paramount in preparing officers to respond to mass demonstrations, particularly in areas around the laws, policies, and regulations regarding public demonstrations, freedom of speech, and use of force. Often, the use of force employed by police officers may culminate in police repression or violence by taking the form of police charges against demonstrators. Soft-skill approaches like de-escalation and peer intervention should be applied, and training considered for officers. Like active shooter and other trainings, mass demonstration exercises should encourage multiagency participation to foster a mutual understanding between the agencies involved in the community.

The U.S. government has failed to create a methodical unified response or guidance to the mushrooming of protests that continue across America. Leadership has treated each as an irregularity rather than a larger trend, failing to scale up capacity to respond to mass demonstrations uniformly. The rise of global mass protests has been unprecedented in frequency of occurrence and in magnitude.

According to a 2020 Center for Strategic and International Studies study, the assessment of the factors suggests the trend of mass protests will persist, and the number and intensity of these events will rise. Higher standards, better training, and coordinated exercises within the law enforcement community are undoubtedly needed. This a difficult challenge in an era of calls for police accountability and reform, which have left departments across America battling to keep the current officers and attract new ones.

Richard Schoeberl, Ph.D., has over 25 years of experience, including the Federal Bureau of Investigation (FBI) and the National Counterterrorism Center (NCTC). He served in various positions throughout his career, ranging from a supervisory special agent at the FBI's headquarters in Washington, D.C., to acting unit chief of the International Terrorism Operations Section at the NCTC. In addition to the FBI and NCTC, he is an author of numerous articles on terrorism and security and has served as a media contributor for Fox News, CNN, PBS, NPR, Al-Jazeera Television, Al Arabiva Television, and Al Hurra. He works with the international nonprofit organization Hope for Justice, combatting human trafficking, and additionally serves as a professor of Homeland Security at The University of Tennessee Southern. He also is an advisor to the Domestic Preparedness Journal.

Protests: Balancing First Amendment Rights and Public Safety

By Matthew Loeslie

In today's society, peaceful protests can occasionally escalate into unlawful rioting. The behavior of those involved in a demonstration or public gathering can vary greatly. This behavior includes:

- Peaceful protests, actions, and speech that are lawful and protected by the Constitution;
- Civil disobedience, which typically involves minor criminal acts; and
- Rioting associated with behaviors such as collective violence, looting, arson, destruction of property, and other unlawful behaviors.

Complicating matters, it is possible for all these behaviors to occur during the same event. However, rioting is different from peaceful protests or civil disobedience. For example, not long ago in Atlanta, Georgia, a peaceful protest quickly changed to rioting when people began throwing bricks at buildings and setting fire to police cruisers resulting in the arrests of several people. Often, when a peaceful protest escalates into unlawful riots, there is a specific trigger and a tipping point that gains widespread media attention.

Consequently, the use of open-source intelligence (OSINT) and social media can also play an important role in obtaining information in advance of protests, especially those with a history of violence. By monitoring social media and other open sources, authorities can gather valuable intelligence and make informed decisions about their response. OSINT can provide insight into the motives, objectives, and tactics of protest groups, enabling public safety planners to better prepare for and respond to potential threats. By leveraging the power of technology, OSINT can be a valuable tool in helping to maintain peace and prevent loss of life and property during protests.

Multi-Agency Command Center (MACC)

A Multi-Agency Command Center (MACC) is a centralized control center that brings together multiple agencies to manage and respond to incidents and potential threats. The financing for MACCs can come from different sources like federal, state, and local government agencies, as well as private sector organizations. However, the funding and jurisdiction for each MACC can differ based on the jurisdiction's specific needs and resources. The National Incident Management System (NIMS), which aims to manage incidents in a consistent and coordinated manner, plays a role in establishing formal MACCs and provides a standardized structure for incident management across all levels of government. In other words, MACCs are established following NIMS principles and guidelines. Moreover, the National Special

Security Event planning structure outlined in the 2013 Presidential Policy Directive 22 (PPD 22) further supports establishing a MACC for large-scale events, such as major sporting events, national political conventions, and other high-profile gatherings.

The authority for setting up MACCs also varies by jurisdiction – sometimes established by a local government and sometimes at the state or federal level. The specific authority for a MACC depends on the jurisdiction's legal and regulatory framework. In each case, the MACC brings together various agencies to manage and respond to incidents, including but not limited to:

- Law enforcement (local, state, federal)
- Fire department
- Emergency medical services
- Transportation department(s)
- Mayor's office
- State
- Federal
- Public relations
- National Guard

The primary goal of a MACC is to provide a unified and coordinated response to potential threats and incidents that ensures the safety and well-being of all those involved.

A (MACC) should be activated – with the goal of maintaining peace and preventing the loss of life and property – when protests have the potential to escalate into large-scale riots. For instance, the Minnesota MAAC was activated during the civil unrest in response to the murder of George Floyd by a Minneapolis police officer in 2020. A noteworthy external review of the Minnesota response in 2022 asserted that the setup and coordination of the MACC started too late. In recent years, there has been an increase in high-profile rioting and civil unrest in cities across the United States and the world. The increase has been attributed to factors such as government corruption, social and economic issues, police brutality, and political polarization. The likelihood of future riots persists, making it imperative for jurisdictions to be thoroughly prepared.

Importantly, members of the MACC come from various disciplines with distinct roles and responsibilities in responding to civil unrest. For instance, the transportation department helps with road closures, the fire department extinguishes fires, emergency medical services provide medical assistance to injured individuals, and law enforcement addresses the unrest and makes arrests when necessary. However, these various disciplines represented in the MACC may not fully understand the intricate balance that law enforcement must strike between upholding First Amendment rights and preserving public order. In addition, when a formal MACC is not an option, due to financial resources or jurisdictional complications such as the size of the locality, it is important to consider alternative options, such as a crisis command center. This type of center can provide similar benefits, such as effective coordination, information sharing, and communication, even in smaller or less resourced communities.

The Complexity of Responding to Protests and Riots

The First Amendment in the Bill of Rights clearly articulates, "Congress shall make no law…abridging freedom of speech." While the words in the founding document are straightforward, it is not surprising that there are legitimate limitations to freedom of speech. For instance, if demonstrators at a public gathering entered occupied buildings and shouted "Fire!" when there was no fire, this would not be considered protected speech and would warrant a police response due to the potential safety hazard it presents.

Law enforcement, though, cannot intervene in most incidents if protesters burn the American flag. The Supreme Court has ruled that flag desecration, whether through burning or other means, is a form of free speech protected by the First Amendment. Flag burning has the potential to elicit a strong reaction from those who hold the national symbol in high regard, leading to potential confrontations with counter-protesters. However, the Supreme Court has determined that the mere outrage of those who disagree with flag burning is insufficient grounds for suppressing speech through police action (Texas v. Johnson, 1989). This highlights the complexity of responding to protests and riots for law enforcement.

Effective communication and strong relationships within the Multi-Agency Command Center are essential to maintain trust and confidence among members.

There is also ongoing debate surrounding the ability of police to protect citizens effectively during riots. In particular, recent laws and regulations limiting police use of force during riots and protests have been established, with some jurisdictions even restricting the use of tear gas, rubber bullets, and other less-lethal weapons. The effectiveness of these laws in protecting citizens during demonstrations remains a topic of heated debate among politicians, police organizations, and activist organizations. Nevertheless, community policing and community relations are essential in preparing for potential threats during a riot, despite the limitations of a jurisdiction's response

abilities. Building strong connections with diverse groups and being knowledgeable about their history, including past instances of violence, helps make informed decisions for effective responses.

Effective Communication & Preparation for Protests

Given the legal complexities surrounding police response to protests and riots, it is crucial for effective communication within the MACC. Effective communication and strong relationships within the group are essential to maintain trust and confidence among members. For instance, if a fire department member thinks that the ignition of a fire and the burning of the flag require a police response, but the police do not act, this could erode trust and cooperation within the team.

Due to the legal complexities surrounding the response to protests and riots, officers might exercise caution in preventing escalation, which could seem unreasonable to some members of the MACC. However, this caution is necessary to protect protesters' First Amendment rights and abide by legal precedents. To effectively address the complexities of responding to public gatherings with the potential to turn into riots, it is crucial for the MACC team to conduct tabletop exercises. Engaging in simulated scenarios through tabletop exercises such as multi-agency-led, senior leadership level, operational level, and functional exercises can help identify, plan for, and address potential public safety concerns that may arise in the future.

Law enforcement and MACC members should have a plan to deal with protests well before a protest begins. The plan and policies should guide law enforcement and MACC members on their respective responsibilities. MACC members should be aware that law enforcement has the additional duty to uphold protestors' constitutional rights and protect others from violence. These dual and sometimes competing roles necessitate that law enforcement and MACC members be trained to recognize First Amendment issues and respond appropriately based on their jurisdiction's laws.

Moreover, law enforcement and MACC members need to be able to communicate with each other about the reasons for various decisions, especially if they seem counterintuitive, such as flag burning. In summary, finding the right balance between the legal requirements of free speech and public safety is a complex and evolving undertaking. Still, it is vital for maintaining order and complying with the law.

Dr. Matthew Loeslie is an Assistant Professor at Minnesota State University, Mankato. He has also held several leadership positions in academia, including academic dean at a community and technical college, program director of the criminal justice program at a state university, and faculty member. Additionally, Matthew has extensive experience in emergency response and training, having served as the training manager for the Minnesota Emergency Response and Industrial Training (MERIT) Center and worked as a police officer and trainer in Minnesota. He holds a Doctor of Criminal Justice from the California University of Pennsylvania, a Master of Arts in Criminal Justice Leadership from Concordia University-St. Paul, and a Bachelor of Science in Sociology from South Dakota State University.

ARTICLES OUT LOUD FOR YOUR BUSY LIFE

Emergency Preparedness Professionals are incredibly busy and often on the road. To give you more opportunities to benefit from the articles in the Journal, you now have access to Articles Out Loud which will be available for a trial period.

You can find our first Article Out Loud on our website under the Podcast channel, or in the iTunes store.

Don't forget about last month's Journal! Click **HERE** to Download it now.

DON'T MISS ANOTHER ISSUE OF THE WEEKLY BRIEF OR DOMESTIC PREPAREDNESS JOURNAL

SUBSCRIBE **HERE**

Winter Storm – Reimagining Recovery Using Support Functions

By Jamie Hannan & Stephanie Wright

In early February 2021, Harris County, Texas, and many other jurisdictions began monitoring a Siberian Air Mass that threatened nearly all of North America. This was the genesis of Winter Storm Uri. In the week preceding the storm's arrival, the Harris County Office of Homeland Security & Emergency Management (HCOHSEM) monitored National Weather Service (NWS) forecasts, sent notifications to the public for them to begin preparation and mitigation, and opened communication with partners in anticipation of a hard freeze lasting multiple days.

In terms familiar to residents of Harris County, County Judge Lina Hidalgo compared the storm to a Category 5 Hurricane at a press conference as a way to succinctly communicate what HCOHSEM and partners were anticipating – loss of power and water and impacts to other infrastructure. Although residents of Harris County – the third largest county in the United States by population, with over 4.7 million residents – are used to preparing for hurricanes, a winter storm of this magnitude was unfamiliar. Preparing for something like this had not been done for many years.

Storm of Historic Proportions

On February 12, HCOHSEM began issuing warnings to help residents and partners prepare for the coming weather. Messages containing reminders about taking care of "the 4Ps: pipes, people, pets, and plants" were sent to county residents. For the first time in its history, NWS issued a Wind Chill Warning for Harris County and the surrounding region to inform residents that "dangerously cold wind chill values were expected or occurring."

Precipitation joined the cold air coming into Southeast Texas, and ice and snow made many roads impassable, causing much of the region to come to a standstill. The statewide power grid struggled, and the Energy Reliability Council of Texas (ERCOT) eventually began rationing power to keep the power grid across the state from collapsing. This led to approximately 1.4 million customers in Harris County with no power, along with a list of cascading impacts to water systems, hospitals, schools, and the broader infrastructure within the county.

Due to the impacts of the storm, Texas Governor Greg Abbott issued a state-level disaster declaration for all 254 counties in Texas and requested assistance from the federal government. In response, President Joseph R. Biden Jr. issued a Major Disaster Declaration for Harris and 107 other Texas counties based on damage data received from those counties. This allowed federal resources to flow into affected areas. Other counties were added later as the extent of the damage became known.

President Joseph R. Biden Jr. and Governor Greg Abbott receive briefings from local and state leaders regarding the impacts of Winter Storm Uri, February 26, 2021 (*Source*: HCOHSEM).

Unprecedented Approach to Recovery for an Unprecedented Storm

Discussions for how to implement the recovery process began before the storm was over. HCOHSEM leadership and the recovery specialist worked together to determine how to approach recovery. They decided to implement the Recovery Support Function (RSF) model as outlined in the National Disaster Recovery Framework created by the Federal Emergency Management Agency.

Winter Storm Uri was the first opportunity for Harris County to implement this recovery model. Previous iterations of recovery involved the HCOHSEM recovery specialist, members of the Planning Section, and office leadership coordinating with other county departments, local jurisdictions, elected officials, non-governmental organizations (NGOs), and business entities in a somewhat ad hoc fashion depending on the disaster. This structure required HCOHSEM to be involved in the day-to-day work of recovery to understand how it was progressing and provide support.

Utilizing RSFs allowed for a more structured approach and model for engaging partners and the whole community in the recovery process compared to a recovery process that generally focused on housing, social services, and public health. It also allowed HCOHSEM to take leadership of the process by being the recovery manager working with RSF leaders, who then worked to carry out the work of recovery through their respective groups.

Once the emergency operations center transitioned into recovery, establishing the RSF structure with partners was one of the first tasks. The RSF process is based on a whole community approach that ensures stakeholders' involvement in each of the RSF areas:

- Economic,
- Community planning and capacity building,
- Health and social services,
- Infrastructure systems,
- Natural and cultural resources, and
- Housing recovery.

As leaders from various NGOs, county agencies, and other entities came together, the work began to identify recovery priorities. The recovery specialist, planning team, and other HCOHSEM support staff helped manage the process.

Recovery Support Function Benefits

The adage "many hands make light work" concisely describes the benefits of the RSF structure. As work began, it became clear that expanding the proverbial recovery tent to include a broad array of partners who fit into the various RSF areas allowed for a wider focus on recovery to support a whole community approach to recovery. The structure lent itself to a more inclusive version of recovery, which allowed for broader engagement with sectors outside of those related to housing, social services, and public health.

Evidence of this inclusivity is found through the learnings in the natural and cultural resources RSF workgroup. Before forming this workgroup, the cultural arts community, which contributes over $1 billion to the local economy ("$579.4 million by nonprofit arts and cultural organizations and an additional $538 million in event-related spending by

Harris County and City of Houston elected leaders update residents on the winter storm and urge residents to make necessary preparations for the arrival of Winter Storm Uri, February 12, 2021 (*Source*: HCOHSEM).

Response partners attend EOC briefing during Winter Storm Uri activation, February 15, 2021 (*Source:* HCOHSEM).

their audiences"), was not directly engaged in recovery conversations. Through this work and their inclusion, HCOHSEM learned more about barriers faced by many artists who are often independent contractors or operate as small businesses. Contractors and small businesses do not have access to the same resources as larger entities. In addition, many members of the broader arts community did not receive recovery support in the past.

HCOHSEM implemented recovery situation reports to help capture new information gained through the process (e.g., like that related to the cultural arts community) and to ensure the expanded work stayed on track. These reports identified the progress of RSF workgroups and their needs, provided updates to county and department leaders, and ensured progress was being made. These situation reports also kept recovery at the forefront after the ice thawed and the power was restored.

Other entities considering adopting RSFs may want to evaluate how they can adapt the National Disaster Recovery Framework structure. Doing this in advance will allow for a smoother transition into the recovery process when it is needed. Utilizing the RSF structure allowed Harris County to identify gaps in planning and start work to adjust plans to prevent barriers to accessing mitigation and resiliency funds. This work with the cultural arts community brought this to the forefront. The Houston Arts Alliance, a local NGO, is now working with the community to map cultural assets across the county and letting the community decide what is an asset to ensure what is important is included. HCOHSEM can then help mitigate, protect, and restore those assets.

Data collection and sharing processes were revamped during this incident as well. Generally, windshield assessments are conducted to understand the impacts of disasters throughout the county. This storm was different in that most of the damage happened to the interior of homes through burst pipes. In response, Harris County, city, state, and several NGOs created surveys to identify residential damage. Not only did this duplicate the effort and prevent the formation of an accurate common operation picture, but it also asked residents to enter the same information into multiple unrelated surveys. In response to this, Harris County entered into an agreement with the Kinder Institute at Rice University to have them assist in data management and data cleanup. In addition, to prevent future data collection issues, Harris County, Harris County Long-Term Recovery Committee, Texas Gulf Coast Regional Voluntary Organizations Active in Disasters, Houston, and an NGO called Connective developed a Damage Assessment Survey that will be sent to residents after a disaster. This single survey will allow for a common operating picture, prevent residents from filling out multiple surveys, and can be easily adjusted for whichever disaster strikes.

Two key lessons: Critical information must be disseminated using familiar terminology, and recovery is a team effort that begins before an event has ended.

Ultimately, the success of the Recovery RSF structure is dependent on building and maintaining effective partnerships across levels of government and the private sector. With engaged partners, an emergency management agency can expand its capacity without increasing its budget or staffing. In the end, long-term recovery efforts are easier to manage and nimbler. For elected officials, community leaders, and other stakeholders, the level of coordination inherent in the system provides for a better common operating picture. For residents and impacted entities, better access to recovery resources leads to a faster, more equitable recovery.

Jamie Hannan, MAT, MPP, is the innovation research analyst for the Harris County Office of Homeland Security and Emergency Management (HCOHSEM) in Harris County, TX. He joined the team in 2021 after working in the non-profit and education sectors for a decade. In his role at HCOHSEM, he works across sections to highlight best practices and innovative processes, serves as a policy analyst, and acts as a liaison to Commissioners Court, the local governing body for Harris County. He holds a Bachelor of Arts in History and Master of Arts in Teaching from Austin College in Sherman, TX, and a Master of Public Policy from the Hobby School of Public Affairs at the University of Houston.

Stephanie Wright started in emergency management in 2011 when she was appointed Deputy Director of the Secretary of the Senate's Emergency Operations Center (EOC). She helped to run the EOC and establish an alternate Senate Chamber during the 2011 earthquake. In 2012, she was promoted to continuity of operations coordinator and director of the EOC, where she managed continuity of operations planning and continuity of government plans for the secretary of the Senate and its 26 departments. In this capacity, she activated the EOC for numerous special events, including State of the Unions, Joint Sessions of Congress, the 2013 Inauguration, and the 2015 Papal visit. After moving to Texas, she worked as a disaster/outreach coordinator for the United Way of Greater Houston and assisted with community recovery efforts for the Memorial Day flood, Tax Day flood, and Hurricane Harvey. In 2019, she transitioned to the Harris County Office of Homeland Security and Emergency Management and currently serves as the recovery specialist. Most recently, she managed the Winter Storm Uri recovery operations. In addition to her work as a recovery specialist, she served as the Chair of the Texas Gulf Coast Regional Voluntary Organizations Active in Disaster (VOAD) and is currently co-facilitating the Harris County Long-Term Recovery Committee.

2023 ANNUAL Fire Schools

TEEX Brayton Fire Training Field® – College Station, TX

Offering Training Solutions to Handle Emergency Situations

JULY 16 –21
INDUSTRIAL SCHOOL

JULY 23 –28
MUNICIPAL SCHOOL

AUGUST 6 –11
SPANISH SCHOOL
SACS Group
Cartagena, Colombia

Course Details and Registration Information:

TEEX.ORG/ANNUALSCHOOLS

Texas A&M Engineering TEEX® Extension Service

Questions? 866-878-8900

E23.1063.02

PACEing a Communications Resilience Plan

By Charles J. Guddemi

On the night of January 10, 2023, the Federal Aviation Administration's Notice to Air Missions (NOTAM) system, which communicates real-time hazards to pilots and airports, failed for an unknown reason. The backup communications provided critical updates to pilots but were insufficient to sustain operations. By morning, operations had to cease for two hours while they located and fixed the problem. In the meantime, 1,300 flights were canceled, and 10,000 others were delayed across the United States. Communication failures cannot always be avoided, but organizations must plan what to do when they occur.

Most organizations have a daily operational plan for their communications that works most of the time. When the power goes out or a system goes down, many have a backup plan to get by for the short term until the problem is resolved. Unfortunately, this is where their plans often end. Occasionally, operations slow or even stop while people wait for instructions on what to do next. Military leaders have long known that operations cannot cease during an emergency for any reason, so they use a primary, alternate, contingency, emergency (known as P.A.C.E. or PACE) plan for critical operational planning tasks.

The District of Columbia Homeland Security and Emergency Management Agency (HSEMA), Office of the Statewide Interoperability Coordinator (SWIC), decided to introduce the concept to organizations in the National Capital Region. However, despite an array of business continuity training programs across the country and the Federal Emergency Management Agency's vast number of courses through its Emergency Management Institute, courses that focused on building PACE plans for civilians were not readily available. To fill this gap, HSEMA reached out to the Emergency Communications Division (ECD) of the Cybersecurity & Infrastructure Security Agency (CISA), which developed a new course and curriculum. CISA conducted its pilot at HSEMA in Washington, D.C., in August 2022. With feedback from the pilot, the course was finalized and opened to organizations throughout the region, with two classes held on January 19 and one on January 20, 2023. As a result of this initial class, ECD is looking to revise this course in 2023 to be rolled out to agencies and organizations nationwide.

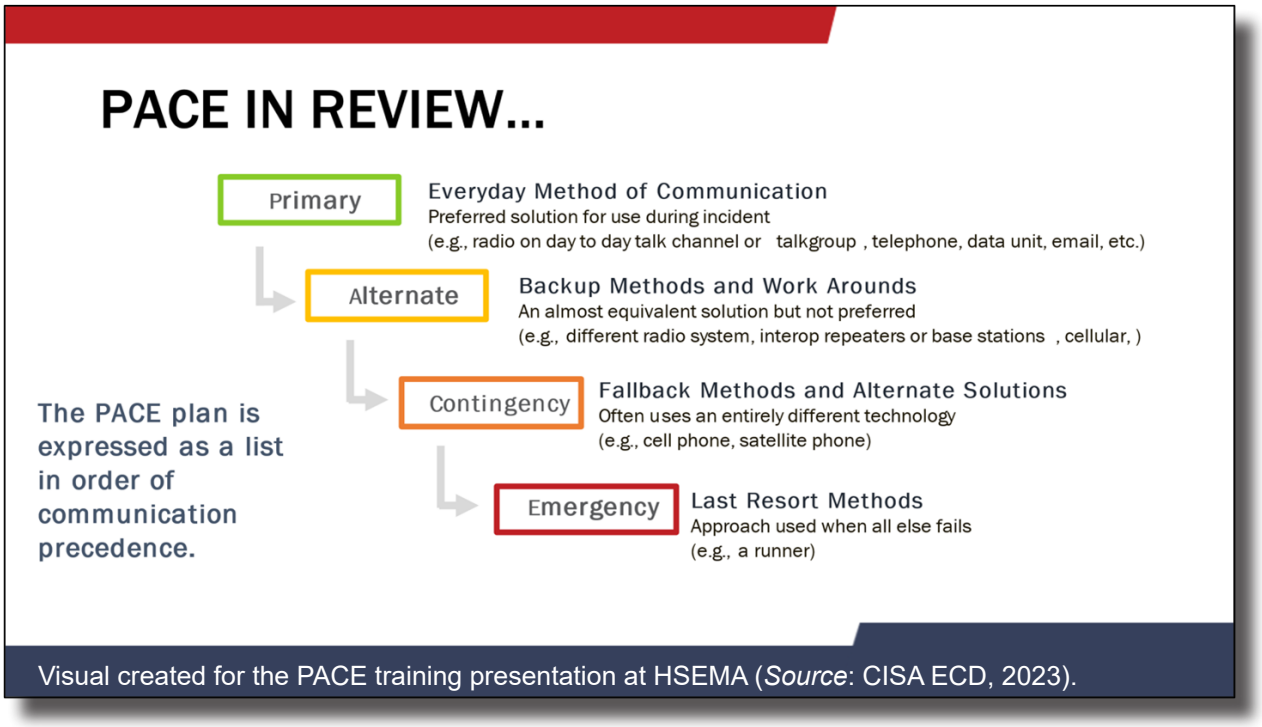
Understanding PACE

Unlike many courses, PACE shows trainees how to teach themselves. By understanding what this type of plan is, the communication methods available, and the many causes of system failures, participants can build a pathway to transfer information under any circumstances. As such, PACE's four-step format should be a component of any communications, continuity of operations, or business continuity plan:

- Primary – This is the go-to method that operations personnel use as a daily solution (e.g., radios for day-to-day operations).
- Alternate – This is a backup method that is not preferred but may serve as a

good workaround until the problem is resolved (e.g., a different radio system).

- Contingency – This is a fallback method that uses totally different technology, systems, etc. (e.g., satellite phones).
- Emergency – This is the last-resort method when the others fail (e.g., a runner).



Visual created for the PACE training presentation at HSEMA (*Source*: CISA ECD, 2023).

To better understand why a simple backup plan is insufficient, consider how CISA describes the communications ecosystem. This ecosystem is bigger than the planning organization, first responder groups, and the boots on the ground. It also includes connections between these key community stakeholders and more:

- *Public to governmen*t – Includes 911 (to include Next Generation 911), 311, agency applications that allow feedback, social media, email, landlines, and cellphones;
- *Government to government* – Includes land mobile radio systems (individual and shared agency), landline phones, cellphones, satellite phone and data systems, alerting applications, special telephone and data connections, email, computer-aided dispatch;
- *Government to public* – Includes government alerting applications, emergency broadcasting systems, broadcast news media, web pages, email, warning sirens, social media, and in-person outreach; and
- *Public to public* – Includes cellphones, landlines, emails, social networking, faith-based organizations, schools, youth sports leagues, and neighborhood organizations.

There need to be multiple pathways for each of the above connections (and other applicable connections in a particular area) to ensure daily operability and interoperability. Of course, everyone involved in the ecosystem should also be planning for these contingencies (public, government, industry, media, non-governmental organizations, and communication companies).

Developing the Plan

System failures can occur for numerous reasons, from user errors to intentional attacks. Identifying and reporting the reasons for and locations of failures are critical for pinpointing the problems and regaining normal operations. Regardless of the type of failure, even small details during and after the event are crucial and make a big difference in getting the information rapidly to the right people to resolve the issue as soon as possible.

Be aware of what is occurring behind the scenes to consider all possible failure points and alternatives. This knowledge helps identify resources that can meet the needs and point out the potential limitations of each resource to determine the best PACE plan methods. When the plan is implemented, though, expectations must be realistic. This means that what may be unacceptable during normal operations may become acceptable under the C (Contingency) or E (Emergency) steps in this plan. So, keep that in mind when identifying the various options.

In addition to direct communications, a PACE plan for communications also includes data and other daily operations. Consider what other jobs might not be possible if communications systems were to go down. For example, suppose security operations at a large sporting venue experience a communications failure. In that case, that failure may

also affect the ticket scanners where thousands of people are waiting to enter the stadium. Sometimes, these jobs involve life-saving field operations such as law enforcement, emergency medical services, and firefighting when dispatch centers, radio systems, etc. are affected. PACE plans consider these various connections.

Once the PACE plan is complete, all users must learn and understand the plans. To do this, they should have opportunities to train and exercise to ensure they know how to identify when to change from one method to the next. Developers must also regularly review and revise the plan as systems and operations change. Organizations can better mitigate operational disruptions by keeping the plan simple and managing expectations.

Six key questions to ask when a communications failure occurs include:

- What systems, operations, activities, etc. are impacted?
- Who in the ecosystem is affected (public, government)?
- Which resources and methods are affected, and which are available?
- Why are they impacted (identifying the cause can facilitate the solution)?
- Is it time to implement the PACE plan, or is it time to move to the next step in the PACE plan?

If the communications failure hinders necessary public safety or public service activities or puts lives or property in danger, the answer to the last question is yes. Starting with the primary method, work through the alternate, contingency, and emergency stages as needed for each situation. However, since switching to the next step is not intuitive, it must be planned and practiced ensuring all key stakeholders know what to do and under what conditions to change methods. A key challenge to the PACE concept is understanding the trigger point for transition to the next component of the plan. This transition between the sender and receiver of information must occur simultaneously, without the benefit of being choreographed by some communications means. This is why the education, training, and exercise piece is so important. Emergency communications ecosystem participants have to understand that the decision to transition to other parts of the plan may have to occur in a vacuum where communications no longer exist. The alerting, signaling, and coaching that many people are used to getting would be gone!

The communications ecosystem is bigger than the planning organization, first responder groups, and the boots on the ground.

Finding Helpful Resources

Before beginning any PACE plan, it is good first to find out if an organization already has a PACE plan or has a continuity of operations or business continuity plan that could be used as a platform to develop one. If some work has already been completed or there are resources available from other organizations, build on those by inserting that information

into the PACE template rather than starting with a blank page. These templates can be for a single resource (e.g., voice communications), a single organization, or multiple organizations. Think outside the box at what all the possible pathways could be.

CISA offers several priority telecommunications services that are helpful for a PACE communications plan. The Government Emergency Telecommunications Services (GETS) provides priority landline access during times of congestion and degradation. The Wireless Priority Service (WPS) also boosts the reliability of calls when communications are congested or degraded. Users can combine GETS and WPS with other services like FirstNet and Frontline to increase priority between carrier services. Finally, the Telecommunications Service Priority (TSP) prioritizes the restoration of voice and data connectivity for organizations with national security and emergency preparedness missions (Note: TSP has a fee and must be set up in advance of the service).

For everyone in the ecosystem, a National Oceanic and Atmospheric Administration (NOAA) weather radio offers an all-hazards network for broadcasting information about all types of natural and environmental hazards (e.g., storms, earthquakes, avalanches, chemical releases, oil spills) and public safety messages (e.g., AMBER alerts, 911 telephone outages).

By taking a fresh look at old continuity plans, preparedness professionals can better assess their communication needs and identify multiple viable solutions to future communication failures. Although this article focuses on communications planning, PACE should be applied to any public safety or public service activities that could put lives or property in danger if any failure were to interrupt those activities.

Lack of PACE awareness was identified as a gap during the 2021 Presidential Inauguration planning process. The preparation plans were rocked in a twelve-day period between the Nashville Christmas Day Bombing and January 6, 2021, insurrection attack on the United States Capitol. Both events challenged operable and interoperable communications, negatively impacting the emergency communications ecosystem.

The message to everyone, whether creating a standard operating procedure or incident response plan, the cop on the beat, firefighter on a ladder truck, paramedic in an ambulance, administrative assistant, teleworker, or homemaker, be sure to "PACE it"!

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

Building Business Post-Disaster – A Florida Case Study

By Mark McQueen

There is a familiar saying among emergency planners: "Never let a crisis go to waste." Though it seems counterintuitive to those outside the industry, planners and decision-makers understand opportunities can be found in the wake of great devastation. Even as they recognize this potential, it can be challenging to know how to plan for the future amid the work to restore critical services and repair the damage left in the crisis's wake.

Developing a Strategic Response Plan With a Future Vision

Most emergency planners create standard detailed response and recovery plans that include steps to restore critical community lifelines, such as citizen health and safety, power, and communications – and rightly so. Disasters, especially extreme weather events such as hurricanes, earthquakes, and tornadoes, severely impact infrastructure systems like energy, potable water, and sanitary sewer services. When these are disrupted, and a community cannot function properly, there is exceptional pressure on local government to restore essential services as quickly as possible.

However, many of these strategic plans do not account for what comes after recovery. Just as emergency preparedness begins before disaster strikes, strategic response plans must also lay a foundation for regrowth and new business – even if this regrowth is expected to come years later. It is often advised to start with the end in mind. To create optimal conditions for business development post-disaster, response plans must develop a framework for strategic recovery that drives investments in infrastructure, security and safety, and quality of life to spur the shift from initial emergency response to recovery and regrowth.

In October 2018, Hurricane Michael struck the shores of Northwest Florida as the first Category 5 hurricane to make landfall in Florida since 1992. Ninety percent of structures were damaged in Panama City alone, and there was a complete loss of power, water, and sewer. First responders restored the bulk of these services within the first two weeks following the Category 5 storm, while the planners examined opportunities to envision the city's future.

In the early stages of development, city planners took a critical first step and surveyed citizens about their vision for the future and what they wanted their city to become. Utilizing a process driven by input from citizens and local businesses is crucial. A visioning process built with citizen engagement helps align community goals as well as build public trust and transparent insight into how the city prepares for recovery and resiliency after a crisis. In the months immediately following Hurricane Michael, Panama City leaders conducted a community engagement campaign to shape their strategic planning. This campaign included dozens of public forums, town halls, and focus groups during which community members could share their direct feedback about the plans for the city's future.

City planners leveraged this citizen feedback to shape the city's strategic plan and formed an open line of communication that remains accessible to this day. Consistently connecting with citizens throughout the implementation of the recovery plan ensures continued trust and support of the community and enables the city to reprioritize as necessary.

Additionally, developing a strategic plan that both responds to disaster and aims for a future vision better enables a municipality to receive crucial funding support – namely from state and federal entities. The post-Hurricane Michael recovery plan prepared by Panama City leaders was a critical factor in securing state and federal funding that enabled the plan's implementation. Developed in tandem with other plans for the city's future economic and quality of life development, this strategic plan served all stakeholders involved by providing a shared vision and path forward – as well as a methodology that outlined stakeholders' responsibilities and goals. Simply put, everyone understood where the city was headed and what they needed to do to help make this vision a reality.

A worker helping to rebuild Panama City's streetscape, which was devastated by Hurricane Michael (*Source:* Mark McQueen, 2022).

Rebuilding Better Than Before

These plans were not necessarily enacted in the first week, or even a month, after the emergency event. However, establishing a framework and priorities at the outset of the response helped avoid quick fixes that would create more work later.

Business owners seek cities with quality infrastructure that will support their growth instead of impeding it. Weak infrastructure, like poor plumbing or damaged roads, can drive key customers away. In collaboration, planners, disaster management officials, and other key stakeholders should take the opportunity to restructure the city to better serve businesses and the customers who frequent them. For example, downtown streets and buildings in Panama City are being rebuilt with the future in mind – advancing long-held plans to beautify the city's public areas and make them more efficient for citizen use. Outdated plumbing systems are being replaced with more durable, modern systems. Wide, walkable pathways, flexible transportation systems, and available parking in a downtown area allow for a better customer experience, paving the way for business growth.

Critical Considerations for Rebuilding Businesses

Other quality-of-life investments are critical factors in businesses' decisions to set up viable businesses, including community amenities like outdoor recreation and gathering spaces, downtown dining areas, public water access, and much more. If people enjoy living in a city, they also enjoy being customers there – a critical consideration not lost on business owners.

Safety and security also rank high on the Federal Emergency Management Agency's priority response list as a critical community lifeline. Disasters provide abundant opportunities for bad actors to take advantage of displaced citizens or abandoned homes and properties. These heightened security needs do not ebb with the tide, however. Maintaining strong security after the immediate response phase has passed encourages new business growth and development as well as the confidence of citizens in local government.

Like infrastructure upgrades, investments in newer security technology and operations are worth the upfront cost to deter criminal activity and restore trust with the community and business owners. Security measures such as partnering with businesses on camera systems and working with real-time crime center technology vastly reduce crime rates and lower police response time. These measures also improve the relationship between the business community and first responders as business owners become more involved in protecting their community and properties.

Adapting strategic plans to prepare for future business development does not mean that the standard emergency response protocols are less critical.

Upgrading infrastructure and security systems set the stage for new business growth after a disaster event by improving the quality of life for business owners and the community. It can be challenging for most citizens to see beyond the devastation left after a disaster. Immediate needs like food and shelter take precedence, quickly followed by the stress of "getting back to normal." Most often, however, it is impossible to return to things as they once were. This does not have to be a bad thing, though.

In Panama City, more businesses are operating today in the downtown area than before Hurricane Michael. By taking advantage of the opportunities to create more walkways, open more parks, plant more trees, invest in safer technology and build reliable infrastructure systems, any city can build a better, brighter future that attracts new citizens and businesses for decades to come.

Even though it often takes longer and more investment upfront to put these proactive plans in motion, it pays off in the long term. Four years after Hurricane Michael, Panama City is executing its ambitious vision. Take advantage of the opportunity presented by the disaster to lay a stronger foundation for the next storm – and new growth.

Mark McQueen, major general, U.S. Army retired, is the city manager for the City of Panama City, Florida.

SAVE THE DATE

MAY 30 - JUNE 2

FORT WORTH

CONVENTION CENTER

MULTI-DAY WORKSHOPS

CONTINUING EDUCATION CLASSES

NETWORKING OPPORTUNITIES

EXHIBIT SHOWCASE

AWARDS LUNCHEON

SPONSORSHIP OPPORTUNITIES

Technological Strategies for Organizational Leadership

By Nathan DiPillo

Integrating information technology (IT) into emergency management and public safety agencies involves balancing technological limitations with the organizational mindset. Finding this balance has been discussed in practice, academia, and across multiple disciplines, with friction sometimes emerging between the leadership mindset, staff, data, training, and implementation. For example, interpersonal and social challenges may arise when some professionals (impacted sometimes by generational gaps) do not understand or are uncomfortable using modern technology while others use it daily. These friction points can delay response and recovery efforts, slow new technology integration, and impact culture.

Structure, Culture & Mindset

Southern New Hampshire University defines organizational leadership as, "a management approach in which leaders help set strategic goals for the organization while motivating individuals within the group to successfully carry out assignments in service to those goals." This approach forms a basis for how public and private organizations operate. For example, policies drive public sector agencies – mainly comprised of government agencies and municipalities – while private sector agencies and companies are in business to make a financial profit. Although the results may differ, the process is similar: goal setting, decision-making, problem-solving, relationship building, understanding environments, etc.

In emergency management and public safety – where future uncertainties can dominate processes, and product solutions must meet an all-hazards environment and an all-encompassing threat landscape – an insightfully designed process can reduce emotional and reactionary decision-making. Fortunately, effective integration of IT can make workflow, goals, problem-solving, and life-or-death decisions more rational and timelier with a higher likelihood of success.

The knowledge-sharing model offers three types of changes leadership can implement when seeking high-quality services from their workforce: economic and geopolitical, technological, and mentality. These change management principles can positively affect organizational culture and IT integration, allowing for better data management and workforce inclusion in the decision-making process. The level of investment in IT can affect the ability to maintain the required balance of intent, mission, and focus when preparing for, responding to, and recovering from emergencies. In addition, the level of

IT integration can directly impact a company or agency's successes or failures. However, IT complexities coupled with public sector funding challenges can make it difficult for emergency management agencies to remain current, especially in rural locations where staff and resources can be scarce. The learning curve for employees, plus the impacts on budget and process, can adversely affect efficiency and productivity. Finally, maintaining IT competency can be even more challenging when employee turnover is high.

As Nancy Torres stated in 2018, "With this rise in crises across the United States, data and technology have an increasingly important role in improving emergency management departments across the country." Of course, while IT can provide tools that emergency management and public safety agencies can effectively leverage, personnel will benefit only if they have adequate and consistent training on how to utilize these tools. In addition, these tools can become costly and cumbersome if organizational leadership does not fully appreciate and commit to maintaining core personnel competencies and effectively addressing issues that may arise, such as data overload, too many solutions to simple problems, or redundancy in IT solutions due to siloed divisions within an agency.

Unlike private industry, the organizational structure of emergency management and public safety agencies – large and small – is challenged by not knowing the timing and magnitude of unplanned events. Although lessons learned from past events lead to process advancements and new technology investments, leadership dynamics, budget constraints, and cultural acceptance will determine how well IT is effectively embedded into organizational processes.

Investments & Challenges

Advancing technology requires a robust organizational structure that can accept and process extensive data. For example, technology for equipment like that on the Cal OES FIRIS plane supports ground units, decision-makers, and planning units in managing resources and saving lives. Although this technology improves insight, response measures, and recovery efforts, the challenges remain in synthesizing the data, determining who can see it, mitigating security concerns, and providing contract oversite.

When these factors fail or have not been mitigated or tested, the challenges may overwhelm employees and leadership. Over-collecting "unorganized" data can lead to confusion and lead to unintended reactionary decision-making, which may result in leadership reverting to "static" and slow decision-making processes that rely on stale or low-quality data – "the old way of doing things."

For example, Esri's ArcGIS Online geospatial information systems (GIS) portal has the capacity to display *thousands* of data layers. If not properly constructed, managed, and collated by users, the portal could generate overwhelming and confusing information

from a multitude of private and public sources. As a result, it may be difficult for planners, end-users, and decision-makers to distinguish between what is useful and what is noise. In an organized environment, all data would be verified, clear, concise, and timely to help decision-makers plan for, respond to, and recover from emergencies on blue-sky and grey-sky days. However, rather than occurring organically, committees often design, test, and plan for these efforts in blue-sky settings –sometimes going untested.

IT security challenges and rapidly changing functions have made it difficult for some agencies to keep up with security concerns. Standards like FedRAMP and the National Institute of Standards and Technology FIPS (Federal Information Processing Standards) are emerging more frequently in federal and state environments and are designed to help set standards for storage solutions, data quality, and data security. As a result, determining how public sector agencies and private industry embed standards-based IT systems and processes into their organizations is critical for achieving their goals.

COVID-19 also presented challenges and opportunities for IT integration when the pandemic significantly impacted communication workflows within emergency management and public safety organizations. By leveraging IT capabilities, organizations have attempted to bridge the physical gaps the pandemic created. Remote access technology has allowed personnel to connect via the internet, but communication impedances and challenges have impacted connectivity between leadership and the workforce. This new work environment has modified how emergencies are handled and will likely be the new normal in agency communication cultures. As the COVID-19 response lessens, the challenge for leadership shifting from being in a health emergency to handling natural and human-caused events will require addressing issues with personnel management and remote workforce options. IT can serve as a medium for impacting accountability, workflow, and process communication.

With so many IT tools plus data overload, how can emergency management and public safety agencies prepare and sustain IT solutions in a fast-paced environment?

Impacts on hiring and recruitment are also paramount when high turnover is part of the emergency management culture. With many employees demanding remote options, some agencies and companies are considering modifying their hiring policies. Remote opportunities are not necessarily bad for agencies (assuming the position could be effectively performed remotely) if there is effective management of oversite, recruitment, and retention expectations. However, a new remote work culture would require public and private sector agencies to adapt and their human resources policies to catch up. The technology would significantly impact how a remote workforce is implemented and tracked.

Implementing Change

It is time for emergency management and public safety industries to adopt and prepare for radical and rapid onsets of IT integration into daily operations more aggressively. From workflow and security standpoints, leadership must evaluate current capabilities and integrate new technologies into their workforce cultures. Understanding the psychology of decision-making, optimizing digital business strategies, and challenging former operational processes are vital for opening leadership to management changes in behavior and bureaucracy. Some action items to consider when applying organizational fundamentals include:

- Understand how IT systems and processes are applied in the agency's culture to balance current IT security standards, support a rotating workforce, and adapt to new remote communication challenges.
- Understand how IT has advanced, so that simplicity, risk identification, and consistency are essential for accountable, accurate, and validated workflows that meet specific standards that cross-pollinate between the public and private sectors.
- Balance human and technological efforts that impact new and existing IT contracts for tools and data acquisition – for example, how artificial intelligence impacts data and workflow.

- Share knowledge to understand IT impacts on processes, workflows, cultures, and decisions.
- Consider the Six Sigma business methodology as a straightforward process for addressing IT challenges:
    - Recognize and understand the problem,
    - Identify and define the problem,
    - Measure and analyze a data-driven solution,
    - Provide a practical solution,
    - Create a system for a long-term solution, and
    - Measure and realize the results.

The key to making all this possible is for leadership to lean into a progressive and sometimes painful process in change management. Reviewing after-action reports and key people in critical parts of the workforce helps ensure the right people are in the correct positions. Because technology is advancing quickly, understanding current technologies and strategies, and seeking outside help when needed, are paramount for understanding operational cycles in both the public and private sectors, highlighting challenges, addressing problems, and implementing technological changes.

Between security concerns, access challenges, and an overload of available options and data, leadership must regularly upgrade and reevaluate processes and contracts. The future of emergency management and public safety is full of IT integration opportunities. However, it is also accompanied by workforce challenges, new and emerging events, and the complexity of multiple emergencies within emergencies, both natural and human causes. The federal, state, and local levels are improving communication, but gaps still exist between adapting IT options and organizational leadership principles.

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

Linking Resilience and Innovation for Emergency Preparedness

By Nia D'Emilio & Christopher Tarantino

Most industries suggest a certain level of resilience and innovation. It is important to get through challenging times to keep a company going, and "innovate or die" has long been a mantra of the business world. While these concepts – or in some cases, buzzwords – come up in various lines of work, they seem to take on a deep meaning in emergency preparedness and response roles. Being resilient is a matter of life and death sometimes, and because no two events are ever the same, this profession demands ever-changing solutions to increasingly complex problems.

These two concepts – resilience and innovation – hold the key to making emergency preparedness and response professionals more effective, efficient, and ultimately successful. When leaders possess a high level of resilience and a high propensity to innovate, the communities they serve are more likely to overcome obstacles with more tenacity and unique solutions. To quantify these observations and make resilience and innovation measurable qualities that professionals could learn to strengthen, Epicenter Innovation launched a research project.

Defining "Resilience" and "Innovation"

Understanding the meaning of each term is critical before understanding the link between these two concepts. *Resilience* allows individuals to endure and overcome challenging circumstances. A high level of resilience serves a person well in various cases. However, it is imperative to strengthen a person's resilience threshold in extreme environmental and emotional circumstances, such as during emergencies and disasters. The first step to make the goal of growing one's resilience actionable was to figure out how to measure the trait in an individual. Research shows that many factors indicate an individual's capability in this area. For example, assessing one's personality, preferences, social resources, spirituality, and attitudes toward adversity are critical for measuring resilience levels. Examining these areas provides a comprehensive assessment that reflects the overall ability of an individual to navigate hardship and arrive at positive outcomes.

Though resilience levels vary from person to person, it is a character trait. One person can be more resilient or less resilient than others, but it is an innate quality of that individual. To *innovate*, however, is a choice. Anyone at any time can choose to approach a problem more innovatively. As with resilience, one's propensity to innovate is measurable, with a similar set of factors to determine one's level of innovative tendencies. Collectively analyzing an individual's personality, motivation, knowledge

base, behavior, emotions, and mood states provides a matrix to determine how creative someone is likely to be. These factors directly impact an individual's capacity to conceive and articulate fresh concepts effectively enough to be embraced by those around them.

Resilience & Innovation: The Link

After defining and measuring resilience and innovation separately, the project's next step was to compare the two as measurable traits that a person can possess. The project analyzed behaviors or characteristics that made one person's resilience and propensity to innovate higher than another's. After reviewing years of literature and conducting interviews with experts in the field, Epicenter Innovation determined that about fifty traits can be measured to determine one's resilience and propensity to innovate.

Measuring all these traits is essential in determining an individual's resilience and innovation levels. Ultimately, measuring these traits is a complicated process that requires the simplification of complex data into digestible results. Among all the traits and behaviors that play a role in this process, one factor stands out above the rest for both multifaceted concepts: an individual's *openness to experience*.

Openness to experience is one of the five factors in the Five-Factor Model of personality, a framework that explores "five broad trait dimensions or domains…extraversion, agreeableness, conscientiousness, neuroticism…and openness to experience." If measured effectively and accurately, a person's openness to experience is the most critical factor when assessing both resilience and innovation potential. An individual measuring a high openness-to-experience level correlates to a high resilience level. In other words, those open to new experiences have a greater chance of showing flexibility around coping with change and uncertainty. Similarly, being open to new experiences encourages creativity and the ability to solve problems in unorthodox ways. This openness to change leads to an inquisitive attitude essential in developing innovative solutions and alternative approaches. As such, those willing to push their comfort zones are more attuned to advance beyond traditional modes of thinking and remain at the vanguard of development.

This research suggests that a human-centered approach to emergencies will yield more effective results when trying to build more resilient communities.

This factor is the crucial link between resilience and innovation. While the research for this project focused on measuring the presence of these two constructs in individuals, the motivation to conduct the research came from years of experience in emergency management. This field requires resilience and demands innovative approaches to constantly changing circumstances. Definitively determining the inherent connection between these two factors offers some critical insights into where the future of emergency preparedness and response roles – from individuals to small teams to entire agencies – lies.

Personal Resilience & New Solutions for Stronger Communities

This research suggests that a human-centered approach to emergency preparedness and response will yield more effective results when trying to build more resilient communities. Strengthening communities through planning processes and trainings are valuable and worthwhile. However, if the people at the helm do not understand their own levels of resilience and innovation, community response will not run as effectively or efficiently.

Increasing community resilience starts with increasing personal resilience. Leaders with high openness to experience approach problems with empathy, strategy, and ingenuity. They are more likely to collaborate with their internal teams and listen to their communities' concerns. They also might be more likely to go through several cycles of trial and error to find a solution that makes the most sense for the scenario. Increasing an individual's resilience and propensity to innovate can help communication effectiveness and community resilience and response.

Emergency preparedness and response professionals face particular challenges when handling stress and pressure simply because of the nature of the work. Growing resilient communities must begin with a willingness to explore new and novel solutions, and that process starts with the individual. Whether working on an incident management team, with a large government agency, or in an office of one, every professional brings their own set of unique traits and strengths to the table. Measuring an individual's resilience and propensity to innovate is vital to building stronger and more effective emergency preparedness and response professionals. Building these leaders is the key to building stronger communities.

Nia D'Emilio is the learning and events coordinator for Epicenter Innovation. Before working in emergency management, she worked in the theater community in Chicago (Illinois) before moving to Los Angeles (California) to work in the film industry. She holds a B.A. in Religion from Denison University and an M.S. in Leadership for Creative Enterprises from Northwestern University.

Christopher Tarantino has almost 15 years of experience in emergency response/management. He has acted in various positions across the public and private sectors, including roles at the volunteer, local, county, state, and federal levels. As the founder and chief executive officer of Epicenter Innovation, he leads a team specializing in training, exercises, and support services for public safety and emergency management professionals. In addition to his full-time role with Epicenter, he is also an instructor for the Federal Emergency Management Agency's (FEMA) Master Exercise Practitioner Program (MEPP). He previously served as a digital communications specialist within FEMA External Affairs. He has trained thousands of emergency management professionals in 38 different states in the U.S. and frequently speaks across North America on disaster response, emerging technology, and crisis communications.