EST 1998

DOMESTIC PREPAREDNESS JOURNAL

VOLUME 20 ISSUE 10

OCTOBER 2024

CYBER AT THE LOCAL LEVEL

Take Domestic Preparedness On The Go

October 2024, Volume 20, Issue 10

Editor-in-Chief	Catherine L. Feinman
Editorial Associate	Christine Anderson
Project Manager	Elisa DeLeon
Publications and Outreach Specialist	Teresa Farfan
Marketing Coordinator	Nicolette Casey
Student Intern	Annette Velasco

Advisory Board

Caroline Agarabi
Raphael Barishansky
Michael Breslin
Paul Cope
Robert DesRosier Sr.
Nathan DiPillo
Kay C. Goss
Charles Guddemi
Robert C. Hutchinson
Rhonda Lawson
Joseph J. Leonard Jr.
Ann Lesperance
Anthony S. Mangeri
Sadie Martinez
Kesley Richardson
Tanya Scherr
Richard Schoeberl
Mary Schoenfeldt
Lynda Zambrano

Cover Source: Image courtesy of Canva.

For more information about Domestic Preparedness, visit DomesticPreparedness.com

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

Copyright 2024, by the Texas Division of Emergency Management. Reproduction of any part of this publication without express written permission is strictly prohibited. Domestic Preparedness Journal is electronically delivered by the Texas Division of Emergency Management, 313 E Anderson Lane Suite 300, Austin, Texas 78752 USA; email: subscriber@domprep.com. The website, DomesticPreparedness.com, the *Domestic Preparedness Journal*, and The Weekly Brief include facts, views, opinions, and recommendations of individuals and organizations deemed of interest. The Texas Division of Emergency Management and the Texas A&M University System do not guarantee the accuracy, completeness, or timeliness of, or otherwise endorse, these views, facts, opinions or recommendations.

Editor's Note

Source: Unsplash/Clark Young

Local-Level Planning for National-Level Threats

By Catherine L. Feinman

Society's dependence on cellphones, computers, the internet, and other cyber-related communication and storage devices creates exponential vulnerabilities as cyberthreats become more sophisticated and prevalent. As cyber-dependencies increase, so does the cyberthreat landscape, which ranges from targeted ransomware attacks to complex phishing schemes. Although financial losses often get a lot of attention, the consequences of such attacks at the local level can have much more devastating effects. For example, critical lifeline services like 911 call centers and food and agricultural supply chains rely on digital communications and data-driven systems that can be desirable targets for cybercriminals.

The scope and scale of the cyberworld increase the likelihood that local agencies and organizations that have not already been targeted will one day be on the frontlines of a cyberattack. This is particularly concerning for emergency response agencies, hospitals, government entities, critical infrastructure, businesses, and other community stakeholders that house systems and data that communities depend upon. The intentional or unintentional release of the information they store or the denial of access to their systems would have cascading effects throughout the community.

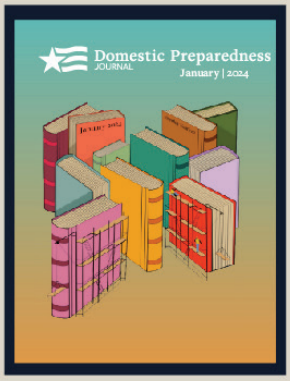
Each malicious or nonmalicious incident highlights the urgency for local agencies and organizations to identify vulnerabilities and close existing gaps. To safeguard these systems and critical resources, local stakeholders should take a proactive approach to assess their threats, hazards, and risks and incorporate additional security measures such as risk assessments, situational awareness training, and incident response plans that include cyber. Raising awareness about common cyberthreats and ethical issues related to data management before, during, and after a crisis can prevent or mitigate these threats.

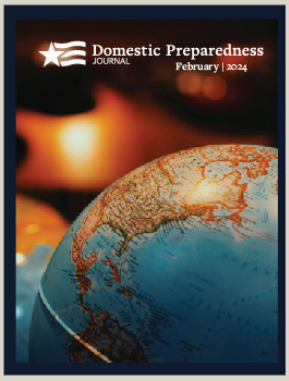
The authors in this October edition of the *Domestic Preparedness Journal* share their knowledge and best practices for protecting communities from cybercriminals, nation-state threat actors, and transnational criminal organizations. These threats, which used to be typically handled at the state and national levels, are now local-level concerns that require robust plans to keep communities safe.

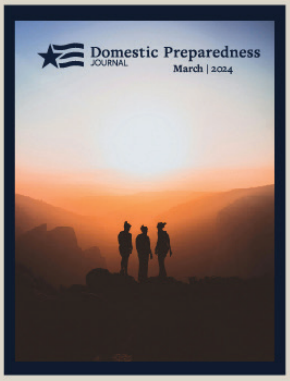
©October 2024 Texas Division of Emergency Management

SHARE YOUR INSIGHTS

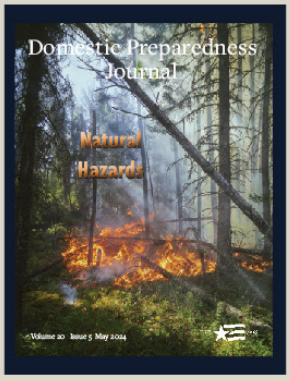
EST 1998

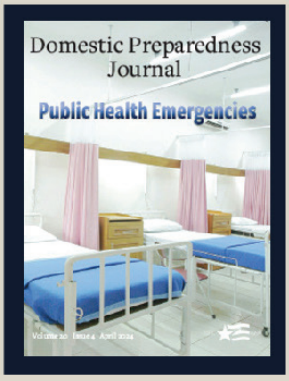


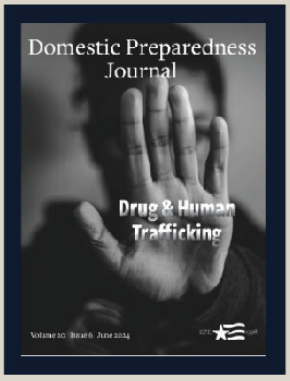




Domesticpreparedness.com/subscribe







SUBMIT AN ARTICLE TO THE JOURNAL

WWW.DOMESTICPREPAREDNESS.COM/AUTHORS

Table of Contents

©October 2024 Texas Division of Emergency Management

Source: Sergey Nivens/Adobe Stock

Malicious and Non-Malicious Cyber Incidents: Education and Preparation

By Dan Scherr and Tanya Scherr

The presale event for Taylor Swift's Eras tour crashed Ticketmaster's service in 2022. The incident caused an outcry that even reached the U.S. Senate, which branded the ticket service a "monopolistic antihero." Ticketmaster had fallen victim to a denial-of-service attack, which is one of the six types of incidents outlined in the November 2023 report *Planning Considerations for Cyber Incidents: Guidance for Emergency Managers* by the Cybersecurity and Infrastructure Security Agency (CISA). Planning for these types of incidents is no longer the purview of only the information technology (IT) department or limited to one area of an organization. To remain secure in today's complex, fast-paced technological environment, everyone in the organization, from the leadership to line personnel, needs an understanding of the importance of cybersecurity – the related risks and the organization's protocols and procedures. Without that knowledge, it is difficult for employees to properly prepare for and support the organization's success and missions. This article seeks to educate those working in the preparedness field on the different types of incidents and provide basic steps to plan for them and mitigate potential damages.

Human Error

On July 19, 2024, a faulty software update by the cybersecurity vendor CrowdStrike caused possibly the largest IT outage in history, impacting millions of Windows systems worldwide. The outage is believed to have caused more than $5 billion in direct damages, with healthcare ($1.94 billion) and banking ($1.15 billion) taking the largest hits, and airlines ($860 million) coming in third. In October 2022, Binance, the world's largest cryptocurrency exchange, reported a loss of $570 million from a bug in its asset transfer software code. According to Binance's chief executive, Changpeng Zhao, "Software code is never bug-free."

©October 2024 Texas Division of Emergency Management

Although hackers may be the first assumption after a cyber incident, the reality is that between 74% and 88% of cyber incidents have a human error component: misconfiguration of updates, failure to apply patches to known vulnerabilities, or phishing emails with malware. Phishing is a social engineering technique where an attacker poses as a trusted source through email to acquire users' sensitive data, such as banking or medical information. According to the FBI's Internet Computer Crime Center (IC3), phishing was responsible for almost 300,000 complaints in 2023, resulting in almost $19 million in damages to individuals. One of the largest loss categories is business email compromise, by which attackers attempt to use social engineering techniques to acquire business data or money using company email. These might include a request from the chief executive officer to send an updated contract quickly, an email from the chief financial officer to send copies of W-2s for review, or other related scams.

With the human error factor being such a large portion of cyber incidents, one of the most important and fundamental prevention techniques is education:

- All personnel should learn about risks and prevention methods. There are free resources, including offerings from CISA and the United Kingdom's National Cyber Security Centre (NCSC), and free and low-cost options curated by the National Institute of Standards and Technology (NIST).
- Policies should include actionable information and detailed procedures, not vague guidelines like "Do not click on phishing emails."
- Personnel should be informed of steps to take if they click on a malicious link or make a security error.
- There should be protocols to manage those situations, and employees should be encouraged to report potential issues. A delay could result in catastrophe.
- Unsolicited requests or emails should not be opened. If an email is questionable, users should contact their supervisors or IT or contact the named sender on their official phone or email rather than the contact information listed in the email.

Structural Failures

In 2016, the failure of a single router at Love Field in Dallas caused the grounding of the Southwest fleet for approximately an hour. The critical failure resulted from a then-unknown data chokepoint at the airline's data center. When the router failed, it led to cascading issues. Although the airline had backup procedures, the unique failure did not trigger the standard procedures for another system to pick up and resolve the issue, leading to catastrophic results. Over 2,000 flights were canceled over the following days as the company investigated the issue, affecting hundreds of thousands of customers and costing an estimated $54 million.

Structural failure is a design flaw in hardware, software, or environmental controls that can cause an outage when the system fails. With the interconnected nature of these systems, it is crucial that managers are aware of their system

©October 2024 Texas Division of Emergency Management

infrastructure, potential risks, and operational requirements. First, without a clear understanding of the infrastructure and nature of systems used by an organization, it is impossible to develop a plan to protect and manage risk. Consideration should be given to current operations, planned changes to infrastructure, for example, whether the agency is moving to cloud-based systems or changing communication platforms, and contingencies that activate in emergencies or mutual aid environments. Once the inventory is established, plans should address replacing hardware (based on service life and operational considerations) and developing redundancy for system failures or outages.

Natural Disasters

When Hurricane Sandy hit New York in 2013, Datagram went offline and caused one of the most publicized data center outages. As a preventive measure, the utility company (ConEd), proactively shut off the power at 7 p.m. to preserve company and customer equipment during the storm. On the 25th floor of a building in Lower Manhattan, the data center switched to backup generator power and continued operations. Four hours later, the center went dark. From their location, they were not aware of the flooding in the basement, where the generator and pumping equipment were located. The center was offline for four days while another generator was placed and started operating, with a daily fuel bill of $10,000. While changes have been made in the interceding years, agencies should revisit preparedness strategies and consider items like the locations of backup generators, server rooms, and associated equipment.

According to the National Oceanic and Atmospheric Administration, the Mississippi River reaching historically low levels in 2023 was the United States' 25th disaster that cost more than $1 billion in a single year. The increasing frequency of major disasters and severe weather across the country necessitates additional focus on the potential impacts of weather events on cyber infrastructure. As an agency creates disaster plans, each potential emergency should include an index for effects on systems and mitigation plans to maintain operational effectiveness. Creating these indexes alongside the other plans allows the team to evaluate needs and expectations during each potential contingency. It is also important to collaborate across departments, backup data in multiple locations (including the cloud, if possible), and rehearse plans and remediation efforts for cyber infrastructure.

Malicious Incidents

Denial of Service

A denial of service occurs when an attacker overloads a host or network with traffic until the target crashes or cannot respond. This prevents legitimate users from using the affected service, which may be a website, customer accounts, email, or other internet-based service. This malicious activity mimics events that occur when excessive legitimate traffic overwhelms a service.

These malicious actors seek to disrupt the service using exploited computers and connected devices, collectively referred to as the rapidly expanding Internet of Things. Of the estimated 17 billion connected devices worldwide in 2022, most were not designed nor built with security in mind. Bad actors

can weaponize easy-to-hack computers and devices as drones for a denial-of-service or distributed denial-of-service attack. Denial-of-service and distributed denial-of-service attacks are implemented with various motivations. Some malicious actors send a message or express discontent, financially harm a company or steal their business, extort money, or inject malware onto a system.

Organizations can take actions before, during, and after these attacks to protect themselves or mitigate damage. Before the attack, organizations should review their systems and reduce the attack area to the extent possible, plan for expected scale, understand the differences between normal and abnormal traffic, plan mitigation options and response plans, and ensure having adequate firewalls for advanced attacks. During an attack, organizations can verify the attack and nature of the threat, deploy countermeasures and mitigations, and monitor other network assets to ensure the attack is not a decoy for another threat. After the attack, organizations should continue to monitor network resources, update the response plan to improve future responses, and report the incident and outcome.

Malware

Malware is short for malicious software that uses a program or file to perform a harmful action on a network, server, or system, such as viruses, computer worms, Trojan horses, spyware, fileless malware, and ransomware. These programs' actions vary and may be limited to a single system or designed to spread across an entire network to damage or compromise systems, exfiltrate data, steal identities, disrupt service, or steal resources.

- A computer virus is named for its ability to infect and replicate like a biological virus. These programs attach themselves to files, insert infectious code, and move to other files. They pretend to be legitimate programs that users must execute and commonly spread through email attachments, downloads, file sharing, and removable media. Defending against viruses centers on using a robust antivirus software, paying attention to attachments and executable files, using strong passwords, avoiding questionable websites, and updating browsers and operating systems.
- Computer worms are similar to viruses in impact and damage but do not require another program to replicate. Once in a system, worms use the device to scan for and infect other systems and networks. Mitigation impacts are similar to those for viruses.
- Trojan horses, such as backdoors, downloaders, remote access, rootkits, and banking malware, look like legitimate programs and, when executed, install malware for a variety of purposes. Mitigation and prevention techniques for trojans are similar to those for worm and virus plans: Do not open attachments from unknown sources, update systems, watch for phishing attacks, and maintain robust antivirus and firewalls.
- Spyware, such as browser session hijacking, browser helper objects, cookies, autonomous spyware (independent programs), and bots, captures and delivers data from the targeted system to the attacker. Commonly targeted data include websites visited; credentials for applications, accounts, and systems;

©October 2024 Texas Division of Emergency Management

TOP ARTICLE TRENDING NOW

DP'S NEW MUST-READS

ESSENTIAL KNOWLEDGE
for practitioners

email and associated information; screenshots; downloads; and other traffic.

- Fileless malware attaches itself to otherwise benign software packages to infiltrate the system memory directly. This malware does not install anything on the infected device (hence the name) and mainly operates through memory code injection and windows registry manipulation.
- Ransomware is one of the most visible types of malware, with high-profile attacks on governments, agencies, and businesses. Ransomware can encrypt files on a device or system, locking out the users and degrading systems that rely on that data. Attackers then demand some form of payment to decrypt the data and regain access. Attackers may copy the data and export it prior to locking out the user – meaning, even if the target pays the ransom, their data is still in the hands of the attackers and could be sold or used to further extort the victim. CISA started a Stop Ransomware campaign and hosts resources on its campaign pages, including best practices, mitigation, response, and available services.

Third-Party Compromises and Supply Chain Attacks

A third-party compromise takes place when an attacker compromises a partner organization, and that company's connection is used to access the host organization. With the accelerating interconnection between organizations and the volume of connected services and devices, these attacks have experienced a 700% increase from 2020 to 2023. Reporting in 2024 found almost every company with a third-party relationship has experienced some level of breach, representing almost 30% of breaches overall. Of the sectors examined, healthcare reported the highest breach rate overall (35%) and the second-highest third-party breach rate (36%). This tracks with the size and scope of the healthcare sector and with the value of the personal health information available to attackers.

Software and related technology products were responsible for 75% of third-party breaches in 2023. One of the largest and costliest breaches in history was the SolarWinds attack, by which attackers were able to access a third-party software company and inject malware into a scheduled update, which then infected the company's customers downstream. The resulting exposure impacted more than 18,000 customers, including some U.S. government agencies and 14% of the *Fortune 1000*. These companies lost an average of 11% of their annual revenue ($12 million average), and the covered losses are estimated at $90 million. School districts are also frequent targets of these breaches, with New York Public Schools, the Los Angeles Unified School District, and Chicago Public Schools – the three largest systems in the country – all experiencing third-party breaches in 2022.

Third-party compromises can be challenging, as the attackers are not entering directly, but instead exploiting a trusted relationship with an established partner. Agencies can take some basic steps to mitigate risk. Passwords and credentials are often vectors (vulnerability or exploit used in an attack) in these incidents, especially passwords reused on multiple systems or accounts by users. Using tools to determine whether passwords were included in a previous breach can identify potential vulnerabilities

©October 2024 Texas Division of Emergency Management

in the system. Reviewing systems and attack surfaces is also critical in the risk management and mitigation process. The risk assessment should include internal systems and vendors and their systems. Organizations should have policies and protocols for monitoring and taking action when they suspect breaches or compromises, including notifying law enforcement and other appropriate authorities.

Making a Team Effort

An organization-wide team effort is critical for reducing vulnerability and exposure to cyberattacks. Individuals can take basic steps to prevent and mitigate a range of threats and reduce operational impacts. Education can help users prevent cyber breaches and incidents and understand which emails or links are safe and which should be reported or deleted. Working with an organization's stakeholders can help ensure cyber resilience in disaster planning and promote forward-looking efforts to prevent oversights or critical failures during larger events. Employing basic security procedures, updating and patching systems, and reviewing policies and procedures are all fundamental elements of overall security. Local agencies can use tools available free of charge from CISA and the Federal Emergency Management Agency to bolster their security and educate their personnel, such as the following:

- *Understanding and Responding to Distributed Denial-of-Service Attacks*,
- The *MS-ISAC Guide to DDoS Attacks*, and
- *FEMA's Planning Considerations for Cyber Incidents: Guidance for Emergency Managers.*

Using these and other resources and being proactive about cybersecurity, planning, and preventive measures can help all agencies raise their security and preparedness without requiring significant financial resources.

Dan Scherr holds a PhD in public policy administration with a terrorism, mediation, and peace focus. He is an assistant professor in criminal justice and homeland security at the University of Tennessee Southern and program coordinator for the cybersecurity program. He is a certified fraud axaminer and U.S. Army veteran who served stateside during the September 11 attacks and has over two decades of experience in homeland security and operations.

Tanya Scherr holds a PhD in public policy administration with a healthcare and emergency preparedness focus. She is an associate professor in healthcare administration for the University of Arizona and has three decades of healthcare experience. Along with being a certified fraud examiner since 2011, she is also a former firefighter–emergency medical technician (EMT), previously licensed in several states and held national certification. She has held several executive and board of director positions for community nonprofits that focus on women's equality, domestic violence, and sexual assault.

©October 2024 Texas Division of Emergency Management

Source: Arrow/Adobe Stock

Securing Cities: The Fight Against Local Level Cyberthreats

By Michael Breslin

Imagine waking up to news of a city plunged into chaos. The water supply has been disrupted, emergency services are offline, and local transportation is at a standstill. A ransomware attack has crippled local government, holding critical infrastructure hostage. Sensitive personal data, from Social Security numbers to medical records, are at risk of being leaked to criminal organizations. Citizens wonder what they should do and how long it will take for their community to recover. This is not a hypothetical scenario but a stark reality that cities across the country face. City officials must ask themselves if they are doing enough to protect their communities from these invisible yet devastating threats. The need has never been greater for robust cybersecurity at the local level as a matter of survival.

Society's interconnected nature means that a breach in one small system can have far-reaching consequences. Cybersecurity is a critical issue at the local level (city and county government agencies and private-sector entities) that encompasses cybersecurity training, cyber hygiene practices, cybersecurity resilience, and incident response. Cybersecurity resilience is crucial for safeguarding critical infrastructure and information systems. State and local governments manage essential services such as water supply, electricity, transportation, and emergency response, which are vital for public safety and economic stability.

Local governments in the United States (U.S.) are as plentiful as the cybersecurity risks they face. In 2022, the U.S. Census Bureau reported 90,837 local governments, including county, township, municipal, and special purpose entities. These entities are highly susceptible to and are constantly at risk of cyberattacks, given the vast amounts of sensitive information they maintain, constrained resources, limited funding, level of awareness, inadequate training, and antiquated information systems. Notable cyberattacks targeting state and local governments include the following:

- Atlanta (Georgia) Ransomware Attack (2018) – A significant ransomware attack affected multiple city departments, including the police and courts. The attack caused widespread disruption and cost the city an estimated $17 million to recover.

©October 2024 Texas Division of Emergency Management

- Baltimore (Maryland) Ransomware Attack (2019) – A ransomware attack crippled thousands of computers and disrupted city services for weeks. The attackers demanded a ransom of 13 bitcoins (around $76,000 at the time), which the city refused to pay.
- Cyberattack on Texas State and Local Governments (2019) – A coordinated ransomware attack targeted 22 local government entities in Texas. The attack disrupted services and required a significant coordinated response from state and federal agencies.
- New Orleans (Louisiana) Cyberattack (2019) – New Orleans declared a state of emergency after a ransomware attack forced the city to shut down its computer systems. The city was forced to rebuild its IT infrastructure.
- Ransomware Attack on Baltimore County (Maryland) Public Schools (2020) – A ransomware attack led to the shutdown of the county's public school network systems, resulting in class cancellations for 115,000 students.
- Dallas County (Texas) Cybersecurity Incident (2023) – This event followed a ransomware attack five months prior, which compromised the personal information of 26,212 City of Dallas employees. The ransomware attack impacted benefits-related information maintained by the city's human resources department. The hacker group Royal threatened to leak sensitive information, including names, addresses, Social Security numbers, medical information, and health insurance information.
- Michigan and New York Ransomware Attacks (2024) – City governments experienced service disruptions and had to shut down some facilities after cyber incidents.
- 10 Major Cyberattacks and Data Breaches (2024) – In the first half of 2024, 10 major events stand out, but more are likely to occur.

The growing threat of cyberattacks on state and local governments emphasizes the need for comprehensive, robust cybersecurity measures, and preparedness. The risks of not taking these steps include increased exposure and vulnerability to cyberattacks, financial losses, damage to critical infrastructure, company branding and reputational damage, legal consequences, and national security risks.

Common Vulnerabilities in Government Systems

A robust cybersecurity framework helps protect these services from malicious attacks, such as ransomware and data breaches, which can disrupt operations and compromise sensitive information. By implementing strong security measures, state and local governments can ensure the continuity of essential services, maintain public trust, and prevent costly and potentially catastrophic consequences. Common vulnerabilities in government systems that cyber attackers can exploit include:

- *Outdated Software and Unpatched Systems* – Many government systems run on software that has not been updated or patched, making them vulnerable to known exploits.
- *Weak Authentication Mechanisms* – Poor password policies and lack of multi-factor authentication can facilitate attackers' unauthorized access.
- *Phishing Attacks* – Government employees are often targeted by phishing attacks, which can lead to credential

©October 2024 Texas Division of Emergency Management

theft and unauthorized access to sensitive information.

- *Insufficient Network Segmentation* – Without proper network segmentation, access to one part of the network can enable attackers to move laterally to other parts, increasing potential damage.
- *Misconfigured Systems* – Incorrectly configured systems and services can expose vulnerabilities that attackers can exploit.
- *Lack of Employee Training* – Employees who are not adequately trained in cybersecurity best practices can inadvertently expose systems to attacks.
- *Remote Work Vulnerabilities* – The increase in remote work has introduced new vulnerabilities, particularly in virtual private networks and remote access systems.
- *Third-Party Vendor Risks* – Government agencies often rely on third-party vendors, which can introduce vulnerabilities if those vendors do not have robust security measures.

In addition to defending against external threats, cybersecurity resilience also addresses the risks posed by human error and insider threats. Employees at all levels can inadvertently expose systems to vulnerabilities through actions such as clicking on phishing emails or misconfiguring security settings. However, the threat does not only come from negligence. Intentional and unintentional insider threats can be just as damaging. Disgruntled employees or others with access to sensitive systems can misuse their privileges, either out of malice or carelessness, leading to significant breaches.

Comprehensive training programs, continuous monitoring, and a culture of cybersecurity awareness are essential to mitigate human error and insider threats. By fostering a proactive approach to cybersecurity, state and local governments can reduce the likelihood of incidents caused by internal vulnerabilities, ensuring that critical infrastructure and information systems remain secure and resilient in the face of evolving threats. Addressing these risks requires a comprehensive approach, including regular software updates, strong authentication practices, employee training, thorough security assessments, and close monitoring of internal access to sensitive systems. Government agencies can improve their cybersecurity posture with the following tools and actions:

- *Implement Zero-Trust Architecture* – Adopting a zero-trust model (strong authentication practices) ensures that no one inside or outside the network is trusted by default. This approach requires continuous verification of user identities and access permissions.
- *Regular Software Updates and Patch Management* – Maintaining software and systems with the latest patches helps protect against known vulnerabilities.
- *Multi-Factor Authentication (MFA)* – Enforcing MFA adds an extra layer of security and restricts unauthorized access.
- *Employee Training and Awareness Programs* – Training with regular sessions help employees recognize and respond to phishing attempts and other social engineering attacks.
- *Continuous Monitoring and Incident Response* – Implementing monitoring tools and a robust incident response plan helps rapidly detect and mitigate threats.
- *Network Segmentation* – Dividing the network into segments limits the spread

of malware and restricts unauthorized access to sensitive information.

- *Secure Cloud Services* – Moving to secure cloud services and ensuring proper configuration can enhance security and resilience.
- *Collaboration and Information Sharing* – Sharing threat intelligence and collaborating with other agencies and private-sector partners improves overall cybersecurity defenses.
- *Endpoint Detection and Response (EDR)* – Deploying EDR solutions can help agencies detect and respond to malicious activities on endpoints across the network.

Collaboration in Action

State and local governments can enhance their cybersecurity resilience through several collaborative efforts. One effective approach is to establish regional cybersecurity alliances or task forces that bring together various government entities, private-sector partners, and academic institutions.

These alliances facilitate the sharing of threat intelligence, best practices, and resources, enabling a more coordinated and comprehensive defense against cyberthreats. Regular joint training exercises and simulations can also help identify vulnerabilities and improve response strategies, ensuring that all participants are prepared to handle potential incidents.

A key aspect of collaboration is the development of standardized cybersecurity policies and frameworks. By adopting common guidelines and protocols, state and local governments can ensure a consistent and unified approach to cybersecurity across different jurisdictions. This includes implementing shared cybersecurity tools and technologies, conducting joint audits and assessments, and participating in mutual aid agreements to provide support during cyber incidents. Additionally, leveraging federal resources and programs, such as those offered by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), further strengthens local efforts and provides access to valuable expertise and funding. Through these collaborative measures, state and local governments build a more resilient and secure cyber environment.

One successful example of state-level collaboration on cybersecurity resilience is the Multi-State Information Sharing and Analysis Center. This organization provides a central resource for gathering and sharing information on cyberthreats among state, local, tribal, and territorial governments. The center offers services such as threat intelligence, incident response, and cybersecurity training, helping to enhance the overall security posture of its members.

Another notable example is the Texas Cybersecurity Framework, which was developed by the Texas Department of Information Resources. This framework provides a standardized approach to cybersecurity across state agencies and local governments, promoting consistency and collaboration. It includes guidelines for risk management, incident response, and security awareness training, ensuring that all entities are equipped to handle cyberthreats effectively. Various states have implemented laws, policies, and structures to govern cybersecurity as an enterprise-wide strategic issue. These efforts include collaboration with public- and private-sector stakeholders to enhance overall cybersecurity governance. They highlight the importance of collaboration in building

©October 2024 Texas Division of Emergency Management

Domestic Preparedness
JOURNAL

Subscribe today.





Scan the QR code or
visit the link below
www.domesticpreparedness.com/subscribe

a resilient cybersecurity infrastructure at the state level. By working together, states can leverage shared resources, expertise, and best practices to better protect their critical systems and data.

Public-Private Partnerships in Cybersecurity

Public-private partnerships play a crucial role in enhancing state-level cybersecurity by leveraging the strengths and resources of both sectors. These partnerships foster information sharing, which is essential for identifying and mitigating cyberthreats. The private sector often has access to advanced technologies and expertise, while the public sector can provide regulatory support and coordination. By working together, they can create a more comprehensive and effective cybersecurity strategy:

- Strengthen cyber protections – In January 2024, the Center for Internet Security reported that cyberattacks against state and local governments rose in 2023. However, it found that some of those agencies have begun strengthening their cyber protections against future attacks (e.g., identity management, cybersecurity awareness training, and implementation of mitigation and recovery strategies).
- *Boost election system security* – In February 2024, the U.S. Cybersecurity and Infrastructure Security Agency introduced a program to conduct more cybersecurity reviews for election offices across the country.

CISA has programs to help protect critical infrastructure. For example, the Cyber Innovation Fellows Initiative allows private-sector experts to work alongside government teams, enhancing mutual understanding and capabilities. Additionally, public-private partnerships can help develop and implement standardized cybersecurity practices, ensuring a consistent approach across sectors and jurisdictions. This collaboration not only improves the overall security posture but also builds trust and resilience within the community. State and local governments can effectively address cybersecurity challenges through innovative and collaborative approaches.

Strategies for building cyber resilience cost money. State and local government officials must implement the use of risk assessments, security policy development, employee training, software updates, network protection, data backup and recovery, incident response planning, regular testing, vendor scrutiny, and continuous improvement efforts. These actions by state and local governments are often hampered by lack of funding. However, funding sources and grants are available to states and local governments for cybersecurity training:

- *State and Local Cybersecurity Grant Program* – Managed by CISA and the Federal Emergency Management Agency (FEMA), this program provides significant funding to help state, local, tribal, and territorial governments address cybersecurity risks and threats. For FY 2023, approximately $374.9 million was available.
- *Tribal Cybersecurity Grant Program* – Also managed by CISA and FEMA, this program specifically supports tribal governments in enhancing their cybersecurity posture. In FY 2023, around $18.2 million was allocated for this purpose.
- *Homeland Security Grant Program* – This program includes the State Homeland Security Program and the Urban Area Security Initiative, which provide funds to enhance the ability of state and local

©October 2024 Texas Division of Emergency Management

governments to prevent, protect against, respond to, and recover from terrorist attacks and other disasters, including cyber incidents.

- *Edward Byrne Memorial Justice Assistance Grant Program* – Administered by the Bureau of Justice Assistance, this program provides funding to support a range of activities, including cybersecurity initiatives, to improve the functioning of the criminal justice system.

These and other programs offer valuable resources to help state and local governments strengthen their cybersecurity capabilities and protect critical infrastructure and information systems. Cybersecurity training for local and state government agencies is vital. Programs like the Federal Virtual Training Environment offer no-cost, online cybersecurity training, highlighting the accessibility of resources for enhancing the cyber-ready workforce. State and local entities must adopt cyber hygiene practices to protect against common threats.

Building Collective Digital Safety and Security

Cybersecurity at the state and local levels is a critical component of a secure and resilient society. As the digital threats against local governments and private entities grow more sophisticated, the need for action becomes urgent. Cybersecurity is a shared responsibility. At the state and local levels, it forms the bedrock of the collective digital safety and security of all. Governments cannot afford to leave their communities vulnerable to attacks that could cripple essential services, compromise sensitive information, and disrupt daily life. The path forward is clear. Through comprehensive cybersecurity training, vigilant cyber hygiene, resilience-building, and swift incident response, local governments can fortify their defenses. Every citizen, agency, and organization must play a part in this effort. The stakes are too high to ignore, especially with global adversaries seeking to undermine U.S. vulnerabilities. The country's collective digital safety and security depend on the decisions municipalities make today – because the next cyberattack is not a matter of *if*, but *when*.

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

©October 2024 Texas Division of Emergency Management

Source: Generated with AI by Kartolo/Adobe Stock

Backyard Cybersecurity: The Local Challenge

By Brian Shajari

In 2019, the Port Neches–Groves Independent School District in East Texas fell victim to a ransomware attack that led to a disruption of networks and a denial of access to student data. To regain access to its network, the school was forced to pay the ransom, resulting in significant financial loss to the district. This is only one of hundreds of cyberattacks that happen each year throughout U.S. municipalities. According to the Capitol Region Council of Governments, in 2021 alone, there were 77 cyberattacks on municipal governments and 88 cyberattacks on education entities throughout the country, resulting in nearly $18 million in costs.

From malicious criminal activity to "hacktivism," the consequences of attacks on digital technology range from inconvenience to disaster. No matter the size of the entity affected, preventing and mitigating cyberattacks will become an increasing challenge for all levels of government, commerce, and community. Numerous threat actors target these municipalities:

- *Nation-state actors* take a tactical and strategical approach on behalf of a foreign government to affecting the target from a tactical and strategic aspect.
- *Criminal actors* conduct cyberattacks for financial gain.
- *Hacktivists* are individuals or groups who typically conduct cyberattacks on behalf of a political or social cause.
- *Thrill seekers* are individuals who target systems for the thrill of disabling or affecting them for bragging rights.
- *Cyberterrorists* conduct cyberattacks on behalf of a terrorist organization.
- *Insiders* are actors who are familiar with and know how to cripple certain systems or functions within a network.

The modern world increasingly relies on rapidly advancing digital technology, and cybercriminals progressively focus on ways to exploit technology's vulnerabilities. With technology necessary for daily life-

©October 2024 Texas Division of Emergency Management

enhancing work environments, reducing costs, driving commerce, managing supply chains, automating functions, and overall managing daily needs, cyberattacks can have a far-reaching, negative global impact. Throughout the world, municipalities use technology for infrastructure operation and maintenance. With the growing adoption of smart technology, municipalities have become an increasingly visible target for malicious actors, thus making protection of this technology from cyberattacks more challenging.

Local municipal governments implement smart technology that interacts with daily functions and services, such as online utility payments, infrastructure maintenance and operation, operations and shipping applications within ports, digital utility meter reading and monitoring ("smart reading"), public facility automation, water and wastewater facility automation, and other affected city activities. Emergency services likewise harness information-based applications to facilitate emergency management plans, maintain communications (such as 911 capabilities), and store records (including school district information and other data relevant to city functions).

With smart technology comes the threat of cyberattack – an attempt to deny, degrade, disrupt, destroy, or alter information resources or the information itself. Examples of cyberattacks on smart technology include malware, insider threats (intentional and unintentional), denial of service, and other techniques intended to compromise the confidentiality, integrity, and availability of data. Although higher levels of government and businesses may possess the tools necessary to protect against cyberattacks and have the resources available to address these threats, local governments often do not. Table 1 illustrates a small fraction of cyberattacks on municipal infrastructure throughout the nation.

Table 1

Date	Location	Incident Type	Impact
May 2023	Philadelphia, Pennsylvania	Data breach	Personally identifiable information of private citizens were exposed.
February 2023	New Orleans, Louisiana	Data breach	Personally identifiable information of private citizens were exposed
January 2023	Atlanta, Georgia	Ransomware attack	$17 million in data recovery costs
Early 2022	Florida	Ransomware attack	Inability to access city government compter accounts

©October 2024 Texas Division of Emergency Management

The Challenges

Protecting against cyberattacks has become a major challenge faced by local governments and communities, which often lack a sufficient cybersecurity program. Factors include inadequate funding, limited vulnerability assessments, lack of cybersecurity integration within emergency management offices, limited training, overlooked threats, or lack of policy governing information-based technology usage. By addressing these challenges, local governments have the potential to significantly reduce their cyber risk.

Funding

Funding for cybersecurity has historically been a significant issue in local municipalities. Without adequate funding, there may be no dedicated cybersecurity staff within the organization. Funding shortages can impact the critical functions of a cybersecurity program and can expose of vulnerabilities throughout a municipality's systems. If a local government cannot budget adequate funding for a cybersecurity office, seeking the expertise of the existing information technology (IT) staff can help establish a cybersecurity program using recognized cybersecurity frameworks.

Assessments

A functional cybersecurity program starts with assessing vulnerabilities and understanding the risk to affected assets if they were to be disabled through a cyberattack. These could be any information-based technology, such as mobile devices, laptops, desktop computers, operational technology applications (including those in water and wastewater treatment facilities), building automation, and any other physical asset connected to the Internet of Things. These assessments provide documentation that may make it easier for stakeholders to understand what vulnerabilities exist for information-based systems within a municipal government and can provide them with the information necessary to either correct the issues or accept the risk that accompanies them.

Integration Into Emergency Management

Emergency management has traditionally focused on incidents such as wildfire, flood, natural disaster, and other disasters requiring government response. However, local emergency management coordinators at the state, county, and city levels should begin integrating cyber incidents into their emergency preparedness plans, exercises, and incident command system to aid them in an actual event. By focusing on how to respond to an incident affecting a critical component of an emergency operations center (EOC) or other assets capable of degrading response, and by categorizing the level of effect, municipalities can be prepared to execute the appropriate response. Everyday cyberthreats such as email phishing would not warrant the activation of the EOC, which occurs mainly on cyberattacks that have the potential to develop into an expanding incident. However, in the case of a more serious threat, the emergency management coordinator should seek outside assistance from federal or state partners. One method to address this is via an Emergency

©October 2024 Texas Division of Emergency Management

Support Function (ESF) with other entities throughout the jurisdiction and the larger region to ensure there is a centralized pool of resources to use in the event of a cybersecurity incident. This ESF should consist of federal, state, and local agencies in addition to private industry partners. An effective ESF can minimize the impact of a cybersecurity event and foster interoperability throughout the region.

Training

The weakest link in any security system is the human factor. Due to the potential for human error, it is often the first point of failure in a cybersecurity incident. Any information-based asset used by members of a local government, or the community are vulnerable to cyberattacks. Users should be trained on how to best protect these devices to prevent the compromise of information. This can be accomplished through computer-based cybersecurity training, in-person awareness courses, emergency management exercises, and end-user agreements, and these tools could ultimately be used to hold users accountable for their actions. Training should include how to distinguish phishing emails, protect personally identifiable information on egovernment systems, recognition of social engineering attempts, regular penetration testing, simulated phishing emails, and other training to create "cybersecurity champions" throughout the organization.

Ignoring the Threat

"It will never happen here" is one of the most dangerous assumptions an emergency preparedness professionals can make. Emergency management coordinators at local levels should begin to recognize that cyberattacks are an increasing threat for communities of any size during and after natural disasters, as the potential impact on human lives can make even small-town networks and assets high-value cyberattack targets. Often during major disasters, scammers pose as insurance companies targeting disaster victims, while at the same time, local government network security may be overlooked. Emergency management coordinators should seek the assistance of their cybersecurity staff to help ensure that assets are monitored for external and internal cyberthreats. There should be a fine line drawn between IT staff and cybersecurity staff. IT traditionally fixes computer problems and cybersecurity personnel mitigate cyberthreats through security measures and monitor systems for unauthorized access. If feasible, the organization should have cybersecurity personnel specifically assigned to protect internal systems. Budgeting for these positions should be a priority of any local government.

Governing Policy

Incident response plans can play a major role in determining ultimate outcomes. Effective cybersecurity programs are built on incident response plans, derived from risk assessments, understanding vulnerabilities, and outlining requirements of cyber hygiene on all information-based assets in use. Local government stakeholders should work with their cybersecurity staff or outside resources to build an effective governing

©October 2024 Texas Division of Emergency Management

cybersecurity plan or policy to establish a common baseline of good cyber practices to protect assets. Smaller government entities should establish mutual aid agreements with regional, larger governments to share cybersecurity personnel and resources if needed. This effort would foster regional teamwork and build relationships, which could prove invaluable during a real-world scenario.

Where to Start

Smaller local governments with no cybersecurity program in place may struggle to identify a starting point, but numerous resources are available to help provide basic building blocks. These are discussed below and can provide the municipality with a solid foundation on which to build:

- In March 2022, the Cybersecurity and Infrastructure Security Agency released Cybersecurity Performance Goals. This framework contains 38 categories written in a common language to help an entity of any size establish a cybersecurity program. It may be used to assess a local government's current cybersecurity position and to plan how to address remaining vulnerabilities. Additionally, this framework can help build a cybersecurity program.
- The National Institute of Standards and Technology released the latest version of the Cybersecurity Framework in February 2024. This framework is nationally recognized and dives deeper into both technical and administrative controls, which can help to develop a functional cybersecurity program.

Local governments should recognize the need to integrate cybersecurity into their daily activities and better protect e-government systems, information-based assets, and the citizens they serve. Cyberthreats can stem from multiple angles, including technical and non-technical threat vectors, and can strike anytime. By following the advice in this article and giving more focus to integrating cybersecurity into emergency management at all levels, local governments and communities can help to reduce the frequency of cyberattacks.

Brian Shajari is a principal consultant at ABSG Consulting Inc. ("ABS Consulting"), Global Government Sector, with 23 years of experience in cybersecurity, intelligence analysis, and emergency management. He holds a Master of Arts in Cybersecurity from American Military University, along with certifications such as CompTIA Security+, Facility Security Officer, and multiple U.S. Coast Guard emergency management qualifications. Brian specializes in developing cybersecurity standards for the U.S. Coast Guard and Cybersecurity & Infrastructure Security Agency (CISA), conducting cyber risk assessments, and leading cyber intelligence efforts throughout the government and private sector. He is committed to safeguarding critical assets and networks by applying his expertise in artificial intelligence, network security, and incident response. As a 23-year veteran of the U.S. Coast Guard, Brian has served in multiple major disasters across the country, spanning from hurricanes to cybersecurity incidents.

©October 2024 Texas Division of Emergency Management

Source: Smart Future/Adobe Stock.

Cyber and Physical Resilience in the Food and Agriculture Industry

By Nathan DiPillo

According to the U.S. Department of Homeland Security, the U.S. Food and Agriculture Sector (Food/AG) accounts for 20% of the national domestic product. The food and agriculture industry serves as the backbone of the U.S. economy, supporting communities and families around the nation and globally. During the pandemic, local farmers lost an estimated $688.7 million in sales and a total loss to the economy of approximately $1.32 billion. For example, one of the most impacted farming sub-sectors to be affected by COVID-19 was the dairy industry. Over 3,000 dairy farms had to dump milk and close operations due to low demand. In the 21century, this sector has become increasingly more complex, and the COVID-19 global pandemic exposed weaknesses, which included food supply chain interruptions, excess milk production, less demand for bio-fuels with less driving, less demand for food as restaurants closed, and other impacts. Dangers in this sector exist on local, national, and international scales. These threats highlight this sector as a vulnerable area and a potential target for foreign threat actors and natural hazards.

FEMA has designated lifeline sectors. While the Food/AG sector is combined with hydration and shelter, the focus is not necessarily resilience but response to provide food, hydration, and shelter to victims. The U.S. Department of Homeland Security defines Food/AG as a critical infrastructure but not a prioritized infrastructure. With the sector's thin profit margins, incidents and threats continue to plague the sectors and sub-sectors' dependencies and inter-dependencies. Contextualizing threats and efforts in Food/AG helps highlight the importance of industries in this sector and the complex nature of threats and risks that its stakeholders face. In addition, new and emerging mitigation measures can make the sector more resilient.

Food and Agriculture Sector Overview

National Geographic states that, since the Neolithic period, agriculture has been one of the driving forces behind thriving cultures for more than 10,000 years. Today, the U.S.

©October 2024 Texas Division of Emergency Management

food and agriculture industry still thrives off basic needs and primary functions like water, rotation of seasonal planting and harvesting, and animal husbandry. However, technological advances, population increases, and withering farmland pose risks to this sector. The U.S. is a leader in food production, but increases in population and decreases in farmland have an impact, "According to USDA's estimates 6.6 million acres of US Farmland has been lost from 2008 through 2015, with a 1 million acre decline last year alone."

Food and agriculture production heavily rely on average temperatures and weather conditions, biological and natural systems, and intergenerational knowledge and experience. As populations grow and farmland shrinks, more processed foods are being produced to meet demands. Corn and other crops are being genetically modified to help build resilience against damage.

Legacy systems and weather-pattern familiarity are vital to maintaining a thriving and profitable food and agriculture sector and sub-sectors. In 2023, the average profit margin for farmers was about 2%. Operational overhead costs like fuel, labor, and insurance impact the farmer's bottom line. Additional threats like ransomware, data breaches, malware attacks, bioterrorism, financial instability, and rising costs all impact these margins. The decreased profitability driving farm families to sell land and cease operations has a significant impact on the domestic and global food supply.

Is Technology Good for the Agriculture Industry?

To stay profitable and sustainable, farmers must find creative ways to integrate technology into their farming practices and business continuity plans. The new but still learning Norm AI (artificial intelligence that assists with regulatory compliance queries) is specific to the food agriculture industry, but other technological advancements for this sector continue. Technological integration within the industry helps with effective decision-making and keeps farmers safe by promoting environmental sustainability and conservation. The intersection of technology with traditional tactics and processes, which heavily depend on seasons and natural cycles, adds to complex challenges and threats. Farmers continue to face physical risks, such as suffocation from engulfment or entrapment, explosions due to high amounts of grain dust, falls from extreme heights, or crushing and amputation from grain equipment. The 2019 data from the U.S. Bureau of Labor Statistics indicates that the agricultural sector is still the most dangerous in America with 573 fatalities, or an equivalent of 23.1 deaths per 100,000 workers. The combination of physical risks, complex commodities markets, changing environments, resource demands, and supply chain stressors can cause interruptions in food supply-chain systems. This complex problem creates significant challenges within the Food/AG sector.

Balancing technology, old-world agrarian cultivation techniques, and an informed, forward-thinking mindset is the answer to sustainability in farming. During the COVID-19 pandemic, weakness in the Food/AG sector was exposed. Issues like market volatility, supply-chain disruptions, and personnel and resource deficiencies demonstrate the fragility of the existing framework. Despite low profit margins and major setbacks caused by natural hazards and disasters, this sector continues to find innovative solutions. Learning to embrace technological changes with an experiential mindset while preserving old-school techniques will reap future gains. Methods

©October 2024 Texas Division of Emergency Management

and processes that use emerging technologies include precision agriculture, vertical farming, cultured meats, livestock tracking, drones for distributing seeds and pesticides, and many others. Balancing and integrating new concepts and technological advancements with an old-school farming mentality will keep this sector resilient and thriving when battling cyber and environmental threats.

Identifying How to Improve

Change management can be challenging to implement. Old-world mentality, especially in the farming industry, is hard to change due to traditional and proven farming methods. Remaining up to date on market volatility and cyberthreats within the Food/AG sector is pivotal to staying resilient by understanding inevitable changes and the necessary actions to stay in business and be prepared for emergencies. However, combining business continuity methods and traditional farming practices can have significant effects. For example, cropland traditionally remains bare between harvesting seasons, but planting cover crops between seasons can help soil function by suppressing weeds and reducing herbicide use. Another example is training operators to integrate precision farming GPS systems with standard visual observation practices in case positioning, navigation, and

©October 2024 Texas Division of Emergency Management

timing signals are lost or diminished. This improves the ability to plant and harvest on time. Cross-sector collaboration, human interface, and partner collaboration are the foundation for improvements and progress. The Food and Agriculture-Information Sharing and Analysis Center (Food and Ag-ISAC) is one organization that facilitates information sharing and threat and risk awareness across the industry.

> *STOP STOPPING A growing body of research shows that often what looks like "multitasking" is actually "rapid task-switching," especially when technology is involved.* -2015 Old Farmer's Almanac

Industry farmers and partners have detailed views of their environments, margins, and challenges. In general, modern farm families embrace technology and integrate new mindsets that adapt to new legal and regulatory frameworks as they prepare for planting and harvesting seasons. Recent legislative actions include the 2021 presidential Executive Order on Promoting Competition in the American Economy, which reaffirms and clarifies the Packers and Stockyards Act regulation and makes available $200 million to expand competition in meat processing and $25 million in workforce training. Investing in training, emerging agriculture products, and technological advancements will help U.S.-based farms compete. Another legislative action in support of the industry was the Agriculture Improvement Act of 2018 (2018 Farm Bill), which provided a five-year continuation and reform of agricultural and other programs. For example, the Farm Support Program maintains and, in some cases, expands support for farmers through crop insurance programs, commodity support programs, and conservation initiatives to provide a safety net for farmers facing market volatility and natural disasters.

Data is currency in today's adaptation of technology. As the Food and Agriculture industry remains beholden to seasons and yields, the data gleaned from these practices is *gold* for farmers. The *Farmers' Almanac*, which is used by farmers and others to predict long-range weather forecasts, for example, uses data and patterns to make long-term predictions. Through regenerative agriculture and farming practice sustainability, it is possible to sustain soil, re-use it efficiently, and still produce food on a global scale.

> *Without protecting and regenerating the soil on our 4 billion acres of cultivated farmland, 8 billion acres of pastureland, and 10 billion acres of forest land, it will be impossible to feed the world.* - *Regenerative Agriculture*

With trends in farmland loss, technological advancements will become a top priority for U.S. and global Food/AG decision-makers. With farming culture and practices adapting to significant variations in average weather conditions and other threats, available tools and best practices can help mitigate threats and improve efficiency and yields.

Solutions Abound

The loss of healthy food and the ability to sustain agriculture would cause cascading impacts across other sectors, on the general health of the public, and on other human support services. Supply chains, financial markets, military readiness, and more are dependent on nutritious, sustainable, and attainable food sources. Solutions to the security and resilience of the food and agriculture industry can be challenging to identify and difficult to implement, but they are the responsibility of whole communities,

©October 2024 Texas Division of Emergency Management

not just farm families or the government. Following are examples of how industry partners can help with Food/AG resilience:

- Connect local and state partners with owners and operators of small and large farms and include them in tabletop exercises and other preparedness and business continuity efforts.
- Learn the roles and responsibilities of industry and government in cooperation and recovery efforts specific in the Food/AG industry.
- Understand cross-sector dependencies and impacts and build resilience into business continuity processes (e.g., transportation or energy backup processes in case of mechanical breakdown or natural disasters) that depend on realistic measures of livestock survivability, crop sustainment, refrigeration, etc.
- Integrate and better understand efficiencies in precision farming practices for small and large operations (e.g., effective drone use for spraying chemicals only when needed or more efficient ways to pick up rocks that damage combines).

Implementing new technologies in the Food/AG industry is paramount when implementing mitigation efforts for sustainable and resilient farming. Farm families and all levels of government must prioritize conversations on threats and farming risks. Perishable commodity production that sustains life and the industry is a necessary endeavor. The ability to balance old-school best practices and data-driven solutions impacts short-term and long-term goals, so staying up to date on legislative efforts, regulations, and emergency response will be crucial to sector sustainment after emergencies. Farmers have experienced the consequences of long-term shifts in average temperature and weather conditions, mechanical failures, and market volatility. With family farms transitioning to the next generation and cyber and physical threats emerging locally and abroad, all key stakeholders must stay invested in the food and agriculture industry and focus efforts on resiliency, not just response and recovery.

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. 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 opposing 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 has a Master's of emergency management/homeland security from the National University and other Federal Emergency Management Agency, U.S. Department of Homeland Security (DHS), and military certifications.

©October 2024 Texas Division of Emergency Management

Source: Generated with AI by Prostock-studio/Adobe Stock.

The Ethics of Data in Disaster Management and Crisis Operations

By Anthony S. Mangeri

Data has become essential to emergency planning and disaster operations. As a valuable asset when making informed decisions, data provides emergency managers with the opportunity to effectively respond to emergencies with decisive efficiency. However, data that emergency management agencies collect and store – such as data that capture travel movements, document structural damage, and provide information on business operational capabilities – need to be protected and archived in compliance with law and standards.

Evidence-based decision-making has made the ethical and legal challenges associated with managing data necessary. As technology advances, the amount of data collected, stored, and recalled in the name of crisis management can be substantial and must be handled in a manner that protects those in need. In disaster management, data can range from personal identifying information to geolocation tracking and resource allocation records. Ethical data practices include measures. The ethical dimensions of data management in disaster scenarios that protect individual privacy and secure critical decision-making data focus on critical principles like accountability, transparency, privacy, and fairness.

The Department of Homeland Security (DHS) maintains a data governance policy for information sharing in its DHS Data Management Directive, 103-1, which outlines that DHS data is to be catalogued and protected as an asset. Data governance policies uphold public trust, ensure regulatory compliance, and ultimately influence the success of disaster response and recovery operations.

Data Sensitivity in Crises

During a pandemic, natural disaster, or other fast-paced emergency, the pressure to act quickly often requires gathering large quantities of sensitive data, including:

- *Personal identifying information* – any data that can be used to identify an individual

©October 2024 Texas Division of Emergency Management

directly or indirectly, such as name, age, contact information, and private communications; and

- *Sensitive personal information* – any data that, whether released without authorization, lost, or compromised, can lead to substantial personal or professional harm, embarrassment, inconvenience, or unfairness to an individual.

DHS Privacy Office published its Handbook for Safeguarding Sensitive PII in 2017 to provide guidance for safeguarding personal data. Emergency management agencies must develop policies and procedures for collecting, storing, using, archiving, and destroying data in accordance with standards and regulations.

As part of the hazard mitigation planning process, emergency managers need to collect substantial amounts of data on repetitive loss (RL) properties to focus on risk-reduction efforts. The National Flood Insurance Program defines *repetitive loss properties* as:

> *any insurable building for which two or more claims of more than $1,000 were paid by the National Flood Insurance Program within any rolling ten-year period, since 1978. An RL property may or may not be currently insured by the program. Currently there are over 122,000 RL properties nationwide.*

Federal policy determined that this data is confidential and difficult to secure due to federal law, which restricts the distribution of any information that can be used to identify property owners.

During the COVID-19 pandemic, for example, governments and health agencies needed and were required to track data from infections, contact tracing, and healthcare resources. These efforts had to be accomplished while respecting data privacy laws. In the United States, there are several privacy laws to consider, such as the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act. Sometimes, even the European Union's General Data Protection Regulation may impact storage and data management operations in the U.S. Reviewing data management processes during the COVID-19 response is an example of how ethical data management is vital to protect individuals' privacy while ensuring the efficacy of response operations.

Ethical principles such as *beneficence*, or acting in the public's best interests, must be weighed against the need to *do no harm*, or *nonmaleficence*. Sharing information during a disaster, such as the personal identifying information collected during the COVID-19 pandemic can save lives, but it also risks exposing sensitive personal or operational information. Determining the right balance between the public good, operational security, and individual rights is a key ethical challenge in disaster data management.

Accountability and Transparency

To inform response strategies, emergency management organizations must rapidly gather large amounts of data during disaster operations. In addition to beneficence and nonmaleficence, accountability and transparency are essential principles in ethical

©October 2024 Texas Division of Emergency Management

data practices – all of which are intertwined to create trust. Accountability requires that organizations involved in emergency operations and disaster assistance explain what personal data is being collected, why the data is collected, and how such personal data will be used.

For example, when an emergency management agency's mobile application (app) collects location data during an evacuation, the agency must be transparent about the scope of data collected, such as whether it tracks the general movement of the population or individual evacuees via the app. This transparency helps to build public trust. Trustworthiness is foundational to ethical leadership. Governments and organizations must ensure that emergency management app use is voluntary and that their guidelines on privacy protections are transparent – for example, ensuring that data is anonymous and not centrally stored. The protection of such data is an essential responsibility of those who collect the data as well as anyone having access to the information collected.

Ethical Frameworks in Data Decision-Making

Structured ethical frameworks, such as *utilitarianism* (the greatest good for the greatest number) and *deontological ethics* (adherence to duties and rules), can guide emergency managers through moral dilemmas as they make critical decisions regarding data during a disaster. An emergency manager might face a decision where they must choose between

©October 2024 Texas Division of Emergency Management

sharing potentially sensitive personal data with other agencies to improve the crisis response or keeping that data private to honor individuals' rights. In that scenario, utilitarianism may favor sharing data if it benefits more people, whereas deontological ethics might advocate for not sharing it to uphold privacy rights. However, ethics and regulation are not the same. When decision-makers confuse the two, they could delay or halt data-sharing efforts regardless of the circumstances. Understanding the limits of regulations highlights the need to develop a strategy for data management during all phases of the emergency management cycle.

Privacy and Confidentiality

The privacy of information collected during emergency operations is one of the most significant ethical concerns in data management. Even when personal information could significantly facilitate the disaster response, the people agencies are trying to help still retain their right to privacy. The ethical challenge lies in determining how to protect personal data yet share information that is necessary for the community's safety and well-being.

Confidentiality requires that such information be shared only with those who have a legitimate need and for purposes that are clearly defined and limited to the crisis response. One approach to the ethical handling of data is referred to as "privacy by design" and emphasizes the importance of building privacy considerations into data systems from the outset. A key component of this approach is data minimization, which involves collecting only essential anonymized information to prevent the unauthorized release of any personal identifying information.

Fairness in Data Use

During disaster response and recovery operations,

©October 2024 Texas Division of Emergency Management

data should be used in ways that are fair. Emergency and business continuity managers must ensure that data-driven decisions do not disproportionately harm or disadvantage any population. This is particularly relevant when using algorithms and artificial intelligence (AI) systems with flawed or biased underlying inputs. For example, if disaster assistance funds are allocated based on an algorithm that uses historical data and that data reflects past injustices in resource allocation, certain communities might receive less assistance than others. This may include algorithms and AI platforms used to estimate or assess damages or losses. To ensure ethical data use in disaster management, audit algorithms to avoid bias, and use data in a way that promotes fair outcomes.

Data plays an invaluable role in disaster management. With the collection of such information to ensure evidence-based operations comes a great responsibility to protect data and dispose of it when it is no longer needed. As such, emergency managers increasingly face complex ethical dilemmas during the process of collection, usage, storage, and destruction of their community members' personal information. By incorporating data management principles like *accountability*, *transparency*, *privacy*, *fairness*, and *beneficence*, they can more effectively and ethically manage that information. Adhering to ethical standards can help organizations build public trust, safeguard individuals' rights, and ensure that the benefits of data-driven decision-making do not come at the cost of personal privacy or fair treatment. As the demand for evidence-based decision-making continues to grow, emergency management professionals must commit to ethical data practices that respect the needs of the community and the rights of individuals. In times of crisis, data can save lives, but it must be managed with care, responsibility, and respect for ethical principles.

Anthony S. Mangeri, MPA, CPM, CEM, is the chief operating officer and principal at the Mangeri Group, LLC, and president of the International Association of Emergency Managers' (IAEM) Region 2. He currently serves on the IAEM-USA board of directors and is a board member of the Philadelphia InfraGard Members Alliance. Before consulting, he served as a town manager, where he navigated the community through the challenges of the COVID-19 pandemic, was responsible for local emergency preparedness, disaster recovery operations, and played a key role in the establishment of a municipal police department. Anthony also served as the New Jersey State hazard mitigation officer for over a decade. During the response and recovery to the September 11, 2001, terrorist attacks, he was the operations chief at the New Jersey Emergency Operations Center, where he assisted in coordinating the state's response efforts. Beyond his professional achievements, Anthony has committed over 35 years to serving as a volunteer firefighter and emergency medical technician. He holds a Master of Public Administration from Rutgers University and has completed a fellowship in Public Health Leadership in Emergency Response.

©October 2024 Texas Division of Emergency Management

Source: Generated with AI by sirisakboakaew/Adobe Stock.

Growing Foreign Threats to National Security, Part 1: Challenges and Considerations

By Glen Woodbury

Sovereign nations – in particular, China, Russia, Iran, and North Korea – continuously challenge the United States. These nation-state threats to the U.S. domestic landscape in physical, cyber, economic, military, and diplomatic domains also pose increasing challenges to traditional emergency response entities. Such threats also put essential services and functions at risk through cyberattacks, such as those against hospital operations, financial services, power provision, water services, and other critical infrastructure elements. These actors interfere with and disrupt normal emergency operations with erroneous information during events to sow mistrust, confuse the public, and widen societal divides. Nation-state threats also include "kinetic" risks, such as sabotage of facilities or even missile attacks.

A growing fear within the national security and defense communities is that confrontational nation-states will activate their full range of capabilities in massive, simultaneous applications of cyberattacks, information influence, and kinetic warfare across wide geographical areas of the U.S. Only recently have these concerns entered the realms of preparedness and strategy at state and local levels. Emergency management is fully committed to current crises' while it simultaneously tries to prepare for acts of greater consequence and complexity. Impacts on the emergency management community from nation-state threats generally fall into four overlapping elements:

1. Attacks directly against public health, safety, and security organizations;
2. Interference in the response operations to traditional incidents and emergencies;
3. Attacks against resources or infrastructure that are critical to

©October 2024 Texas Division of Emergency Management

communities in normal and emergency environments; and

4. Attacks against critical national defense and security assets collocated with or dependent upon state and local communities.

Four Nation-State Threats

According to the 2024 Annual Threat Assessment of the U.S. Intelligence Community produced by the Office of the Director of National Intelligence (ODNI), China, Russia, Iran, and North Korea present multifaceted threats to the U.S., leveraging influence, cyber operations, and – to varying extents – military capabilities. China is actively expanding its global influence through sophisticated operations, including the use of artificial intelligence, to undermine U.S. leadership and democracy. It is also the most persistent cyberthreat, targeting critical U.S. infrastructure and preparing for potential conflicts. Russia, similarly, uses influence and cyber operations as key tools to divide Western alliances and shape global perceptions, particularly during U.S. election cycles. Both nations maintain significant military capabilities, with China potentially possessing chemical and biological weapons and Russia focusing on operations related to its actions in Ukraine which domestically has become a divisive political issue.

The ODNI report states that Iran and North Korea also pose serious threats through cyber and missile programs. Iran's cyber activities have become increasingly aggressive, targeting U.S. infrastructure and attempting to influence elections, attacking financial accounts of organizations and individuals, while its weapons program continues to develop more accurate and lethal missiles. North Korea remains focused on expanding its nuclear arsenal and advancing missile technologies alongside a sophisticated cyber program aimed at espionage and financial theft, particularly through cryptocurrency operations.

Collectively, these nations utilize a blend of influence operations, cyberthreats, and military capabilities to challenge U.S. interests globally. Their actions highlight a strategic convergence where cyber and influence operations are often the first lines of attack, with their militaries serving as powerful deterrents or, in some cases, active threats to U.S. and allied forces.

Emergency Management Relevance

Potential scenarios requiring emergency management include the following:

- Campaigns of misinformation (incorrect), disinformation (intentionally misleading), and malinformation (misuse for manipulation) during events or crises intended to disrupt response capabilities, sow distrust of government agencies, and increase societal friction;
- Disruption or destruction of critical local and national infrastructures, limiting emergency resources with economic and social impacts;
- Attacks on essential crisis services such as first response agencies, emergency health facilities, dispatch centers, operations centers, etc.;
- Attempts to limit or divert traditionally available surge resources to other emergencies, such as activation of National Guard units to overseas conflicts or border security operations; or
- Military attacks, such as missile launches against U.S. territory.

©October 2024 Texas Division of Emergency Management

Events of the highest complexity would be combinations of such scenarios promulgated simultaneously across domestic U.S. locations.

Effects on Emergency Management Mission

The emergency management profession has had increases in the scope and scale of its mission space. Intensifications in weather events, along with other natural and technological hazards, have put all communities more and more at risk. Additionally, the expectations placed on emergency management organizations have grown, making it difficult to keep up with a surging workload and meet those expectations.

How the emergency management community addresses the expanded scope and scale of its mission and simultaneously mitigates, prepares for, responds to, and recovers from nation-state threats is a significant challenge. Emergency planners determine which threats to prioritize, how best to allocate resources in preparation, and which responses are most critical in each situation. Nation-state threats might manifest in emergency management in four general categories:

1. *Direct attacks against public health, safety, and security organizations* – Deliberate targeting of emergency organizations and facilities degrades, if not destroys, the underlying infrastructures of a planned emergency response. These attacks might include cyber or military operations against dispatch centers, emergency operations facilities, first responder communications, healthcare and emergency room capabilities, and law enforcement centers.
2. *Disruptive attacks that interfere in the response and recovery operations during traditional emergencies* – Disruptive attacks can influence the public by promulgating false or misleading reports and incorrect data to confuse public perceptions of the event, its causes, and the effectiveness of the response. The goal is to instill a loss of confidence in government, cause the public to question official information and guidance, and amplify societal divides.
3. *Attacks against the resources or infrastructures critical to communities in normal and emergency environments* – Cyber, military, and influence operations might be used singularly or in combination to degrade, divert, or eliminate essential services that communities rely on and the assets critical to mitigating and minimizing the impacts of disasters as they occur. For example, attacks against communications, power, and water services impact a community's normal functions and the essential resources for responders and governments during an incident.
4. *Indirect attacks against critical national defense and security assets that are collocated with or dependent on state and local communities* – Defense and security facilities are vulnerable to attacks and interference outside their often-formidable fence lines. Although military bases and transportation hubs are robust in their security, they rely on local communities and distant jurisdictions to maintain and protect critical infrastructures necessary for daily operations and mobilization efforts. These threats are twofold: Attacks against national security assets could spill over into communities, while assaults against the infrastructures that sustain and support these assets could occur outside the capabilities,

jurisdictions, and authorities of defense agencies.

Cascading and Intersecting Implications

Each threat presents cascading implications for emergency management operations and essential government functions. For example, while improved public information efforts might mitigate incident misinformation, the mistrust or confusion that fake information creates may evolve and manifest outside the bounds of traditional emergency endeavors. For example, well-placed disinformation implying that one segment of a population receives more beneficial disaster relief from officials than another could amplify already existing divides, suspicions, and animosities.

Additionally, emergency management professionals cannot assume these threats are one-offs or linear events that can be singularly planned for and responded to. Adversaries might use several of these attack avenues to maximize the impact with operations intent on spreading misinformation while cyberattacks degrade community services, creating complex and increasingly challenging effects.

Preparedness Perspectives

The types of contingencies that emergency managers prepare for – from increased attention to terrorism prevention and response following 9/11 to the broadened expectations of agencies and the profession during a pandemic – have increased over the past two decades. Concurrently, the effort required to address traditional hazards or novel emergencies exceeds past expectations. This difference is better appreciated when viewed from different perspectives.

Operational

An operations function executes tactics and coordinates resources to solve near- and mid-term issues during the response to an incident, including training on protocols, processes, and practices. Nation-state threats, however, present challenges to traditional operational processes. For example, misinformation, disinformation, or malinformation generally impact traditional joint information centers and public affairs activities. Information professionals must learn new response tactics to address new threats and exercise skills. Other operational impacts also could be consequential, such as interruptions of essential communications systems, emergency computer networks, command and control centers, facility degradation, etc. New or modified plans and resources are necessary to prepare for this new scenario.

Capabilities

Nation-state attacks affect resources in two ways: those required during a response and those necessary for effective preparedness. Asset supply chains that nation-state attacks could disrupt need to be assessed, and contingency plans developed to prepare for the loss of expected and planned-for resources, such as mutual aid, National Guard, and other surge capabilities. In addition, standard preparedness resources dedicated to planning, training, exercising, and asset acquisitions may not be adequate for the nuances and extremes of a nation-state attack.

Policy and Authorities

In the event of a nation-state attack, emergency management governance needs the appropriate policies and authority structure to deal with the preparation, response, and recovery unique to such an event. A 2011 essay by former Department of Homeland Security Secretary Michael

©October 2024 Texas Division of Emergency Management

Chertoff, suggests that in the post-9/11 environment; intelligence and information-sharing policies among law enforcement, national security, and the military remain complex which would seemingly compound in today's nation-state threat environment even more. Emergency declarations must be adequate for the consequences of a nation-state attack. The Stafford Act must be appropriately structured to help communities recover from cyberattacks, infrastructure sabotage, or more serious military attacks. This statute was written in a period that could not have envisioned the hazards and threats faced more than four decades later. Alternatively, new authorities should be developed to address nation-state attack consequences. Likewise, state and local emergency authorities, which originating mostly in the context of the Civil Defense Era of the Cold War (circa 1950-79,) should be reviewed with an eye toward the implications of current and future nation-state threats against state and local communities.

Doctrine

Unified command, mutual aid, resource and aid prioritization, and requests for assistance are examples of doctrinal approaches that could be challenged in the face of a nation-state incident. A unified command may differ in composition and authority in a widespread nation-state attack. When national security is at stake, priorities may also need to change. Federal response to needs and suffering at local levels may require top-down decision-making instead of the current bottom-up structure. Additionally, there are new demands on emergency management systems in a nation-state threat environment. One new element of emergency response even includes civil support to military operations, which may demand new ways of organizing, planning, and resource acquisition. For example, the ability to protect military transportation routes and hubs may require resources from local public safety communities.

Relationships

Core relationships essential to emergency preparedness have been built to support traditional and expected hazards arising mostly from the natural environment. Many of these relationships are codified in comprehensive plans and doctrinal frameworks such as Emergency Support Function agency assignments in the National Response and Recovery Frameworks. Nation-state threats, however, demand information, resources, coordination, and cooperation from entities outside these routine and established relationships. For example, intelligence data from law enforcement entities might be necessary to understand how an incident might unfold and how best to mitigate its effects. Understanding the national security implications of an attack might require interacting with federal agencies that are not normally in communication and coordination channels of emergency response, and the potential impacts on military and other defense assets might require conversations unique to the nation-state context. The incursion over Canadian and U.S. airspace of a Chinese balloon in 2023 demonstrated the challenges of international, interagency, interjurisdiction, and interdisciplinary information and intelligence sharing.

Public and Private-Sector Leadership

In a traditional emergency management landscape, governmental and non-governmental entities' overall goals and objectives align to alleviate public suffering, support disaster survivors, and help communities recover and rebuild following emergency events. In an adversarial nation-state attack, however, the same alignments

©October 2024 Texas Division of Emergency Management

may not exist, and friction among agencies, organizations, and levels of government might result. For example, the actions to protect a military facility might be at odds with the normal functions of the surrounding community. A private-sector entity's response to a cyberattack might conflict with the population's needs, dependent on that company's services. What might be considered prudent public messaging in an emergency could conflict with national narratives during international conflict.

Other Important Perspectives

Nation-state threats and their implications might not be viewed in equal measures of severity and importance by those with oversight of emergency management agencies. Governors, mayors, commissioners, legislators, and other officials may differ with their emergency management professionals' risk assessments and prioritization of nation-state threats. Even emergency managers may disagree with each other along these lines and differ as to where the focus of their efforts should be or how to spend money and time. The public's perception of these threats also shapes the discussions and debates surrounding the distribution of resources and attention.

All these perspectives intersect and interact in complex and sometimes unpredictable ways. A governor's perspective on what an emergency management agency should focus on may differ from guidance in a federal grant designed to prepare for nation-state threats. National defense priorities can conflict with traditional disaster response and preparedness efforts. Perceptions of urgency, seriousness, and prioritization of nation-state attack preparedness are as varied as the organizations required to collectively respond to them.

The Next Step

Some paths and challenges that emergency managers consider are foundationally based on perceptions of victory. Nation-state attacks are real and credible as well as confusing and complex. The first question may be more philosophical but might help guide further strategy and effort: *How would the emergency management community define success in light of the growing threats of nation-state adversaries?*

In Part 2, learn how emergency management decision-makers at all levels might address the implications of foreign threats within the U.S.

Glen Woodbury is an adjunct international/defense researcher at RAND, a nonprofit, nonpartisan research institution. He is also a professor of the Practice Emeritus at the Naval Postgraduate School's Center for Homeland Defense and Security and was their director for 17 years. He served as the director of the State of Washington's Emergency Management Division and is a past president of the National Emergency Management Association as well as a former U.S. Army signal officer.

©October 2024 Texas Division of Emergency Management

Source: Generated with AI by typepng/Adobe Stock.

Growing Foreign Threats to National Security, Part 2: Emergency Management Approaches and Choices

By Glen Woodbury

Part 1 of "Growing Foreign Threats to National Security" addressed challenges and highlighted four nation-state threat actors and their relevance to the emergency management practice. The next step is to prepare for and mitigate these threats at the state and local levels in partnership with federal agencies and private entities. External and internal factors influence the decision-making abilities and calculations of emergency management leaders. Given these threats and their potential implications, an initial emergency management approach could use the following methodology:

1. Increase understanding and awareness,
2. Evaluate urgency and criticality,
3. Maintain flexibility, and
4. Create a decision framework.

With the evolving and complex nature of this threat landscape and the constant changes within the broader context of emergency management, these steps may occur concurrently while continuously considering new, incoming information.

Increase Understanding and Awareness

There is an uneven awareness of nation-state threats and their impact on emergency response and preparedness among emergency management leaders and personnel. Unlike a natural disaster, which can more easily be dissected and researched, data for nation-state threats are simultaneously partially classified, owned by multiple entities, and reliant on national security perspectives and global political interests. Each emergency management organization across the U.S. has different levels of access and

©October 2024 Texas Division of Emergency Management

permissions to information about nation-state threats. However, much of the intelligence and relevant analysis necessary to address these threats is openly available, and the profession should not wait for either a massive personnel security clearance process or for the nation to solve the longstanding challenge of sharing information across multiple sectors, agencies, and professional disciplines.

While some form of nationwide effort to inform and educate the emergency management profession is necessary, each organization should find ways to inform their personnel as much as possible, as they would for any new potential hazard or threat to their communities. Skepticism about the threat's relevance and a resistance to change are natural as the potential to redirect resources from current priorities becomes a compelling, but not necessarily optimum, option. Uninformed reactions to these threats and their implications impede effective preparedness and may unintentionally increase risks and vulnerabilities.

Evaluate Urgency and Criticality

The analysis of effects and implications of nation-state threats listed in Part 1 of this article should be customized to each jurisdiction. Once a better understanding of the threats and their implications are known for a specific jurisdiction, some methodology to include that information within the context of all that a jurisdiction prepares for is necessary. Realistically, initial decisions will be experience-based intuitive calls by the emergency management leader to determine if this is a "stop the presses" moment or if the data fall short of a crisis-level re-direction of resources and people. What should then follow are a deliberate analysis and thoughtful decision-making as to where the nation-state threat fits within the larger contexts of a community's risk profile.

Existing tools and practices may assist in determining criticality and urgency in more deliberate ways. Agencies can consider inserting nation-state threat information into the following existing risk assessment tools: such as the Threat and Hazard Identification and Risk Assessment (THIRA) process; predictive analysis tools used by fusion centers; the Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognizability (CARVER) model; and war-gaming or red-teaming exercises.

Another critical factor for emergency management decision makers to consider is the *source* of demands for action in response to nation-state threats. For example:

- Is the "boss" calling for this threat to be taken more seriously than others? Or less? (The perspectives of the governor, mayor, commissioner, chief, etc., might not align with their emergency manager's assessment of where nation-state threats fit in the spectrum of resource and effort dedication, potentially creating friction between them.)
- Is action being called for by entities and agencies that, while influential, do not have direct authority over the emergency management organization? (For example, while a state's military department, National Guard leaders, or law enforcement officials may call for the emergency management agency to pivot toward these threats, they may not have command and control over the agency,

©October 2024 Texas Division of Emergency Management

nor, in many cases, should they, just because of these threats.)

- Is the call for action coming from those who fund the emergency management organization? (If not, who has authority to redirect funding toward preparation for and mitigation against nation-state threats? Who is responsible for notifying the appropriators or funders of emergency management programs that an agency is shifting its resources?)
- Is grant guidance requiring it?
- Is grant guidance allowing it?

The quickness to act and the priority level of the threat, in some way, is driven by a combination of expert intuition, deliberate analysis, and external influencers. Each individual emergency management organization may evaluate these factors and respond differently from each other.

Maintain Flexibility

Complex problems require adaptable courses of action. A higher prioritization of resources to face immediate nation-state effects is obvious, such as a cyberattack on a dispatch center or misinformation disrupting an effective emergency response. Acting in the moment and making decisions during crises are traits of the emergency management profession. However, prioritizing resources to *prepare* for nation-state threats is more challenging, as it often involves re-directing an agency's resources and focus in varying degrees, depending on the specific context of each threat to the jurisdiction and its ability to adapt.

The more difficult aspect of prioritizing in the face of nation-state threats is that the probabilities and severities of such incidents vary in type (vector and magnitude), space (location), and time (imminent or remote). So, while one jurisdiction might see the need for a complete pivot toward these threats in the near and long-term (e.g., Guam under missile threats), other jurisdictions might foresee little exposure or minimal community-wide impacts that would require any significant change in operations and organization. Therefore, federal and other "upper echelon" guidance should consider that, while there may be some baseline requirements for all jurisdictions, the actions necessary for each are context-dependent. Additionally, the fluid nature of nation-state threats requires that jurisdictions frequently re-evaluate their relative risk and emergency management priorities while maintaining their flexibility and adaptability.

Create a Decision Framework

Practical decision frameworks for complex situations do not need to be created from scratch. The Cynefin Framework and its area of research are particularly useful for the nation-state adversarial environment. It is a "sense-making" model that can help categorize potential decision paths yet be flexible as information and situations change. Following is an example of how this framework could be applied to the nation-state challenge.

Simple or Obvious

Some actions and techniques may be used in other areas that are also easily applied or modified for the nation-state context. Identifying simple and/or obvious efforts often reveals the easier and more cost-effective actions to prepare for, prevent, and mitigate

©October 2024 Texas Division of Emergency Management

consequences. Most of these decisions are in operational and tactical areas but not solely. Decisions about what is simple or obvious might include training and exercise adjustments with unique-scenario attributes of a nation-state attack, such as dealing with misinformation. Other simple or obvious areas might include reassessing the relationships that emergency management offices need to work with on these unique contingencies. For example, increased interactions with fusion centers and military authorities may be necessary. Conducting agency- or system-wide briefings on nation-state threats and implications can be easily developed to increase general awareness. Best practices usually exist within this sense-making stage that can aid in quick implementation. Efforts might include the following:

- Updating public information training modules to reflect current examples of nation-state influence operations and information interference to teach best, or smart, practices in responding to them.
- Updating and presenting threat and hazard briefings to the emergency management organization's personnel, its partner agencies, and its stakeholders, including nation-state threat information and potential consequences.
- Including nation-state interference assessments as a required component of traditional situational awareness elements and briefings.

Complicated

Some activities and decisions require expertise or analysis not currently in place or not readily applied to the context of a nation-state threat. Tools and processes can be used or modified to better understand the potential implications and consequences of nation-state influences and attacks. Mapping or diagraming the vulnerabilities of essential supply chains or the cascading impacts of cyberattacks takes time and resources. Many processes already exist, but where this expertise lies may have to be discovered and employed. There are complicated but achievable actions that might include these examples:

- Requesting assistance from national laboratories to dissect and map out dependencies of critical infrastructures that might be targeted in nation-state attacks, such as is done by the Idaho National Laboratories All Hazards Analysis project.
- Determining which new essential elements of information regarding nation-state threats should be added to multi-hazard and intelligence fusion centers.
- Deciding what and when to include nation-state injects into traditional and scheduled exercises as well as when (and how) to resource and conduct nation-state specific scenario exercises.

Complex

Decision-making and difficult choices are often more time-consuming and resource-intensive when decisions involve interacting variables where uncertainty and evolution are

©October 2024 Texas Division of Emergency Management

constant. The players and actors in this domain may be new or have different roles than other traditional emergency management-related efforts in the context of nation-state threats. However, because the nation-state impacts and choices for the emergency management community might be considered "wicked problems," the techniques used in complex decision-making would be appropriate. Complex choices would include discussions of doctrine and strategy:

- Are authorities "right-sized" and "right-applied" for nation-state threats?
- What level of wholesale organizational changes are necessary, if at all?
- What national systemic changes are necessary to prevent, mitigate, respond to, and recover from attacks?

Identifying complex challenges and issues helps guide the effort and investment required to improve, if not solve, them. Complex problem-solving takes more time, involves negotiation, anticipates uncertainty, requires trial-and-error processes, and demands adaptability and flexibility. Some examples of complex problems to address include:

- Deciding on the appropriate messages and public information campaigns for a community, given nation-state threats, uncertainties, and levels of information security.
- Figuring out and designating the "center of gravity" for preparing the U.S. and its communities for a nation-state threat environment at all levels of government. A closely related challenge of deciding who will be "in charge" at each jurisdictional level in events that cross disaster response, criminal investigation, and national security divides must also be considered.
- Postulating and assessing the cascading effects from a complex incident involving nation-state attacks and the potential vectors that an enemy could employ.

Chaotic

This area of the Cynefin Framework is where decisions and choices are made to stabilize a crisis in progress. Emergency management leaders may employ resources or dedicate agency focus without significant deliberation or input. "Do *something*" is a mantra for situations where lives might be jeopardized and no clear answers or past practices are evident. In this area, the application of authorities, such as imminent life-safety responses from military forces, may be required, which shortens the timeframe for the more deliberate request for "Defense Support to Civilian Authorities" process. Examples include the following:

- Provide life-saving search and rescue after a kinetic attack on a population or soft target.
- Respond to critical and urgent shortages of medical or life sustenance supplies.
- Restore power to critical infrastructures such as trauma centers and first response facilities.

Disorder

When emergency management professionals are unsure of what type of nation-state

©October 2024 Texas Division of Emergency Management

threat they are dealing with (e.g., simple or complex), they may require more information, input, and deliberation. For example, does the response to election interference from a foreign actor have simple and obvious tactics, or are there complicated and complex areas as well? Disagreement and discussions among participants in this process about which domain an issue may best be placed in are actually very beneficial. Arguments encourage diverse views and opinions that often reveal new information and insights as well as create potentially innovative and novel approaches.

Regardless of the domain from which decisions and actions may come, it is also important *not to* solely rely on "worst-case scenario" planning, as this type of preparedness methodology may miss important nuances and consequences that fall short of a catastrophic threshold.

A final emphasis of the Cynefin sense-making model is the caution to not prefer or bias decisions in search of simple and obvious answers. Many of the issues that emergency managers deal with in the nation-state dynamic are not solved with existing practices or "silver bullet" ideas. Any one entity trying to force what they believe to be the "right" answer on others can create more confusion and animosity, rather than beneficial solutions.

Making Choices

This discussion should help inform whether the profession or individual jurisdictions should take the path of gradual absorption of these threats into current efforts or demand a full pivot to different priorities, focus, and expenditures – or something in between these options. Identifying low-hanging fruit often found in the simple or obvious may be the most pragmatic and cost-effective initial path. At the same time, more complicated and complex choices demand greater collaboration and interaction with entities within and new to the traditional ecosystem of the emergency management profession.

The approach and frameworks presented in this article are intended to be a starting place for emergency management professionals and organizations. As such, further iteration and progress towards greater resilience and security against nation-state threats to our communities will need to follow.

Glen Woodbury is an adjunct international/defense researcher at RAND, a nonprofit, nonpartisan research institution. He is also a professor of the Practice Emeritus at the Naval Postgraduate School's Center for Homeland Defense and Security and was their director for 17 years. He served as the director of the State of Washington's Emergency Management Division and is a past president of the National Emergency Management Association as well as a former U.S. Army signal officer.

©October 2024 Texas Division of Emergency Management

Source: Yury Zap/Adobe Stock

Tren de Aragua: From Prison Gang to Transnational Organized Crime Syndicate in the U.S.

By Anthony (Tony) Mottola and Dan Scherr

The United States (U.S.) has never been shielded from transnational organized crime syndicates or transnational street gangs operating in its borders. Historically, as hard-working migrants entered the U.S. in search of the "American dream," gang members have been embedded within the fleeing migrants. Researchers have long studied this phenomenon, and one theory is called the "importation model," which suggests that gangs or criminal organizations entrench members among hard-working migrants to engage in criminal activity and expand their organizations. Transnational criminal organization Tren de Aragua (TdA) has become a paradigm of this theory as its operations spread from Venezuela across Latin America to the U.S. due to loose border regulations.

More than eight million Venezuelans are fleeing the autocratic reign of Nicolás Maduro's regime. Federal and local authorities fear that TdA members are embedded in these communities. In a report published on June 7, 2024, the U.S. Department of Homeland Security's Office of Inspector General reported the shortcomings of the U.S. Customs and Border Protection and U.S. Citizenship and Immigration Services' screening and vetting processes. The report noted both agencies' challenges when verifying identities and ensuring that bad actors are not admitted into the country. Additional technology (e.g., surveillance facial recognition and DNA collection and procedures), better collaboration and coordination with federal, state, and local partner agencies, and more connections within migrant communities to build awareness of this transnational threat and its historical background are needed.

History of Tren de Aragua

TdA emerged from the Aragua Penitentiary Center (the Tocorón prison) in Aragua,

©October 2024 Texas Division of Emergency Management

Venezuela. The group grew from a prison gang under founding leader and fugitive Hector Rusthenford "Niño" Guerrero Flores. Guerrero was serving a 17-year sentence for crimes that included murder and the trafficking of narcotics. The gang was able to flourish in Tocorón as the Venezuelan government and local authorities took a hands-off approach. Investigative journalists conducted extensive research and determined that the Venezuelan government had bargained with prison gangs to allow them to police the prisons themselves with little oversight from the Ministry of Prisons. This allowed the prisoners, gangs, and especially TdA to run the prison through intimidation and fear.

Guerrero and the Tocorón prisoners turned the jail into the gang's fortified palace, featuring a local casino, a nightclub, a restaurant, a swimming pool, and even a zoo with exotic animals. Sophisticated tunnels under the prison allowed prisoners and locals to come and go without detection, which enabled TdA to amass weapons within the facility. The gang's ability to influence government officials and control prisons is a concern when arresting and processing members in U.S. state systems. Law enforcement, courts, and corrections personnel must be aware of TdA's capabilities to foster misconduct and bribe officials as a general course of their business.

In February 2023, veteran journalist Ronna Rísquez exposed the gang's control of the prison, forcing the government to raid it in September of that year. Officials verified TdA's luxury accommodations in the prison and discovered a stockpile of military-grade weapons, including explosives, hand grenades, machine guns, and ammunition. Four ranking prison officials arrested during the raid identified government representatives under the gang's control. Gang leader Niño Guerrero was tipped off and fled with approximately 100 leaders and members of the gang. He is currently a wanted fugitive by Interpol.

The state of current migration to the U.S. raises the question: Have these missing gang leaders crossed into the United States? The U.S. Customs and Border Protection and local law enforcement agencies must work together to identify TdA fugitives and other gang members in the refugee and migrant relocation process. U.S. agencies responding to emergencies in immigrant communities should be aware of the gang's ability to manipulate residents through fear and intimidation into not speaking to officials. To overcome this, human intelligence and confidential informant programs are essential.

Since 2012, TdA has been expanding its operations in three criminal phases. In the exploration phase, the group focuses on migration routes, exploiting a need for their services. Once they set up shop in an area, violence soon follows with murder, dismemberment, forced prostitution, and robberies. The group then moves into the penetration phase with crimes such as extortion, trafficking for exploitation, kidnapping, and loan sharking. In the consolidation phase, the group corrupts local security forces, subsumes rivals (such as taking on Colombia's foreign terrorist organization, the National Liberation Army), and focuses on money laundering and securing their positions. Countries such as

©October 2024 Texas Division of Emergency Management

Chile, Peru, Brazil, and Mexico have been subject to the gang's expanding network of trafficking humans, children, narcotics, and weapons.

Tren de Aragua's Expansion

In Venezuela, TdA's growth did not occur in a vacuum. The state allowed the group to establish influence and control at the Tocorón prison and regionally, creating a hybrid state. The evolution of this state of governance can be traced back to the rule of Venezuela's former president, Hugo Chavez, but it has been exploited in recent years by TdA. The gang funds a nonprofit organization, Somos El Barrio JK ("We are the Barrio JK"), that serves as the organization's public face. It sets rules and regulations, provides services in the controlled areas, and enforces compliance, acting as a second government. These areas coincide with Venezuela's so-called "peace zones," where the central government agreed to limit police operations as long as local groups keep violent crime down.

Colombia has long been a stopping point for migrants heading north to the U.S.-Mexico border. Colombia and Venezuela's porous borders have been home to Venezuelan migrants fleeing poverty, violence, and an authoritarian regime. Migrants utilize the dangerous and precarious jungle through the Darian Gap that connects Colombia and Panama. It is estimated that in 2023, approximately 520,000 migrants crossed the Darian Gap, with Venezuelans accounting for 209,000 of those migrants in the first half of the same year. TdA has taken advantage of these migrants through sex and labor trafficking. From 2019 to 2021, the gang fought the National Liberation Army for control of the border with weapons and tactics reminiscent of larger transnational organized crime syndicates. TdA's strategy was to obtain military-grade weapons and threaten locals with violence by posting executions on social media platforms.

TdA violence has crossed from South America into U.S. communities. Local police agencies have confirmed TdA's presence in Colorado, Florida, Georgia, Illinois, Louisiana, New Jersey, New York, Texas, and Virginia. As of the last week of September 2024, there are over 100 investigations nationwide involving suspected TdA associates. In January and June 2024, multiple New York City Police Department police officers were shot or assaulted by TdA members. In Miami, a TdA member was arrested in January 2024 for the 2023 murder of a former Venezuelan police officer living there.

These attacks, along with a memo from the Homeland Security Investigations office in Chicago warning of an active threat to law enforcement officers, show the gang's lack of concern for law and order. The growth of transnational organized crime syndicates' criminality (e.g., human and fentanyl trafficking) and terrorism in the region has led the New York City Police Department Intelligence Division to post law enforcement personnel in Bogotá to collaborate with local officials. Comparable to the New York City Police Department, the first stage of combating TdA for law enforcement is through the gathering of intelligence, databasing, and investigating their criminal activity.

©October 2024 Texas Division of Emergency Management

TdA's Social Media

The level of brutality and tactics used by TdA has been described as a throwback to the "bad old days" of cartel violence and turf wars. The range and reach of violence, however, is amplified by the gang's use of social media. Social media is a critical component in taking over new territory and controlling the target population, as evidenced by broadcasting the killing of a person being shot 31 times. While the group is comfortable utilizing violence to further its goals, these messages and online behaviors can avoid outright confrontations with opposing gangs, and it demonstrates their resolve and willingness to commit unspeakable acts.

TdA also uses the internet in various ways. In Venezuela, known for its beauty pageants, the organization recruits young women with promises of cash, jobs, and other incentives to compete in pageants. These recruiting pitches are posted online, and potential contestants are invited to attend parties the organization hosts. These women are then forced into sex trafficking locally or into cross-continent trafficking operations.

The group also steals cell phones in New York, then recruits members through social media to use those stolen phones to empty bank accounts and commit identity theft. The phones are then wiped and sent back to gang members in South America and sold. To communicate with members across New York City, the group relies heavily on WhatsApp, an end-to-end encrypted messaging service. The stolen phones and the encrypted messaging service continue the recruitment cycle for sex work and trafficking, reinforcing the criminal throughput from origin to destination.

Criminal Designations

On July 11, 2024, the U.S. Department of the Treasury designated TdA as a significant transnational criminal organization based on the group's threat to the United States and the region. Under this declaration, all property or interests in property of the group were blocked and must be reported to the Department of the Treasury's Office of Foreign Assets Control. The same day, the U.S. Department of State issued a $12 million reward for TdA leaders, and $5 million of that is specified for the capture of Niño Guerrero.

On September 16, 2024, Texas Governor Greg Abbott reiterated the State Department's declaration of TdA as a transnational criminal organization. He announced the launch of a campaign to crack down on TdA and other groups across the state. He upgraded the organization to a "foreign terrorist organization" in Texas. This campaign includes directing the Texas Department of Public Safety to create strike teams across law enforcement agencies to target the group's activities and create a database of TdA members. This comes as members of the organization have been accused of kidnapping, extortion, trafficking, and other crimes in Houston, El Paso, and across the state.

Deportation and Cooperation

On September 12, 2024, the U.S. imposed economic sanctions on the Venezuelan government, leading to the regime halting the acceptance of deported Venezuelans back to their country. Without the country's consent, the U.S. cannot deport illegal migrants to their home country. Venezuela, like so many other countries (e.g., China, Russia, Iran, Iraq, and

©October 2024 Texas Division of Emergency Management

Cuba), does not provide background checks for their citizens captured in the U.S. illegally. Furthermore, the U.S. must allow them to stay in the U.S. if they claim asylum, even if the migrants have broken border laws or committed crimes.

TdA rapidly grew from its local origins in Venezuela to a multinational organized crime organization spanning South, Central, and North America. The group has demonstrated its violent disregard for laws, life, and human decency and its focus on consolidating its power and maximizing profit using drug trafficking and extortion to more modern cybercrimes.

The violence TdA has demonstrated in the U.S. is severe and ongoing. With the challenges the U.S. Customs and Border Protection and U.S. Citizenship and Immigration Services face vetting those seeking to enter the country, groups like TdA will continue to be a threat. The intelligence community must recognize the nature of that threat and understand TdA's operations to create a plan to identify gang members. Federal, state, and local law enforcement agencies, prosecutors, and government officials must work together to prevent the further spread of TdA's crimes and hold its members accountable for their actions.

Anthony (Tony) Mottola, Ph.D., has over 35 years of law enforcement and security experience, including the New York City Police Department, United States Air Force, and the National Basketball Association. He retired as a sergeant detective (SDS) after 25 years as a member of the New York Police Department (NYPD). He served as executive officer for the NYPD Intelligence Bureau's Strategic Unit, which is a covert counterterrorism initiative, and director of the Domestic Liaison Program. He represented the Intelligence Bureau in numerous investigations, including the Boston Bombing, civil unrest, mass shootings, and large-scale incidents outside New York City. During his tenure with the NYPD, he worked additional assignments in Counter Terrorism, Gang Intelligence, Detective Bureau, Task Force, Street Narcotics Enforcement Unit, anti-gang/graffiti units, and patrol. He was a first responder/search leader for recovery efforts and supervisor of security details in the immediate aftermath of the World Trade Center attacks. Dr. Mottola has conducted extensive research into human trafficking, labor trafficking, border operations, and transnational organized crime. He is currently an assistant professor of Criminology and Homeland Security at the University of Tennessee Southern.

Dan Scherr holds a Ph.D. in Public Policy Administration with a terrorism, mediation, and peace focus. He is an assistant professor in Criminal Justice and Homeland Security at the University of Tennessee Southern and program coordinator for the Cybersecurity Program. He is also a co-director of the Honors College. He is a Certified Fraud Examiner and Army veteran who served stateside during the September 11th attacks and has over two decades of experience in homeland security and operations.

©October 2024 Texas Division of Emergency Management

Advisory Board Spotlight: Interview With Ray Barishansky, DrPH

Ray Barishansky, DrPH, is on the advisory board for the *Domestic Preparedness Journal* and has a passion for public health and emergency management. He sat down with the *Journal's* Nicolette Casey to share the story of his journey from an emergent medical technician to a doctor of public health.

Nicolette:

What inspired you to join the Domestic Preparedness board?

Dr. Barishansky:

I started writing, originally, for *Domestic Preparedness Journal* [*Journal*] in either 2008 or 2009. I was getting my feet wet regarding the still-emerging discipline of public health preparedness. I had just moved to the Washington, D.C.–area, and I started writing articles. I was communicating with Cathy Feinman [editor of the *Journal*] and some other advisors on the Domestic Preparedness board in the 2012-2013 timeframe. I had various work obligations and had to leave the board and when I had more time, I started writing again, and a whole bunch of my articles made their way into the pages of the *Journal*. Cathy reached out to me in the beginning of this year and asked if I would rejoin the board, and I was more than honored to. I think the message

©October 2024 Texas Division of Emergency Management

that the *Journal* brings out to practitioners is extremely important, and I consider it a privilege to be on the board.

Nicolette:

That is wonderful. I am so glad to hear that, and we're fortunate to have your perspective. You lead me to my next question: What do you see as the biggest challenges and opportunities in emergency preparedness right now from a public health lens?

Dr. Barishansky:

I think right now we are in a really interesting time in what I'll call the post-COVID era, even though I think COVID is still a threat as it moves from pandemic to endemic. But I think that, in general, we are not seeing the same number of people sick or dying from COVID, and public health preparedness has gone from being a front-page issue to once again being a back-burner type issue.

It is sad to see this because even though we have seen things like a resurgence in COVID and even Mpox, we've seen things like that that clearly impact the public's health and clearly show the need for the public health preparedness efforts we're seeing. There are impacts in regard to funding, and then when we don't have enough funding, the first thing that gets cut is personnel. And then, when you start cutting things that are infrastructure-based, such as personnel and other programs, it will impact your overall preparedness. It is sad right now, but we're seeing this strange domino effect of people who are forgetting what public health is and what public health professionals did during the COVID pandemic.

Nicolette:

That is an excellent point. Now, can you share a bit of your background and how it ties into emergency preparedness?

Dr. Barishansky:

Sure. So, mine is kind of interesting. I started off as an emergency medical technician (EMT) in northern New Jersey, and I was a volunteer, and it kind of was one of those things that really helped me pull it all together.

I got a paid position as an EMT as well and became a supervisor. And most of my background was really related to emergency medical services (EMS). One of the things I saw is that decision makers, policymakers – they were all people with structured degrees. And so my EMS background really helped push me to finish a long, lingering bachelor's degree and then move toward a master's in public health.

I was in EMS administration, but I took a job in public health preparedness. And it was eye-opening. People were driving initiatives in public health preparedness, and it was great.

It was great to see, and it really gave me an opportunity to kind of, you know, get my feet wet in public health preparedness. My career has kind of been on two separate tracks. It's been in EMS but also in public health preparedness, and my last position before I became a consultant was as a deputy secretary of health in the Commonwealth of Pennsylvania. Two of the bureaus that I oversaw were EMS and public health preparedness.

And it was really kind of an interesting moment where I got to see two of my, let's say, occupational loves, for lack of a better term, coming together and seeing the team really work together toward shared goals.

©October 2024 Texas Division of Emergency Management

Nicolette:

What is one key takeaway you'd like to share with our readers about staying prepared?

Dr. Barishansky:

I would tell people to not focus on the last event. I think that's one of the pitfalls that we tend to fall into in emergency preparedness. We tend to think of the closest thing in the rearview mirror. But at the same time, there are so many other things that we should be focusing on. I think that true preparedness isn't about focusing on the last thing, but true preparedness is understanding the systems, the personnel, the infrastructure, and everything that goes into it. And so, you know, if we focused only on, say, COVID, we might not be as prepared for something like Mpox, or even for a natural hazard, with significant public health impact. We need to look at things holistically. We need to look at them in totality.

Nicolette:

To focus on what is to come, we have to be able to learn from what worked and what didn't. That is what Domestic Preparedness is all about. Would you agree with that?

Dr. Barishansky:

I totally agree with that. I think it's about looking at what worked and then also what did not work but understanding why it didn't work. It is not about how you trip and fall. It is about how you pick yourself up and dust yourself off. We really need to focus on the moments where things did not go as planned – what we did about it and how we persevered.

Nicolette:

Do you have a specific article that you particularly enjoyed writing for the *Journal*?

Dr. Barishansky:

The one that I would say I really enjoyed writing was "Are Public Health Agencies Ready, or Just Prepared?" It made a clear delineation between what preparedness is and what readiness is and how, in the beginning of the discipline of public health preparedness, when it was okay to be prepared, because we were kind of finding our legs. But we've moved into a much different era. And at the risk of repeating myself, as we look at things like COVID or Mpox – and even if they're not public health-specific – we need to very clearly move to a state of readiness. Being able to write that article, actually, I felt very proud of that article.

©October 2024 Texas Division of Emergency Management

Nicolette:

Do you have any advice for someone who is new to the field?

Dr. Barishansky:

I do. Speak to as many people as possible and learn as much as possible. When I got my position in Prince George's County, Maryland, I was the chief of public health preparedness. I very quickly realized what I didn't know. And it was a lot. And speaking with people around D.C., learning as much as possible, asking as many questions as possible, really was the difference between success and failure.

And I had a lot of great mentors and a lot of people who showed me the way. But we are all in positions, or we all potentially could be in positions where we just don't know as much as you thought. Those are the moments where you need to stop, reflect, and ask as many questions as possible to then figure out your own personal and professional answers and move forward with them.

I also can't say enough for structured educational programs. There are so many good ones out there specific to emergency management, public health preparedness, and areas just like that. And it is really important for our professionals to be well-trained and well-educated.

Nicolette:

Do you have anything that you would like to say just to finish up here about your time with Domestic Preparedness? What do you see on the horizon in emergency preparedness? Is there anything you would like to leave us with?

Dr. Barishansky:

I have always been impressed by the *Domestic Preparedness Journal*, and the staying power of the *Journal* is extremely impressive to me personally and professionally. I think that as we move forward, one of the things that we need to focus on in the disciplines of emergency preparedness is succession planning and really picking out the next round of leaders and making sure that they are as well-trained as possible, so they can pick up the reins potentially when we're not there to pick them up. This is an area where some professions are lacking. I am not saying all, but some are. And as we move forward, we'll need to focus on that overall as a profession, as well.

Nicolette:

Thank you so much for your time.

Raphael (Ray) M. Barishansky, DrPH, is a public health and emergency medical services (EMS) leader with more than 30 years of experience in a variety of systems and agencies in positions of increasing responsibility. Currently, he is a consultant providing his unique perspective and multi-faceted public health and EMS expertise to various organizations. His most recent position prior to this was as the deputy secretary for health preparedness and community protection at the Pennsylvania Department of Health, a role he recently left after several years. Mr. Barishansky recently completed a doctorate in public health at the Fairbanks School of Public Health at Indiana University. He holds a BA from Touro College, a master of public health degree from New York Medical College, and a master of science in homeland security studies from Long Island University. His publications have appeared in various trade and academic journals, and he is a frequent presenter at various state, national, and international conferences.

©October 2024 Texas Division of Emergency Management

Advisory Board Spotlight: Keeping It Real With Lynda Zambrano

Lynda Zambrano is on the advisory board for the *Domestic Preparedness Journal*. Lynda is the executive director of the Northwest Tribal Emergency Management Council and the National Tribal Emergency Management Council, and has been inducted into the International Association of Women in Emergency Management's Hall of Fame. She sat down with *Journal* Editor Catherine Feinman to share her story.

Cathy:

I am here with Lynda Zambrano, the director of the National Tribal Emergency Management Council, and we are doing an advisor spotlight to highlight what she's done to further the emergency preparedness profession and what advice she has for other people in the field.

Lynda, what inspired you to join the Domestic Preparedness board?

Lynda:

When I first heard about the board, I was very excited that we had a new venue to share and distribute information to people. I was inspired to join the board when I learned about the caliber of some of the other advisors who would be sitting on the board and the work we would have the opportunity to do. I knew that anytime we could encourage people to submit articles and share the important work they were doing with the rest of the country, it would benefit

©October 2024 Texas Division of Emergency Management

many. Any small part I could play in helping to review those articles, provide feedback, and assist authors in making their work more digestible felt like a great opportunity to share my skills. Everything about this project has been inspiring to me from the beginning. I've been very blessed and humbled to be a part of it, and I'm very grateful for the time I've had to work on all we've achieved together, as an advisory board member.

Cathy:

You have done so much to prepare and launch initiatives. Can you share a bit about your background, including some current initiatives you're working on and how they connect to emergency preparedness?

Lynda:

I've been working in the emergency management field for close to 35 years. I started with the Snohomish Sheriff's Department in the block program, where I worked for 15 years. As part of the program, we took on crime prevention, and we needed something to keep volunteers motivated. We introduced Community Emergency Response Team training, which usually falls under emergency management, not law enforcement. That was something we could bring to the community level, which was very exciting because it's where the program belongs.

While running the block program, I started working for the Tulalip Tribes, initially in the health clinic for five years, before transferring to the police department for the next five years. At the police department, I helped create our first office of emergency management. From there, we were one of the first Tribes in the nation to start drafting, writing, and receiving grants such as the Tribal Homeland Security Grant, the State Emergency Management Performance Grant, and many CDC grants. Other Tribes were interested in our approach, so one day, my Tribal chief of police handed me a set of car keys and asked me to drive to the other seven Tribes in our region to encourage them not only to attend our next Homeland Security meeting but to understand why it was so important for them to be there.

I often say that my proudest moment in the last 35 years was attending a Region 1 Homeland Security meeting, surrounded by seven uniformed chiefs of police. We showed unity and mutual support by attending together. In 2008, our group decided it was essential to incorporate and become a 501(c)3 nonprofit. Our Tribes understood that we were doing this work free of charge, and in 2010, FEMA recognized our efforts. They asked about the possibility of creating a national organization to support Tribes across the country. That year, our board of directors voted to expand our work and engage all 574 Tribes through our website, Facebook, Zoom calls, online training, and annual conferences.

That brings us to today, at our 21st annual National Tribal Emergency Management Conference, where we are sharing many current projects and initiatives, including our newest endeavor a National Tribal Emergency Management Council Innovation Center. This think tank will allow people to develop ideas they've long wanted to grow but didn't know how to approach. We'll have a 1-800 number for Tribes to call, seeking grants or assistance with writing and reviewing grants.

We're also covering each of the 15 emergency support functions established under the National Response Framework, with subject matter experts assigned to each function. This means anyone can call and request assistance with any emergency support function, and we'll have someone ready to answer or find the information needed. Our Innovation Center is one of the most exciting things we're working on for the next 12 months. Additionally, we plan to establish a university, journal, printing house, and library. One of our degree offerings will be a master's in research, allowing students to access valuable elder collections

©October 2024 Texas Division of Emergency Management

of information never released publicly, housed in the library we're creating. Big things are coming in the next few years.

Cathy:

There's no shortage of projects over those past 35 years! What have you found to be the biggest challenges and opportunities?

Lynda:

The biggest challenges have been funding. When the Department of Homeland Security funding was allocated, it was divided among the states. FEMA is state-centric, so the funds went to states, which then distributed them to counties. Since counties hadn't worked with Tribes before, they didn't know how to get the funds to the Tribes. For example, in Region 1 in Washington, all eight Tribes received meeting invitations, but none had emergency managers then, so those invitations went unanswered. Consequently, all the counties sent their emergency managers, while the Tribes received nothing.

When I attended that first Homeland Security meeting, I brought the budget details back to the chief of police, explaining that we could accomplish so much more with just $200,000 of the $5 million allocated. We could hire part-time staff, draft emergency management plans for all eight Tribes, and help them meet mandatory document requirements. Without anyone at the table speaking on behalf of the Tribes, the chief gave me car keys and told me I would attend every future meeting, help create an office of emergency management for the Tribes, and assist any other interested Tribes in doing the same.

I was so proud to attend that meeting with the seven chiefs of police, showing unity and belief in our mission. Ironically, the counties were nervous because, according to the charter bylaws, we had equal voting rights. Although we had the majority, we weren't there to take the full $5 million but to create a more level playing field, allowing us to build our emergency management offices and share resources. With 574 Tribes across the U.S., I saw these as potential security gaps, and if we're serious about protecting our nation, it's essential to address Tribal needs and engage them fully. This was the start of the Northwest and eventually the National Tribal Emergency Management Council (NTMC).

The greatest opportunities in emergency preparedness today come through NTMC. Not only have we helped set up emergency management programs nationwide, but we've also brought valuable skills, resources, and grant money. We've written hundreds of millions of dollars' worth of grants that went directly to Tribes, helping them build their preparedness infrastructure.

Cathy:

Throughout all those experiences, is there one key takeaway about preparing for an emergency or disaster that you'd like to share with readers?

Lynda:

There are so many it's hard to narrow down! Key takeaways for readers about staying prepared: Share the link to the Domestic Preparedness Journal and stay engaged with it. The Journal does a fantastic job of sharing our work and that of similar organizations. By staying connected, you'll be far more prepared than you otherwise could be, so stay engaged with the Domestic Preparedness Journal, and you'll be much better off in the end.

Cathy:

With the next generation coming into the field, what advice do you have for them?

Lynda:

For Tribal emergency managers, I suggest starting with the National Tribal Management Council. We can guide them on federal organizations, resource acquisition, program

©October 2024 Texas Division of Emergency Management

development, and training. I highly recommend close collaboration with FEMA, the Department of Homeland Security, and Health and Human Services. People often forget that our largest disasters require us to work closely with the CDC. Our Innovation Center will also be available to support anyone entering the field, providing all the information we can share. However, as for sharing funding opportunities and grants, those are earmarked for our Tribal members and organization affiliates.

Cathy:

One more question. I've seen you engage people across disciplines and jurisdictions. How do you inspire and maintain enthusiasm, bringing together Tribes and non-Tribes alike?

Lynda:

I strive to keep it real. Emergency management should be like brushing our teeth daily—a natural part of life, not an extra chore. For example, my son visits me in the hospital daily. He's someone who doesn't see emergency management as an obligation; it's part of how he lives. When he comes in, he wipes down the mattress before they change the bedding, then cleans the bedframe. It's not something he's checking off a list; it's just part of life. People's lives are already so full, so if we can integrate emergency management as something natural rather than another item on their to-do list, more people will engage.

Using real-life experiences and learning about others' lives helps us find shared experiences. This common ground makes it easier to inspire people, regardless of who they are or where they come from. Returning to the question, keeping it real has been the key to inspiring so many.

Cathy:

Do you have any final thoughts you'd like to share?

Lynda:

I want to thank the *Domestic Preparedness Journal* and everyone involved, from the advisors to the top leadership. Cathy, I especially thank you for your years of support for the Journal, which has grown to be a far more significant asset than we ever imagined. With the future library, Tribal member scientist journal, and Tribal Innovation Center, we see the *Domestic Preparedness Journal* as a resource we can direct people to. I'm very grateful for that.

Cathy:

We can't thank you enough for everything you've done for us and the inspiration you've provided.

Lynda Zambrano currently serves as executive director of the Northwest Tribal Emergency Management Council and the National Tribal Emergency Management Council (NTEMC). She is an adjunct professor at Pierce College, Centers of Excellence for Homeland Security, authoring and teaching the Grants Writing and Management curriculum. She began her career in law enforcement 20 years ago, working with federal, state, local, and tribal governments. She has served as health director for several Tribal Nations, which provided a unique perspective to bring together different disciplines to work together in emergency management. She has an extensive background in finance, contracts management, and audit compliance. She is a grants writer, assisting with securing more than 100 grants and tens of millions of dollars for Tribal Nations in Washington state and across the country. She has received recognition for her work in Indian Country from the Federal Emergency Management Agency, U.S. Department of Homeland Security, and U.S. Bureau of Indian Affairs. She was inducted into the International Association of Women in Emergency Management's Hall of Fame. She helped co-found the Fresh Food Coalition and oversees food and supplies distribution in 35 states to over three million people.

©October 2024 Texas Division of Emergency Management


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