MARCH 2025 | AUSTIN, TX

THREATCASTING.AI

IN CASE OF FLOOD

IN THE AGE OF SOCIAL MEDIA, WHEN DISASTER STRIKES, THE CRISIS ISN'T LIMITED TO THE PHYSICAL DOMAIN. WHAT FLOODS ONLINE, FLOODS OFFLINE.

> “A crisis is a terrible thing to waste.”
>
> - Paul Romer

Threatcasting guards against strategic surprise.

When a crisis occurs, or an opportunity presents itself, a decision-maker is not caught off guard.

Instead, their reply is: ***“We have talked about this before. We know where to start…”***

TABLE OF CONTENTS

WHAT IS THREATCASTING?

Threatcasting is a strategic foresight methodology, developed in 2007 by futurist Brian David Johnson at Intel and further advanced by applied futurist Cyndi Coon, designed to help organizations and individuals navigate complex and uncertain futures. A descendant of scenario planning, Threatcasting draws from futures studies and military strategic thinking to provide a novel method to model the future. By using subject matter expert (SME) interviews, scenario planning, and operationalization exercises, Threatcasting equips decision-makers with actionable insights and strategies to anticipate and mitigate risks or capitalize on opportunities.

The methodology fills gaps in existing military futures thinking and provides a process to specify actionable steps as well as progress indicators. Threatcasting is inherently collaborative and human-centric. It provides a systematic, transparent, and collaborative approach to model a range of possible and potential futures.

At its core, Threatcasting is about equipping leaders to shape their futures with intention and clarity. It encourages leaders to move beyond reactive thinking and instead adopt a proactive, human-centered approach. This ensures that the futures we imagine and prepare for are not only technologically advanced but also equitable, sustainable, and reflective of our shared values. By embracing Threatcasting, organizations and individuals can transform uncertainty into opportunity, ensuring they are always ready to face the challenges and possibilities of tomorrow.

HERE COMES THE FLOOD

Greg Lindsay

In September 2024, Hurricane Helene made landfall in Florida's Big Bend, becoming the strongest — and deadliest — to strike the U.S. mainland since Katrina in 2005. As the storm churned northward into Georgia and the Carolinas, record rainfall in the Appalachian Mountains triggered catastrophic mudslides and flooding. More than 400 roads closed; bridges and passes were washed away along with entire neighborhoods and villages. Nearly a half-million residents of North Carolina lost cellular service and power, severing the hardest-hit communities for days, if not weeks.

Into this void of information flowed a tide of falsehoods. In one town near Asheville, NC — the epicenter of the disaster — rumors swirled that public officials were concealing the true death toll. Local authorities took to social media, pleading with the public to stop sharing "sensationalized" information. By then it was too late. Relief workers from the U.S. Federal Emergency Management Agency (FEMA) were soon welcomed with protests and death threats, requiring police protection even as they offered assistance.

This toxic convergence of climate catastrophe and information disorder wasn't coincidental, but representative of a pattern increasingly evident in American disaster response. As climate change increases both the frequency and intensity of extreme weather events and political polarization deepens social fractures, communities in crisis become targets for misinformation and disinformation alike, both organic and orchestrated.

The paranoia seen in North Carolina is the product of a compound disaster — one in which physical infrastructure collapse is amplified by a simultaneous breakdown of information ecosystems. The dual flood creates cascading vulnerabilities traditional disaster response frameworks were never equipped to address. When official communication networks fail, people naturally turn to the alternatives at hand. In this vacuum, unverified claims flourish, exploiting pre-existing distrust in neighbors and institutions.

What makes these disasters particularly troubling is how they've been weaponized by actors seeking to destabilize federal, state, and local governance. During Helene's aftermath, for instance, high-profile figures including then-former President Trump and tech billionaire Elon Musk amplified false narratives politicizing the disaster response. Intelligence analysts and experts later identified disinformation campaigns linked to foreign actors attempting to deepen political divisions at a moment of crisis during presidential elections. What began as confusion evolved into something more insidious — a coordinated assault on public trust when it was most vulnerable.

This new landscape requires rethinking resilience beyond physical infrastructure. Following Maui's 2023 wildfires, for example, Chinese disinformation campaigns promoted conspiracy theories about secret U.S. "weather weapons" while stoking misplaced fears FEMA would seize Hawaiian land. These narratives resonated with historical anxieties, undermining federal response efforts. Similarly, communities experiencing extreme weather for the first time — such as hurricanes in southern Appalachia — are especially susceptible to misinformation.

This challenge demands multi-layered responses. FEMA has tried to adapt by creating "rumor control" resources to directly address falsehoods in real-time. During Helene, the Biden White House created dedicated fact-checking accounts on social platforms while hosting regular public briefings alongside FEMA leadership. While necessary, they are insufficient — the product of a reactive stance rather than a preventative one.

The critical question facing communities and their elected officials is how to build resilience against both physical disasters and the disinformation flowing in their wake. Effective strategies will require collaboration between community leaders, emergency managers, and social media platforms, to name just a few. They must not only address the technical components of misinformation but also the underlying erosion in social cohesion that make them vulnerable in the first place, including political polarization, economic insecurity, and failing trust in institutions.

As climate-driven disasters become more frequent and more severe, the information environment surrounding them will determine whether communities come together or fracture in moments of crisis. This dual flood — of water and lies — demands a new integrated approach to resilience.

At SXSW, a bold experiment combined public storytelling with mayoral strategy, turning imagined disasters into real-world solutions. This is how Threatcasting became a tool for futureproofing governance.

SXSW X USCM

What happens when imaginative storytelling meets practical policymaking?

At SXSW in Austin, Texas, a unique experiment unfolded that did just that—bridging speculative foresight with actionable strategy. In a two-day adaptation of the Threatcasting methodology, members of the public first imagined the lives of fictional characters caught in cascading crises—floods, cyberattacks, deepfakes, and infrastructure collapse. Through prompts and collaborative storytelling, participants grounded complex systemic risks in deeply personal experiences. These narratives became launchpads for civic insight, surfacing fresh ideas about vulnerability, trust, and the fragile lines between order and chaos.

On Day 2, a room full of mid-sized city mayors attending the US Conference of Mayors (USCM) took those very scenarios and reverse engineered solutions. Working backward from the fictional futures, they identified policy gaps, infrastructure risks, and communication failures—and then charted clear milestones to mitigate them. This case study demonstrates how a narrative-first, community-engaged approach to foresight can directly inform municipal governance. When collective imagination is paired with strategic backcasting, it doesn't just predict the future—it equips leaders to shape it.

> “IF IT FLOODS ONLINE, IT FLOODS OFFLINE.”

A Case Story in Adapting the Threatcasting Methodology

FUTUREPROOFING GOVERNANCE:
Integrating Public Foresight with Policy

by Cyndi Coon

Threatcasting is a structured approach to exploring potential futures, identifying emerging threats, and developing strategies to disrupt, mitigate, and recover from them. For this event, we adapted the multi-step methodology into a two-part framework that connected broad public engagement with targeted policy development. By splitting the process across two days—first with SXSW 2025 attendees building personas and prototypes of catastrophic events in mid-sized cities—followed by mid-sized city mayors at the US Conference of Mayors using backcasting to design actionable solutions, we created a seamless transition from speculative foresight to pragmatic policy intervention.

Day 1: Public Threatcasting at SXSW

The first session at SXSW leveraged the diverse perspectives and imagination of the public to generate compelling future crises. Participants engaged, on small teams of three or four, in an interactive Threatcasting exercise where they built personas, which are fictional individuals living in mid-sized American cities who were experiencing extreme events such as cyberattacks, environmental disasters, or misinformation-driven social instability. Using a structured randomization process, each team rolled dice to determine three key factors: a disaster scenario, a location, and a multiplier (an element that amplifies the crisis).

(cont'd on next page)

From there, the small teams constructed detailed narratives around their personas, exploring how these individuals would navigate the cascading effects of the crisis. This exercise centers on the human dimension of future threats, grounding systemic risks in personal experiences.

The teams then moved into a **prototyping** phase, where they visually represented key moments of the crisis using paper and worksheets. These artifacts captured insights into behavioral responses, misinformation vulnerabilities, and systemic weaknesses within disaster response frameworks. The process of public participation in Threatcasting catalyzed broader civic discourse, helping to surface new perspectives on urban resilience challenges.

Day 2: Backcasting with USCM

The following day, we shifted the methodology from foresight to **backcasting**, using the SXSW-generated crisis scenarios as a foundation for policy development. Unlike the first session, which focused on speculative narrative-building, the mayors workshop was structured around reverse engineering solutions—working backward from the crisis moment to identify preemptive measures, policy interventions, and infrastructure improvements.

Each small group was assigned a printed SXSW scenario and asked to dissect its underlying vulnerabilities. They systematically explored:

- What current weaknesses allowed this crisis to unfold? (e.g., outdated infrastructure, lack of public trust, digital illiteracy, and gaps in emergency response coordination.
- What interventions could reduce these vulnerabilities? (e.g., early warning systems, public education campaigns, policy shifts, investment in cyber resilience)
- What milestones would ensure sustained preparedness over time? (short-term, medium-term, and long-term)

By using the public-generated threats as policy springboards, city officials were able to connect abstract future risks to concrete, immediate actions. This session also facilitated peer-to-peer knowledge exchange as mayors discussed shared challenges and best practices for building civic resilience.

The dual-session structure of this Threatcasting adaptation successfully bridged public foresight with governmental action, demonstrating **the power of collective intelligence in resilience planning.** The process highlighted how public engagement enhances institutional foresight. The SXSW session uncovered grassroots concerns and nuanced perspectives that often remain absent from policy discussions, enriching the understanding of emerging threats.

Narrative-based models aid in planning and are valuable tools for decision-making. By grounding threats in personal stories, policymakers were better able to empathize with community vulnerabilities and design more effective interventions. This approach transforms abstract risks into tangible experiences, making it easier to craft policies that address real-world consequences.

Backcasting provided a strategic roadmap for preemptive action. Rather than waiting for crises to unfold, city leaders can use the Threatcasting methodology to implement safeguards before threats materialize. This proactive stance ensures that communities are not just reacting to dangers but are actively mitigating risks before they escalate.

Collaboration between diverse stakeholders proved essential for strengthening resilience. By aligning public input with municipal strategy, this Threatcasting adaptation fostered a framework that encourages ongoing cooperation between communities and decision-makers. The integration of multiple perspectives and expertise created a more robust foundation for long-term security and adaptability.

This adaptation of the Threatcasting methodology demonstrated a novel approach to future-proofing cities against emergent threats through rapid prototyping. By integrating speculative storytelling and rapid prototyping with structured policy planning, we transformed foresight into a tool for real-world governance. This model can be replicated across other urban resilience initiatives, ensuring that anticipatory thinking does not remain an academic exercise but becomes a functional component of strategic municipal planning. The fusion of public creativity and governmental pragmatism in this adaptation serves as a blueprint for proactive crisis preparedness and civic innovation.

CIVIC I/O
Input Local Output Global
@usmayors
THIS INCLUDES YOUR INFORMATION BROADCAST
:(:(

The subsequent pages contain fictitious scenarios. Any resemblance to real people or real events is completely coincidental.

Though many scenarios came out of the SXSW prototyping, we have selected three representative examples and included the backcasting portion from the mayors, further analyzed and extrapolated for purposes of this report.

We further selected Scenario 3 to supply additional outputs to help visualize the contextual detail.

After the scenarios, we have included Safety Cards, yet another output, to serve as high-level "in case of emergency" guides. We welcome feedback on these various outputs, which can be submitted via the contact form on threatcasting.ai.

SCENARIO #1

DISASTER: FLOOD, RANSOMWARE

TITLE: A PERFECT STORM

LOCATION: REGIONAL AIRPORT

Official communications disrupted by cyber attack. Compromised IT systems preventing access to relief information. Conspiracy theories spreading among isolated airport personnel. Misinterpretation of incoming support as hostile action. Steven Lisbon is in the midst of a multi-dimensional storm in rural Missouri. How does he respond?

SXSW SCENARIO

In rural Missouri, 43-year-old **Steven Lisbon**, a local systems administrator, finds himself at the epicenter of a cascading crisis. As torrential flooding isolates his tight-knit agricultural community, the regional airport—crucial for supply delivery and emergency evacuations—is overwhelmed. Simultaneously, a phishing-based ransomware attack, triggered by a targeted conspiracy-laden message, disables vital communications infrastructure.

With power out and digital systems compromised, the airport becomes a chaotic shelter where misinformation spreads rapidly by word of mouth. Steven, grappling with his own guilt and confusion, inadvertently amplifies disinformation, deepening the community's distrust in government and scientific institutions.

THREATS

This scenario highlights how environmental disasters, cyber vulnerabilities, and social fracture points can intersect, compounding the impact of each threat and straining fragile rural systems already stretched thin.

Critical communications failure: The ransomware attack disables airport and regional IT systems, severing coordination with emergency services, aid providers, and transportation hubs.

Supply chain disruption: Flooded roads and compromised airport logistics delay or prevent the delivery of essential supplies like food, water, fuel, and medicine.

Misinformation cascade: With no access to official updates, locals turn to speculation and hearsay—accelerating the spread of conspiracy theories and deepening mistrust in government and media.

Erosion of public trust: A targeted cyberattack exploits existing distrust in science and government, creating fertile ground for foreign or domestic threat actors to manipulate public sentiment.

Internal social division: As misinformation spreads, community members begin to blame each other or outside groups, risking civil unrest, vigilante actions, or breakdowns in cooperation.

Economic paralysis: Local agriculture and manufacturing grind to a halt due to flooded infrastructure and IT disruption, jeopardizing jobs and long-term recovery.

Increased vulnerability to future attacks: The community becomes a soft target for follow-on cyber operations, disinformation campaigns, or financial exploitation due to weakened infrastructure and morale.

When a flood and cyberattack strike simultaneously, a rural airport becomes ground zero for chaos, misinformation, and cascading system failures—exposing the fragility of trust and infrastructure in overlooked communities.

MAYORS' BACKCAST

Prioritize situational assessment: Immediately assess the scope of damage, identify how many people are impacted, determine medical needs, and evaluate infrastructure vulnerabilities.

Leverage on-site expertise: Identify and mobilize any passengers or personnel with relevant skills—such as engineers, water specialists, or medical professionals—to assist with the crisis response.

Activate and adapt the airport's crisis management plan: Utilize existing emergency communication protocols, especially when digital communications are down. Implement person-to-person communication chains to prevent misinformation and ensure calm.

Combat misinformation with consistent updates: Regularly scheduled information briefings help stabilize the situation and build trust among stranded passengers and staff.

Address cybersecurity vulnerabilities: Acknowledge that the IT system was compromised due to a phishing attack and stress the need for stronger cyber hygiene training—emphasizing the basic rule: don't click the link.

Enhance staff preparedness: Introduce mandatory training for emergency readiness, including maintaining personal "go bags" with essential supplies for all airport personnel.

Implement policy upgrades for digital infrastructure: Review/strengthen cybersecurity policies and redundant communication systems to better withstand future disruptions.

Rebuild with resilience in mind: Consider long-term infrastructure improvements, such as elevating key facilities above flood-prone areas to minimize future risks and ensure passenger safety, even if operations are temporarily halted.

In the face of cascading failures—from cyberattacks to flooding—mayors emphasized the need for human-centered crisis planning, resilient infrastructure, and proactive training to **turn chaos into coordination.**

SCENARIO #2

DISASTER: FLOOD, INFRASTRUCTURE

TITLE: A FLOOD OF MISINFORMATION

LOCATION: MID-SIZED CITY

Heavy rainfall causes extensive flooding in a tech-centric metropolitan area, culminating in a catastrophic dam failure with mass casualties. While the city is submerged in floodwaters, An influencer's race for relevance becomes a catalyst for chaos when a viral deepfake she posts spreads faster than official updates—turning misinformation into a compounding disaster.

SXSW SCENARIO

In a sprawling and fast-growing city of over 3 million people, 29-year-old Cameryn, a popular influencer with strong brand partnerships and a loyal online following, finds herself trapped in her home as catastrophic flooding overtakes the area.

With roadways submerged, the power grid offline, and emergency services overwhelmed, Cameryn turns to her phone for updates, relying on a steady stream of TikTok, Substack posts, and niche media channels. Desperate to stay relevant—and keep her followers engaged—she quickly shares a video, which she doesn't realize is a deep fake, purporting to show government negligence in managing the dam that failed.

The post goes viral, fueling public panic and conspiracy theories, and further undermining trust in traditional news and local authorities. In her race for clicks and credibility, Cameryn inadvertently becomes a super-spreader of misinformation, triggering real-world consequences in a city already drowning in chaos.

THREATS

This scenario explores how digital influence, platform incentives, and fractured trust in institutions can turn one person's panic post into a catalyst for citywide unrest during a disaster.

Misinformation Amplification: Influencers with wide reach can unknowingly spread false or misleading content (e.g., deepfakes) that gets algorithmically boosted, accelerating panic and confusion in already vulnerable populations.

Loss of Institutional Credibility: Viral narratives that contradict official messaging further erode public trust in government, emergency services, and legacy news outlets—weakening their ability to respond effectively in real time.

Public Panic and Civil Unrest: Rapid dissemination of unverified claims (e.g., accusations of government negligence or conspiracy) can lead to protests, looting, or even violence.

Delayed Emergency Response: Emergency comms may be ignored or questioned if overshadowed by trending misinformation, complicating evacuation efforts, resource distribution, and safety coordination.

Influencer Liability and Legal Risk: Individuals like Cameryn may face backlash, legal challenges, or reputational damage for unintentionally causing harm—raising questions about the responsibility of digital creators during crises.

Exploitation by Malicious Actors: A chaos environment can be exploited by state or non-state actors to inject disinformation, deepen polarization, or manipulate public sentiment for geopolitical or financial gain.

Digital Platform Failures: Social media companies may be unwilling to flag or contain fast-spreading deepfakes for political, legal, or other reasons.

When floods hit a major city, an influencer's deepfake-fueled post goes viral—turning confusion into crisis and proving that misinformation can spread faster than water.

MAYORS' BACKCAST

Prioritize credible crisis communication: Deploy trusted first responders and emergency personnel as the face of public messaging to establish authority and combat misinformation early.

Rapidly counter false narratives: Identify misinformation circulating online—such as the influencer's deepfake video—and issue timely, fact-based corrections across multiple platforms.

Engage with influencers directly: Re-establish contact with the influencer who spread the misinformation, and work collaboratively to redirect their platform toward disseminating accurate, official updates.

Activate multi-channel messaging systems: Use local media, emergency alert systems (e.g. Amber Alerts), and social media platforms in tandem to ensure wide and redundant distribution of verified information.

Strengthen EOC communication protocols: Ensure Emergency Operations Centers have integrated communication plans that include protocols for identifying and responding to social media misinformation during disasters.

Invest in community trust before the crisis: Build long-term relationships between public officials and the community, so official messages are more likely to be believed in high-stress scenarios.

Coordinate with news agencies: Work proactively with local and regional media partners to reinforce consistent messaging and amplify corrections to viral falsehoods.

Explore legislative and sustainability solutions: In the long term, consider infrastructure and policy changes—such as flood mitigation strategies and regulations for digital platforms—to prevent both physical and informational disasters from recurring.

Recognizing the scenario's eerie realism, mayors emphasized the need for trusted messengers, rapid corrections, and re-engaging influencers to turn misinformation into an opportunity for truth.

SCENARIO #3

DISASTER: RANSOMWARE ATTACK

TITLE: RANSOM WAVE: FLOOD OF LIES

LOCATION: UNIVERSITY TOWN

As digital systems fail and misinformation spreads, a university president in a small Washington state college town faces rising student unrest and institutional paralysis in a campus overtaken by confusion and fear.

SXSW SCENARIO

In a small eastern Washington college town, Susan Lawson, the 43-year-old president of the local university, finds herself at the center of a spiraling crisis. A coordinated ransomware attack cripples the town's emergency response systems—including 911 dispatch—while deepfake videos begin circulating online, falsely showing a catastrophic breach of the nearby hydroelectric dam and widespread flooding of surrounding agricultural areas.

With institutional communication channels down and public panic surging, Susan watches as protests erupt on campus and students attempt to evacuate. She can't verify what's true, and neither can anyone else. The videos spread rapidly through student networks, exploiting the generational divide and longstanding tensions between the town's permanent residents and its transient student population. The chaos is further compounded by the revelation that the ransomware attack originated locally, a desperate act by community members resentful of their economic dependence on the university and fearful of its possible decline.

Trapped between misinformation, infrastructure failure, and civil unrest, Susan is forced to navigate a collapsing information ecosystem with her institution—and her reputation—on the line.

THREATS

This scenario probes the vulnerabilities of trusted institutions when digitally-enabled misinformation, social tensions, and economic precarity converge under the pressure of a manufactured disaster.

Emergency response system paralysis: The ransomware attack disables critical infrastructure like 911 and public alert systems, leaving the community without trusted channels during an unfolding crisis.

Campus unrest and panic evacuations: Students—unable to distinguish real from fake—begin evacuating or protesting, placing additional strain on limited city resources.

Breakdown of trusted information flow: With government communication systems offline, even institutional leaders like Susan are left in the dark, relying on unverified sources.

Exploitation of social fracture lines: The attack capitalizes on pre-existing tension between students and permanent residents, turning economic dependence and cultural frustration into digital rebellion.

Institutional credibility under siege: As the crisis unfolds, the university president's inability to respond effectively threatens both her personal reputation and the institution's authority.

Locally motivated cyber insurgency: Unlike foreign cyberattacks, this threat emerges from within the town itself—underscoring how economic decline and social discontent can radicalize local actors.

Failure of generational communication bridges: Students' reliance on social media and viral content collides with older institutions' dependence on traditional systems, delaying coordinated response.

When a ransomware attack and deepfake flood videos crash a college town's emergency systems, a university president must navigate digital chaos, economic resentment, and the collapse of institutional trust.

MAYORS' BACKCAST

Deliver clear, transparent communication: Prioritize authentic and verified messaging to counteract deepfakes and restore public trust during a digitally-driven crisis.

Partner with universities and community leaders: Collaborate with institutional voices—including elected officials, university leadership, and trusted social media influencers—to ensure cohesive and credible communication.

Secure critical infrastructure systems: Assess and fortify vulnerable digital systems one sector at a time, with an initial focus on hospitals and essential public services.

Deploy rapid-response messaging teams: React swiftly to false information by issuing corrections and real-time updates across both traditional and digital channels.

Address underlying town-grown tensions: Acknowledge the social and economic divisions between university populations and local communities that can fuel resentment and vulnerability to internal cyber threats.

Ensure equitable economic benefits: Develop strategies to make sure that surrounding communities share in the economic prosperity generated by the university, reducing feelings of exclusion and antagonism.

Investigate root causes of internal cyberthreats: Treat localized cyberattacks not only as technical issues but as social signals, prompting dialogue and trust-building between disconnected constituencies.

Strengthen cross-sector preparedness: Recognize universities as both potential targets and allies in cybersecurity efforts—incorporating academic expertise into citywide resilience planning.

Tailor response realism to local context: Acknowledge that different university settings carry different capabilities and risks; cybersecurity preparedness plans should reflect institutional strengths and limitations.

Mayors saw the scenario not as fiction but a warning—underscoring the need for transparent communication, digital resilience, and bridging divides between campus and community before distrust turns into disaster.

Radiating light and truth in service of our great community.

UNIVERSITY OF WASHINGTON AT EVANSVILLE
OFFICE OF THE PRESIDENT, SUSAN LAWSON, PHD
PRESIDENT@UNIWE.EDU | PHONE (555) 444-6660 | UNIWE.EDU

March 19, 2030

To the Students and Faculty of the University of Washington at Evansville,

As you know, yesterday we faced a confusing and troublesome attack that extends beyond our physical campus and university community. Please know that as I write this letter, my primary concern is that you all are safe and the events of yesterday have not adversely impacted the lives of UWE's community. This letter is the first of what I assume will be multiple communications to the UWE family. In subsequent letters, I will provide more detailed information as it becomes available.

Summary of events. At approximately 9:23am yesterday, a deepfake video was spread on multiple social media platforms. The video and accompanying text and headlines showed the North Fork dam had suffered a catastrophic collapse and the resulting floodwaters were threatening our UWE campus community. At the same time the video began to appear on personal devices, a ransomware attack of unknown origin disrupted many of the city of North Fork's municipal services. This included all emergency services and the city town hall and municipal leadership. The confusion and fear this disinformation created caused campus-wide disruptions of classes, unplanned evacuations, and led to the shutdown of all UWE functions and facilities. North Folk's limited transportation infrastructure was brought to a near standstill as vehicles and foot traffic flooded the surrounding streets.

What we know now. Because of the coordinated distribution of the deepfake video and ransomware attack, it was not until 5:45pm that I could personally confirm with the city authorities that there was never any damage to the North Fork dam and no flooding occurred. While it was unclear at the time, this false story was primarily distributed to personal electronic devices of the faculty and students of UWE – though some people not connected to the university but who reside adjacent to the campus also received the videos.

In the confusion that unreliable social media postings created, some residents believed the hoax was perpetrated by the UWE itself as an attack on the North Fork district. We believe the perpetrators intended to perpetuate disharmony between UWE and the North Fork community.

Next Steps. Beginning tomorrow, all academic classes will return to normal. All athletic and non-academic events and campus facilities will be open as normally scheduled. In a separate letter and on all campus online portals, contact information for counseling services, campus emergency services, and IT support for personal electronic devices will be made available. All services will be free of charge to current students and faculty. On Friday of this week, I will meet with municipal leaders to create a plan to uncover the root of this deepfake video. UWE will reach out to state and national resources to explore the likelihood of further digital attacks. We will partner with the community to leverage our exemplary academic resources to bolster citywide resilience. I will champion a working group of faculty and student volunteers to develop an improved emergency communications plan, campus evacuation plans, and any other improvements to the UWE community.

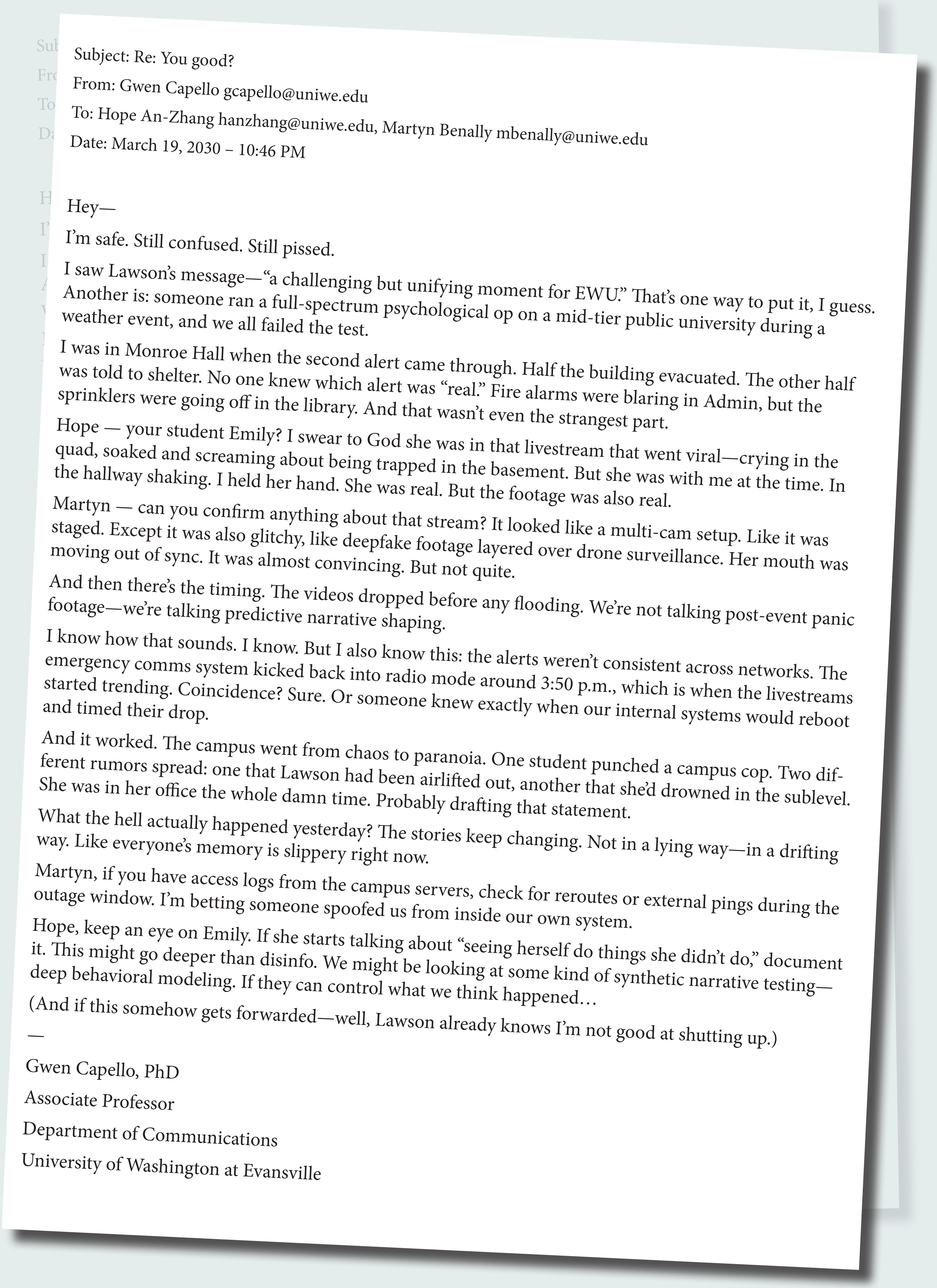
As soon as practical, I will meet with North Fork community leaders to create a long-term relationship with the following goals:

1. Improve university and community relationships.
2. Understand how UWE positively or negatively impacts North Fork's economy and municipal stability.
3. Explore ways that the UWE campus can be leveraged as an academic and research resource to the surrounding the North Fork community.

This is a challenging but unifying moment for UWE. As I mentioned at the beginning of this letter, I want to ensure the university community that I prioritize the safety of our student body and faculty. Within the next two weeks, I will provide updates to the above initiatives and communicate changes as they occur. All faculty and students are encouraged to be on the lookout for opportunities to participate in focus groups and committees as they are formed. Thank you for your patience and cooperation as we all work together to recover and secure the future of this great community.

Sincerely,

Susan Lawson
President, University of Washington at Evansville



Subject: Re: You good?
From: Gwen Capello gcapello@uniwe.edu
To: Hope An-Zhang hanzhang@uniwe.edu, Martyn Benally mbenally@uniwe.edu
Date: March 19, 2030 – 10:46 PM

Hey—

I'm safe. Still confused. Still pissed.

I saw Lawson's message—"a challenging but unifying moment for EWU." That's one way to put it, I guess. Another is: someone ran a full-spectrum psychological op on a mid-tier public university during a weather event, and we all failed the test.

I was in Monroe Hall when the second alert came through. Half the building evacuated. The other half was told to shelter. No one knew which alert was "real." Fire alarms were blaring in Admin, but the sprinklers were going off in the library. And that wasn't even the strangest part.

Hope — your student Emily? I swear to God she was in that livestream that went viral—crying in the quad, soaked and screaming about being trapped in the basement. But she was with me at the time. In the hallway shaking. I held her hand. She was real. But the footage was also real.

Martyn — can you confirm anything about that stream? It looked like a multi-cam setup. Like it was staged. Except it was also glitchy, like deepfake footage layered over drone surveillance. Her mouth was moving out of sync. It was almost convincing. But not quite.

And then there's the timing. The videos dropped before any flooding. We're not talking post-event panic footage—we're talking predictive narrative shaping.

I know how that sounds. I know. But I also know this: the alerts weren't consistent across networks. The emergency comms system kicked back into radio mode around 3:50 p.m., which is when the livestreams started trending. Coincidence? Sure. Or someone knew exactly when our internal systems would reboot and timed their drop.

And it worked. The campus went from chaos to paranoia. One student punched a campus cop. Two different rumors spread: one that Lawson had been airlifted out, another that she'd drowned in the sublevel. She was in her office the whole damn time. Probably drafting that statement.

What the hell actually happened yesterday? The stories keep changing. Not in a lying way—in a drifting way. Like everyone's memory is slippery right now.

Martyn, if you have access logs from the campus servers, check for reroutes or external pings during the outage window. I'm betting someone spoofed us from inside our own system.

Hope, keep an eye on Emily. If she starts talking about "seeing herself do things she didn't do," document it. This might go deeper than disinfo. We might be looking at some kind of synthetic narrative testing—deep behavioral modeling. If they can control what we think happened…

(And if this somehow gets forwarded—well, Lawson already knows I'm not good at shutting up.)

—

Gwen Capello, PhD
Associate Professor
Department of Communications
University of Washington at Evansville

OFFICE OF THE MAYOR

CITY OF EVANSVILLE, WASHINGTON

OFFICIAL STATEMENT (For Immediate Release)

March 19, 2030

RE: DEEPFAKE VIDEO OF DAM BREACH AND MUNICIPAL RANSOMWARE COORDINATED ATTACKS.

At approximately 9:23am on Monday, two simultaneous cyberattacks were leveraged against our community. The first was the distribution of a video that showed the North Fork Hydroelectric dam suffering a catastrophic breach and a flood that was presumably racing towards the University of Washington at Evansville district. The second attack was a ransomware attack on the city's municipal systems that effectively disrupted key emergency services and communications systems.

THE TRUTH: First and foremost, I want to assure all of our citizens that the condition of the hydroelectric dam was never in question and there was no flooding that impacted the farming community below the dam or the UWE campus and surrounding neighborhood.

In the hours that followed the cyberattack, many in our community inadvertently furthered fear and panic as the spread of the false narrative of the deepfake video only served to assist the yet-to-be identified perpetrators of the attack. The reaction of the community, powered by fears of their own safety, clogged our municipality's limited transportation hubs, congested streets where emergency vehicles were needed, and led to further falsehoods that the cyber-attack originated from the UWE community as an attack against the North Fork municipal district.

I personally met with the city's senior staff and the President of UWE, Susan Lawson, and we agree that the goal of the cyber-attack was to further strain the relationship between UWE and the district of North Fork. Experts from the Cybersecurity and Infrastructure Security Agency (CISA) are already working to investigate the source and methods behind the attacks. It is important for residents of North Fork to understand that while investigations into this attack are only in the beginning stages, we will work to build resilience against future attacks.

The full recovery from this event will take time and resources. It is my aim to make our community an innovator of resilience and a model for other communities. To accomplish this, initiatives will begin in the coming days and weeks. First, municipal leaders will create a regional communications plan that can immediately respond to disinformation designed to harm or cause fear in our community. This will include methods to quicky respond to disinformation attacks. UWE will be leveraged as resource for research and learning for our community. A review of the city's emergency response plans will create recommendations that build resilience in our transportation infrastructure that includes funding and resource proposals. Working with CISA, Evansville will develop defenses of our digital communications systems that will include protection from digital intrusion and disruption.

Lastly, I have assigned leaders in the North Fork community to collaborate with UWE leadership to build rapport and cohesion and address concerns about real and perceived inequalities between citizens and the UWE institution.

Sincerely,

G.H. Evergreen, Mayor of Evansville, Washington

From: Martyn Benally <mbenally@uniwe.edu>

To: President Susan Lawson, Mayor G.H. Evergreen, UWE Crisis Response Thread
CC: Director Janell Rowe (IT Security)
Date: March 19, 2030 - 8:19 AM
Subject: Conflicting Alert Origins & External Routing Incident

Summary of Findings Emergency Alert & Network Activity

Following yesterday's coordinated incident involving disinformation and ransomware activity, I conducted a preliminary log revi

1. Conflicting Alerts Dual Origin Triggers
- Two separate alert signals were registered by the EWU Emergency Alert System (EAS) at 9:21 AM and 9:23 AM.
- One originated from an expected administrative endpoint in Patterson Hall (authorized).
- The second appeared to route through the same server ID but was traced back to an unregistered external node masked behind a
- This second alert contained the phrase "FLOOD_WATCH MANDATORY EVAC" and reached 82% of student devices before su

2. Media File Propagation - "floodLive_cascade.avi"
- Prior to the alert, 17 devices across campus downloaded or cached a file titled floodLive_cascade.avi (hash signature: b0af83
- This file was hosted on a temporary CDN registered to a foreign domain no longer active as of 3:00 PM yesterday.
- Early frames of the video show high-resolution imagery of water breaching a concrete structure resembling the North Fork dam

3. Network Disruption Sync with Municipal Systems
- EWU's routing tables briefly redirected outgoing campus traffic through a mirror proxy that matched part of city's municipal
- Municipal and campus DNS logs both indicate queries to a now-deleted subdomain (n0fork-alert[.]net) between 9:059:32 AM.

Recommendations:
- Immediate engagement with federal forensic teams (CISA liaison has been briefed).
- Isolate and secure all devices showing early propagation of "floodLive" assets.
- Pause development of internal EAS update until full origin traceback can be confirmed.
- Strongly advise against public attribution of responsibility until spoofing vectors and routing paths are fully verified.

Let me know if you need this formatted for briefings.
-M.B.

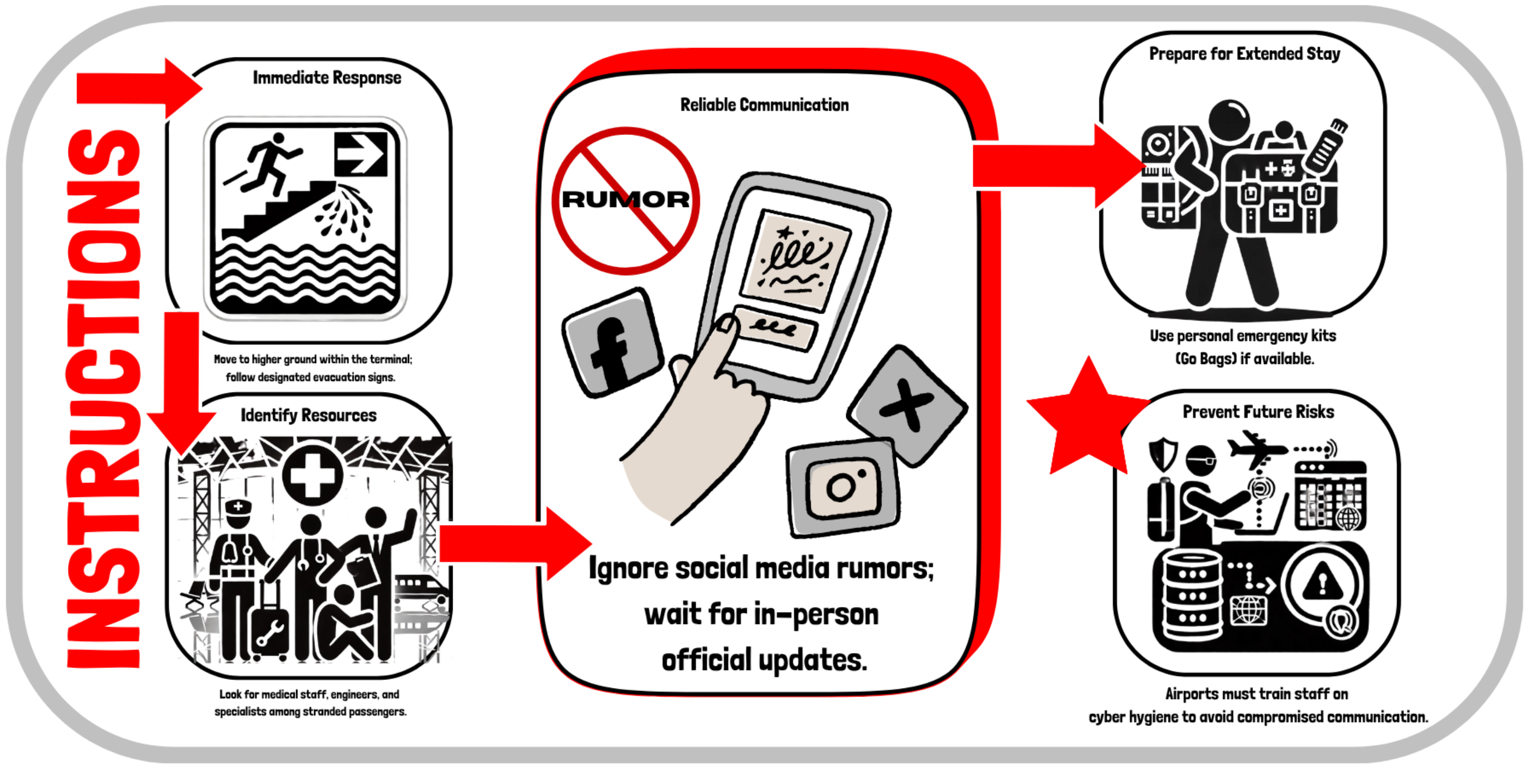
CRISIS COMMUNICATIONS

In times of crisis, it is impossible to quell the chaos and satisfy much less reassure everyone with a single well-worded statement, no matter how sincere or thorough. What could the University president have done differently or said differently to better ameliorate the situation? Was a traditional letter truly her best form of communication to convey to the student body that she valued their safety? Besides engaging CISA and releasing a press statement, what else could the mayor of Evansville have done to better connect with the public and rebuild trust such that more misinformation and disinformation would be less likely to take root?

Airport Flooding & Cyber Disruption

Stranded & Disconnected? What to Do When the Airport Goes Under

Threatcasting.ai



Immediate Response

Move to higher ground within the terminal; follow designated evacuation signs.

Identify Resources

Look for medical staff, engineers, and specialists among stranded passengers.

Reliable Communication

Ignore social media rumors; wait for in-person official updates.

Prepare for Extended Stay

Use personal emergency kits (Go Bags) if available.

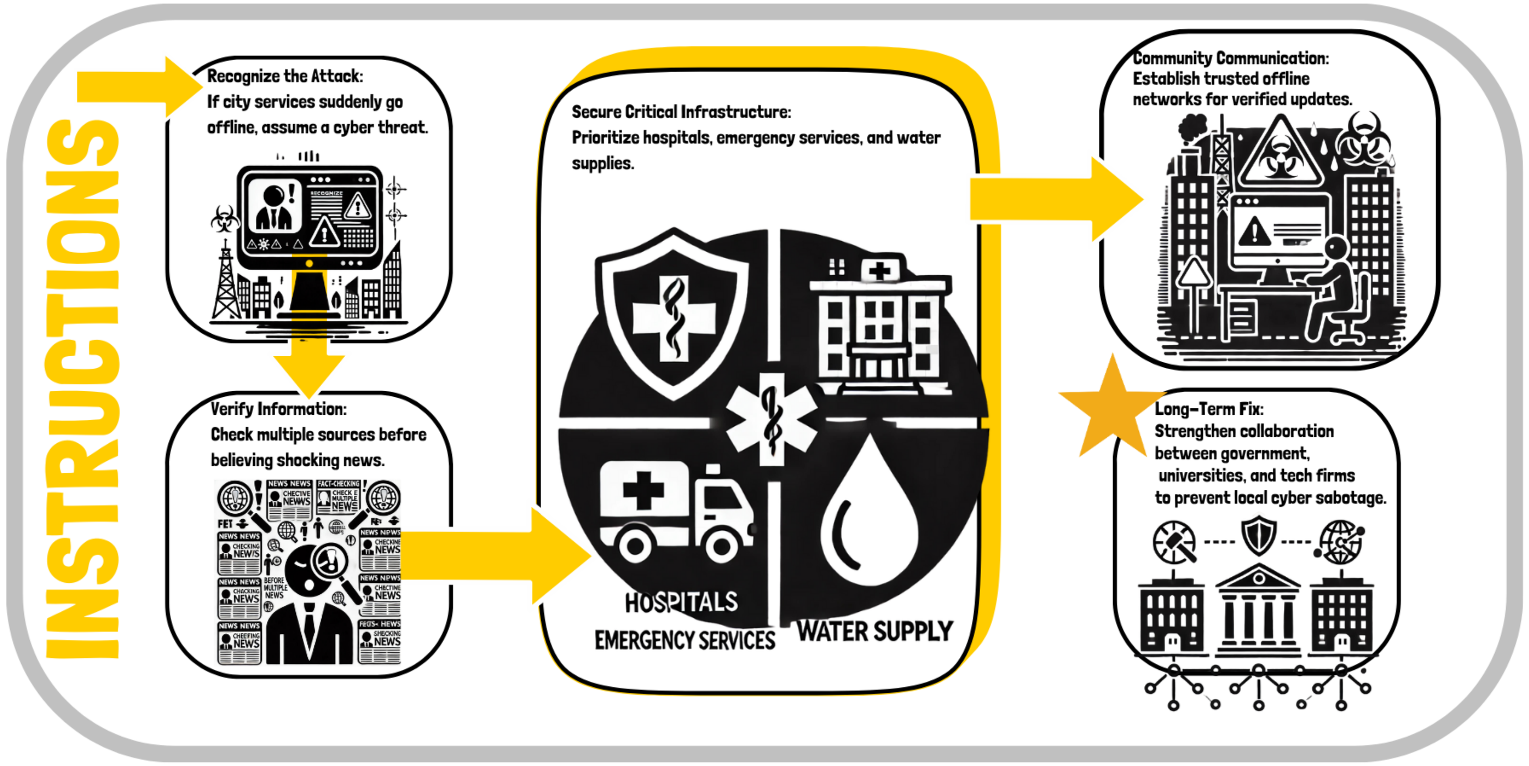
Prevent Future Risks

Airports must train staff on cyber hygiene to avoid compromised communication.

Ransomware Attack & Deepfake Crisis

Misinformation Lockdown: When the City Goes Offline

Threatcasting.ai



Recognize the Attack: If city services suddenly go offline, assume a cyber threat.

Verify Information: Check multiple sources before believing shocking news.

Secure Critical Infrastructure: Prioritize hospitals, emergency services, and water supplies.

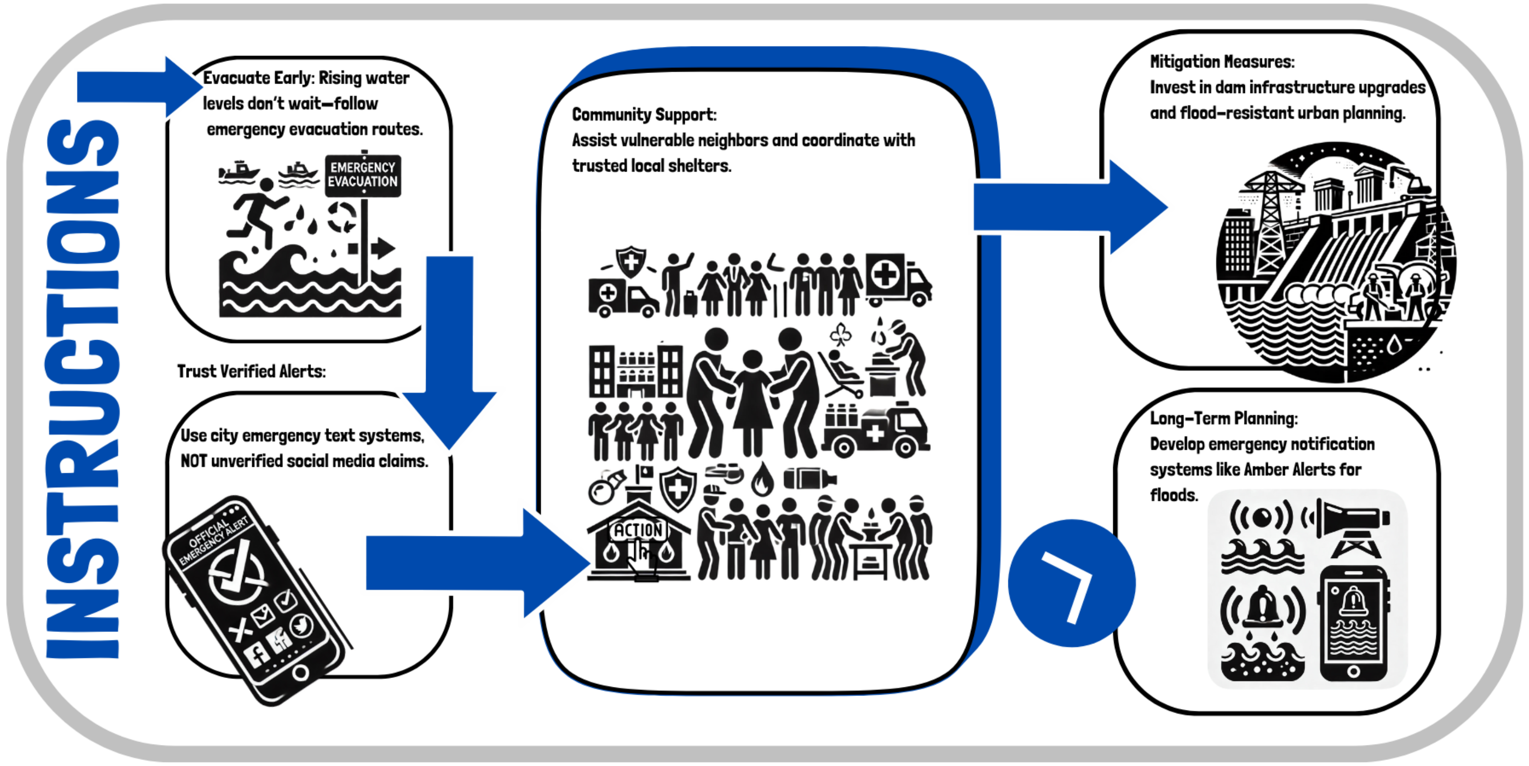
Community Communication: Establish trusted offline networks for verified updates.

Long-Term Fix: Strengthen collaboration between government, universities, and tech firms to prevent local cyber sabotage.

Dam Failure & Flooded Community

The Water is Rising: Navigating a Dam Collapse

Threatcasting.ai



Evacuate Early: Rising water levels don't wait—follow emergency evacuation routes.

Trust Verified Alerts:

Use city emergency text systems, NOT unverified social media claims.

Community Support: Assist vulnerable neighbors and coordinate with trusted local shelters.

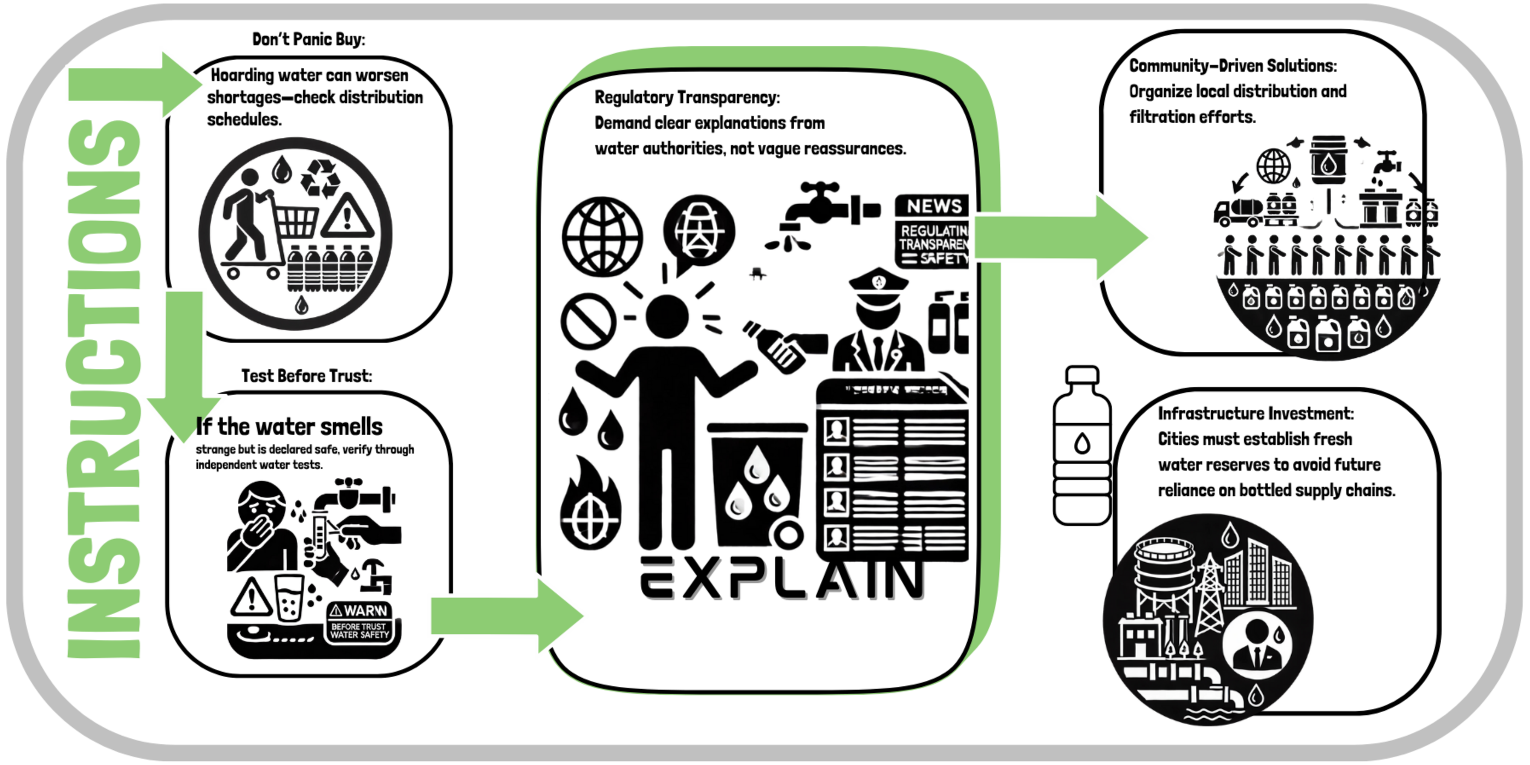
Mitigation Measures: Invest in dam infrastructure upgrades and flood-resistant urban planning.

Long-Term Planning: Develop emergency notification systems like Amber Alerts for floods.

Toxic Water Crisis & Public Distrust

When the Water Turns Sour: Who Do You Trust?

Threatcasting.ai



Don't Panic Buy:

Hoarding water can worsen shortages—check distribution schedules.

Test Before Trust:

If the water smells strange but is declared safe, verify through independent water tests.

Regulatory Transparency: Demand clear explanations from water authorities, not vague reassurances.

Community-Driven Solutions: Organize local distribution and filtration efforts.

Infrastructure Investment: Cities must establish fresh water reserves to reduce future reliance on bottled supply chains.

PROMPT LIST

Disasters: Natural and Manmade Scenarios

1. Major dam failure upstream leads to catastrophic flooding in low-lying neighborhoods.
2. Cyberattacks on city infrastructure disable power grids and emergency services during a heatwave.
3. A category five hurricane makes an unexpected inland turn, flooding the city beyond existing floodplain models.
4. An AI-generated deepfake of the mayor spreads during an evacuation, causing mass confusion.
5. The derailment of a freight train carrying hazardous materials leads to a citywide evacuation.
6. Extreme heatwave and rolling blackouts coincide with a senior care facility crisis.
7. Widespread food and water contamination following a significant flooding event.
8. Coordinated ransomware attack cripples emergency communication and dispatch systems.
9. Mass protests over climate migration policies turn into violent unrest, diverting emergency resources.
10. Surprise outbreak of a vector-borne disease spreads after increased mosquito populations due to shifting climate.
11. An unregulated AI misinformation campaign falsely declares the city unsafe, prompting a mass exodus.
12. Toxic algal bloom in the city's primary water source, forcing mass reliance on bottled water.

Locations: Geographic Focal Points

1. A city with large refugee or migrant populations, where misinformation targets vulnerable communities.
2. A rapidly growing ex-urban community struggling with outdated infrastructure.
3. A historic downtown district prone to flooding due to aging stormwater systems.
4. A college town where misinformation spreads rapidly among students and faculty.
5. A transportation hub city is dependent on a single highway or railway line.
6. A river-adjacent industrial zone is vulnerable to chemical spills and flooding.
7. Disaster response failures disrupt a tourist-driven economy reliant on seasonal revenue.
8. A military-adjacent city where base operations intersect with civilian life.
9. A post-industrial town still recovering from economic downturns is now facing climate migration.
10. A sprawling suburban region dealing with increased wildfire risks from unchecked development.
11. A tech-boom satellite city where rapid development has outpaced emergency planning.
12. A regional airport and logistics hub critical for disaster response is extremely vulnerable to cyber threats.

PROMPT LIST Continued

Multipliers: Factors That Influence or Amplify Threats

1. Deepfake videos and AI-generated crisis actors spreading false reports during an emergency.
2. Automation-driven job losses leave a city’s population economically vulnerable before a disaster even strikes.
3. Privatized disaster relief efforts create inequitable recovery between wealthier and poorer districts.
4. A generational divide in trust, where older residents rely on traditional media while younger populations turn to unverified online sources.
5. Social media-fueled misinformation causing panic and distrust in official emergency alerts.
6. A fragmented news ecosystem where competing narratives create confusion.
7. A newly implemented AI-based emergency system that malfunctions in a crisis.
8. A rapid influx of climate refugees is straining city resources.
9. Political polarization within city leadership, delaying coordinated disaster response.
10. Corporate control of local infrastructure, prioritizing profit over public safety.
11. Widespread distrust in scientific expertise, hindering effective disaster preparedness.
12. The rise of unregulated private security forces, stepping in where local law enforcement is overwhelmed.

Step 1: Roll the Dice.

Use the provided Prompt Sheet and dice to select one option from each category randomly:

- □ Disasters: Natural and manmade scenarios.
- □ Locations: Geographic focal points.
- □ Multipliers: Factors that influence or amplify threats (e.g., technology, societal shifts).

Once you have your 3 selections, list the numbers in the boxes above. Now, move on to step 2 to build your person.

Step 2: Who is Your Person?

In your small teams, start by reviewing the three prompts you rolled. These will shape the foundation of your character—the person who is directly affected by the disaster in the selected location and influenced by the chosen multiplier. Using these elements as a guide, work together to build out your person. Consider their background, daily life, and how they will need to navigate this unfolding crisis. Who are they, and what challenges do they face in this moment?

Name

Age

Occupation

What is your person's family & social network like?

How do they generally get their information?

What is your person's biggest fear right now?

Step 3: Where Is Your Person?

Now that you've defined who your person is, consider the environment they are navigating. Based on the location prompt you rolled, describe the setting in detail. What does this place look like? What key infrastructure—such as hospitals, schools, or transportation hubs—shapes daily life here? What are the community's strengths and vulnerabilities? How does your person typically move through this space, and how is that movement affected by the disaster? Use these details to ground your model in a realistic and tangible setting.

What is the size of the city and what is its Type (Growing, declining, industrial, suburban, etc.)

What Key Landmarks & Infrastructure does this city have (Hospitals, schools, transport hubs)

What are Community Strengths & Weaknesses (Trust in leadership, economic stability)

How Does Your Person Move Around? (Public transit, personal vehicle, walking)

Step 4: What Event Are They Facing?

With your person and location established, it's time to define the crisis they are experiencing. Look at the disaster and multiplier prompts you rolled—these elements shape the event unfolding. Now, describe what has just happened. How does this disaster disrupt daily life in their city? What immediate challenges does your person face? Consider how misinformation spreads in this scenario—what conflicting messages are they receiving, and how do they decide what to trust? Focus on how this crisis impacts not just infrastructure but emotions, behaviors, and decision-making in the moment.

What Just Happened? (Describe the disaster that hit their city.)

How Does It Impact Their Daily Life? (Work, home, community, safety.)

What Information Do They Receive? And from where? (Social media, news, government alerts.)

What IS Causing Them To Question? (Trust in leadership, rumors vs. facts.)

Step 5: Prototyping

Now, bring your models to life using the provided materials (markers, pens, paper). Your team will choose one of the following approaches to represent your person's experience in this crisis visually:

- □ **Draw a Snapshot:** Sketch a pivotal moment in your person's journey through the disaster.
- □ **Create a Flowchart:** Map out how misinformation spreads in their situation, showing key sources, interactions, and consequences.
- □ **Design an Infographic:** Depict their crisis response journey, highlighting challenges, decisions, and outcomes.
- □ **Draw a Timeline:** Show the sequence of events leading up to, during, and after the crisis, capturing key turning points and misinformation impacts.

Sketch here or on blank paper provided

Now that your sketch for your visual prototype is complete, write a brief description explaining what it represents and how it connects to your model.

Finally, assign your model an Experience Title:

MAYORS WORKSHOP

- Form Small Groups (3–4 mayors per group)
- Receive an assigned SXSW-generated model related to misinformation in disaster recovery
- Backcasting Exercise: Using guided steps, work backward from the future threat to identify vulnerabilities and interventions.
- Develop Milestones: Establish key steps to implement these interventions over time.
- Share & Discuss: Present findings to the larger group

Step 1: Understanding the Scenario

Review your assigned SXSW-generated model. Discuss as a group and take notes:

What disaster and misinformation challenges might this scenario present?

Who are the key stakeholders affected?

How does misinformation shape public response and trust?

Step 2: Identifying Current Vulnerabilities

Work backward from the crisis and identify:

What existing weaknesses in city infrastructure, policy, or communication might make this scenario possible?

What gaps in coordination, trust, or technology worsen the situation?

How might past events have contributed to these vulnerabilities?

Step 3: Pinpointing Key Interventions

Now, let’s shift toward solutions:

What policy changes could address these vulnerabilities?

How could education and public awareness reduce misinformation’s impact?

What technology could improve disaster communication and resilience?

What partnerships (public/private, community groups, media) would strengthen response efforts?

Step 4: Defining Milestones for Implementation

Break down the necessary steps over time:

What are some Immediate Actions (Next 6 months): Quick wins and rapid-response measures.

What are some Short-Term Actions (1–4 years): Building foundational policies & infrastructure.

What are some Long-Term Actions (5–10 years): Institutionalizing resilience and future-proofing.

CYNDI COON.

Director | Applied Futurist

Time traveler and rule-bender, and co-founder of the Threatcasting methodology.

WORKSHOP FACILITATORS & SPEAKERS

GREG LINDSAY.

Futurist | Urbanist

Generalist, urbanist, futurist, and speaker focused on the future of cities, climate, and AI.

DAISY THOMAS.

Researcher | Policy Expert

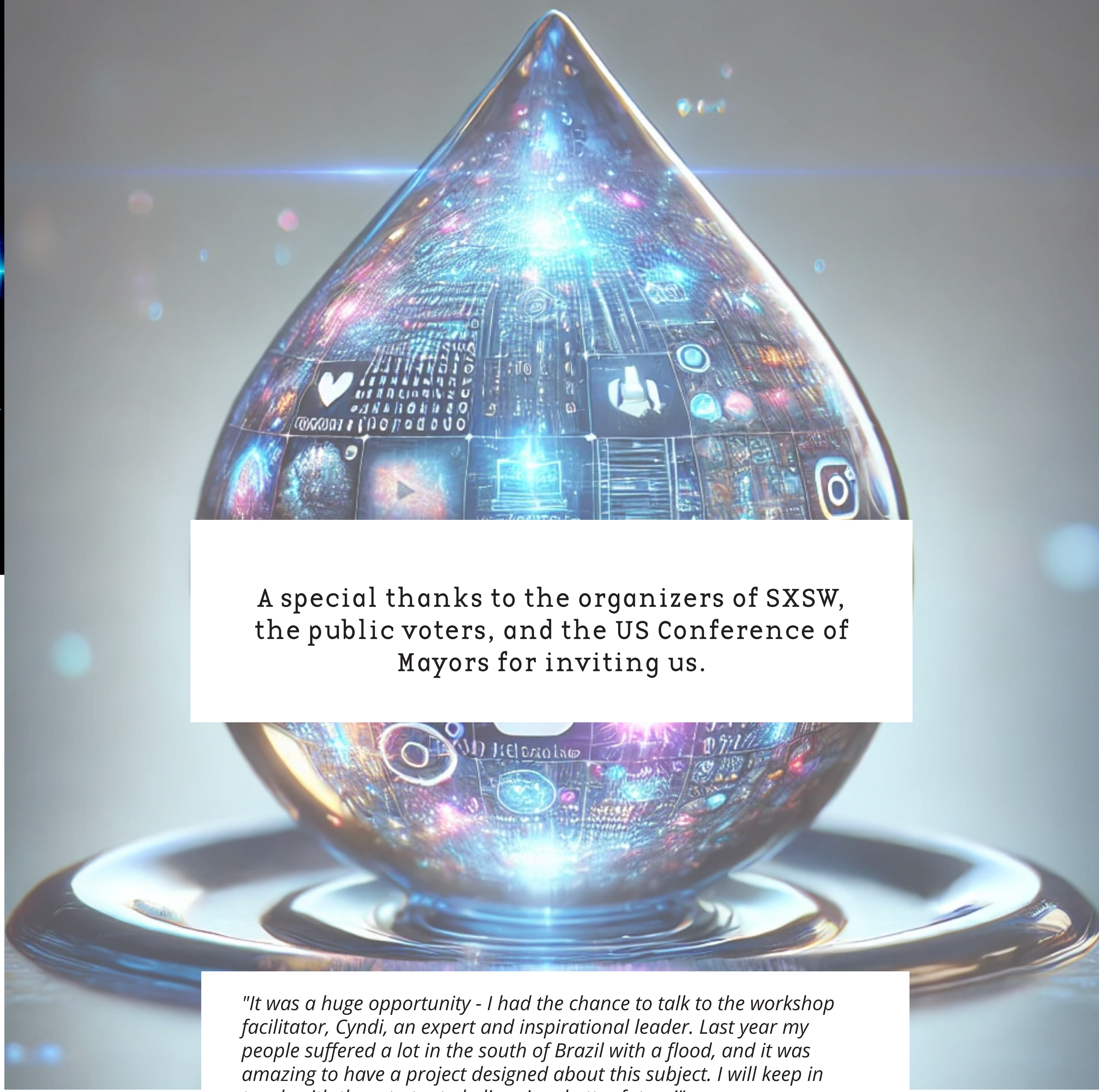
Conceptual architect & visionary specializing in pattern recognition across AI implementation, innovation, and systemic transformation

REPORT ANALYSTS

BUCK OWENS.

Writer | Analyst

Front End, JTA and Gap analysis expert building resilience, sustainability and foresight.



A special thanks to the organizers of SXSW, the public voters, and the US Conference of Mayors for inviting us.

"It was a huge opportunity - I had the chance to talk to the workshop facilitator, Cyndi, an expert and inspirational leader. Last year my people suffered a lot in the south of Brazil with a flood, and it was amazing to have a project designed about this subject. I will keep in touch with them to try to believe in a better future!"

- Bernardo Krebs
CEO e sócio na @ gama.mkt
Universidade do Vale do Rio dos Sinos
São Leopoldo, Rio Grande do Sul, Brazil

Report designed by
Michelle Daniel, Deputy Director
Threatcasting.ai

THREATCASTING.AI

THANK YOU TO ALL PARTICIPANTS.
CONNECT WITH US AT THREATCASTING.AI

MARCH 2025

We envision a world where foresight fuels action, where individuals and organizations anticipate and shape preferable futures, and where emerging threats are understood and mitigated before they become crises. Through the power of foresight and storytelling, we seek to drive transformative action to secure a better tomorrow for all.