Domestic Preparedness Journal

Nation-State Threats

Volume 20 Issue 2

EST 1998

Take Domestic Preparedness

On The Go

February 2024, Volume 20, Issue 2

Publisher
Michael Hull

Editor
Catherine L. Feinman

Cover Source: Muhammad Shoaib/Vecteezy.com

For more information about Domestic Preparedness, visit DomesticPreparedness.com

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

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.

Source: Unsplash/Clark Young

Nation-State Threats – Preparing at All Levels

By Catherine L. Feinman

In August 2023, Maui faced its deadliest wildfire in modern history – taking more than 100 lives and destroying thousands of homes and structures. That tragic event drew massive response efforts at the federal, state, and local levels. Two months later, FEMA Administrator Deanne Criswell spoke to the National Association of Emergency Managers in Memphis, Tennessee. She began by thanking all those who responded to Maui and acknowledging that responding to and recovering from natural hazards has become ingrained in the emergency management playbook.

What is not ingrained, though, is what Administrator Criswell said keeps her up at night, "the looming danger presented by nation-state threats to our homeland." She went on to describe what a nation-state attack could look like, why everyone should care, and how to balance natural and human-caused threats to ensure readiness. As first responders, emergency managers, health care workers, volunteers, military personnel, and many others respond to catastrophic events, oftentimes, so do foreign actors and others with nefarious intent. Misinformation that spread with the Maui wildfires in just one example.

Nation-state threats could include false information campaigns, cyberthreats, and physical threats, including chemical, biological, radiological, nuclear, and high-yield explosive weapons. The millions of cyber-intrusion threats the Port of Los Angeles combats each year demonstrate the importance of protecting critical infrastructure, which has become a desirable target. As emphasized by Criswell, all agencies and organizations should adopt a national security mindset, which begins with an awareness of the threats and capabilities of the nation's adversaries. Entities should then collaborate with defense and intelligence agencies, build external partnerships, and share information. Finally, individuals at all organizational and governmental levels should think creatively about how threats could manifest and ways to address them.

The authors in this February edition of the *Domestic Preparedness Journal* build awareness of some of the nation's threats and vulnerabilities. They also share protective measures and approaches for combating nation-state threats and strengthening homeland security and national resilience.

Source: Unsplash/Juliana Kozoski

Table of Contents

Editor's Note

Feature Articles

After the 1980s Cold War fears ended, attention shifted away from nation-state threats.

U.S. Military personnel move personnel and cargo to aid Hurricane Irma recovery relief (*Source:* Sgt. Juanita Philip/ Virgin Islands National Guard, September 9, 2017).

The [Evil] Empire Strikes Back: National Security Emergencies

By Robert J. (Bob) Roller

The recent increase in both global tensions and the frequency of natural disasters should spur discussion about the overlooked concept of *national security emergencies*. Revisiting this concept can help leaders more rapidly and effectively address modern threats.

Emergency managers in the United States are overstretched having to address increasingly frequent and more deadly disasters. This mission is complicated by increased tensions with nuclear-armed authoritarian dictatorships because many of the same resources are needed to address both natural hazards and warfighting. Unfortunately, U.S. policy solutions adopted since the end of the Cold War conceive a world where disasters are relatively small or regionally localized, with military support available to supplement civilian and private sector resources. This inaccurate model is even less accurate now. Instead, leaders should revisit the national security emergency concept and how to apply it to the problems of today and tomorrow.

Cold War Fears

Along with the hair bands, yuppies, Live Aid, and other cultural trends of the 1980s was the renewed threat of nuclear war with an increasingly belligerent Soviet Union. This danger was the focus among professionals across the U.S. and, in particular, by the Federal Emergency Management Agency (FEMA) established in 1979. Mostly forgotten now is that FEMA was born in large part from civil defense efforts during the Cold War. In fact, the Latin motto on the FEMA flag translates to "Service in Peace and War" because the threat of a catastrophic attack on the United States was its primary concern when the agency was founded.

National policy documents and other guidance promulgated during the 1980s tasked agencies to prepare for nuclear war, with natural disasters considered a secondary concern. President Ronald Reagan captured the culmination of this approach in Executive Order 12656: Assignment of Emergency Preparedness Responsibilities in 1988. The Executive Order (EO) makes clear in the preamble that:

> *The policy of the United States is to have sufficient capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency. A national security emergency is any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States.*

The sections that follow within EO 12656 include specific responsibilities for all levels of government, unique coordination responsibilities to address these threats, and the establishment of a permanent FEMA liaison to NATO Headquarters in Belgium. It is also clear that the EO addresses the perceived "Evil Empire" of the Soviet Union, given that the term "nuclear" appears 27 times in the 33-page document. However, the broad *national security emergency* definition allowed flexibility for problems like catastrophic earthquakes and pandemics, which might also cause severe consequences that endanger U.S. security.

Shifting Priorities

The nuclear threat posed by the Soviet Union receded with the fall of the Berlin Wall in 1989 and the almost simultaneous rise in deadly natural disasters in the U.S. These events forced FEMA and the federal government to serve as the "cavalry" that actively supports the natural hazards response as its primary mission. The shift away from nation-state threats as the central concern accelerated in the 1990s and early 2000s when the threat of international terrorism and the formation of the U.S. Department of Homeland Security (DHS) led to the most significant reorganization of the federal government since the end of World War II.

Among the many changes that followed was bringing a separate cabinet agency – FEMA – under the newly established DHS with a mission focused primarily on terrorism, borders and immigration, and cybersecurity. The formation of DHS also included new policy prescriptions to guide the national response to major incidents. However, with DHS's mixed record during Hurricane Katrina and the 2009 H1N1 pandemic, it was unclear whether these changes in organization and authority would lead to positive results. Excluding any mention of hostile nation-state threats in the 15 National Planning Scenarios developed during this period also highlights a lack of interest in this enduring problem from the past, in addition to those present during the early years of DHS.

Conflicting Guidance

Following Hurricane Katrina, Congress provided updated legal authorities in 2006 concerning national incident management. The National Preparedness System replaced the planning scenarios in 2011. Then, in 2016, the president issued further incident management guidance that set an expectation for federal agencies with the most applicable statutory authorities and relevant capabilities to take charge of a national incident response with support provided by FEMA. However, the implementation of this latter document was hindered by the fact it was not made public until 2022. In addition, it did not specifically cite the unique emergencies, where government "czars" develop short-term, high-visibility solutions with limited operational reach as its intent. This implementation created confusion when trying to decide which policy framework is best-suited to a particular incident.

Each attempt to provide appropriate incident management direction was intended to fix the challenges that were present at the specific moment each was published. Unfortunately, nearly all these additions occurred without rescinding or revising the older documents. The result was layers of confusing guidance for federal agencies attempting to address the current threat landscape and emerging incidents within it. These documents were also published before attention shifted back to the re-emergence of peer and near-peer international competition and the unique challenges this will place on military and civilian officials. These roles are responsible for supporting military operations, responding to attacks on the homeland caused by adversaries during a contested deployment of U.S. forces, and managing scarce resources needed to continue responding to natural disasters without having clear guidance explaining how to support these missions simultaneously. The result is a hodgepodge of guidance developed since the late 1980s to address threats of the past that will likely impede attempts to address threats of the present and future.

Way Forward

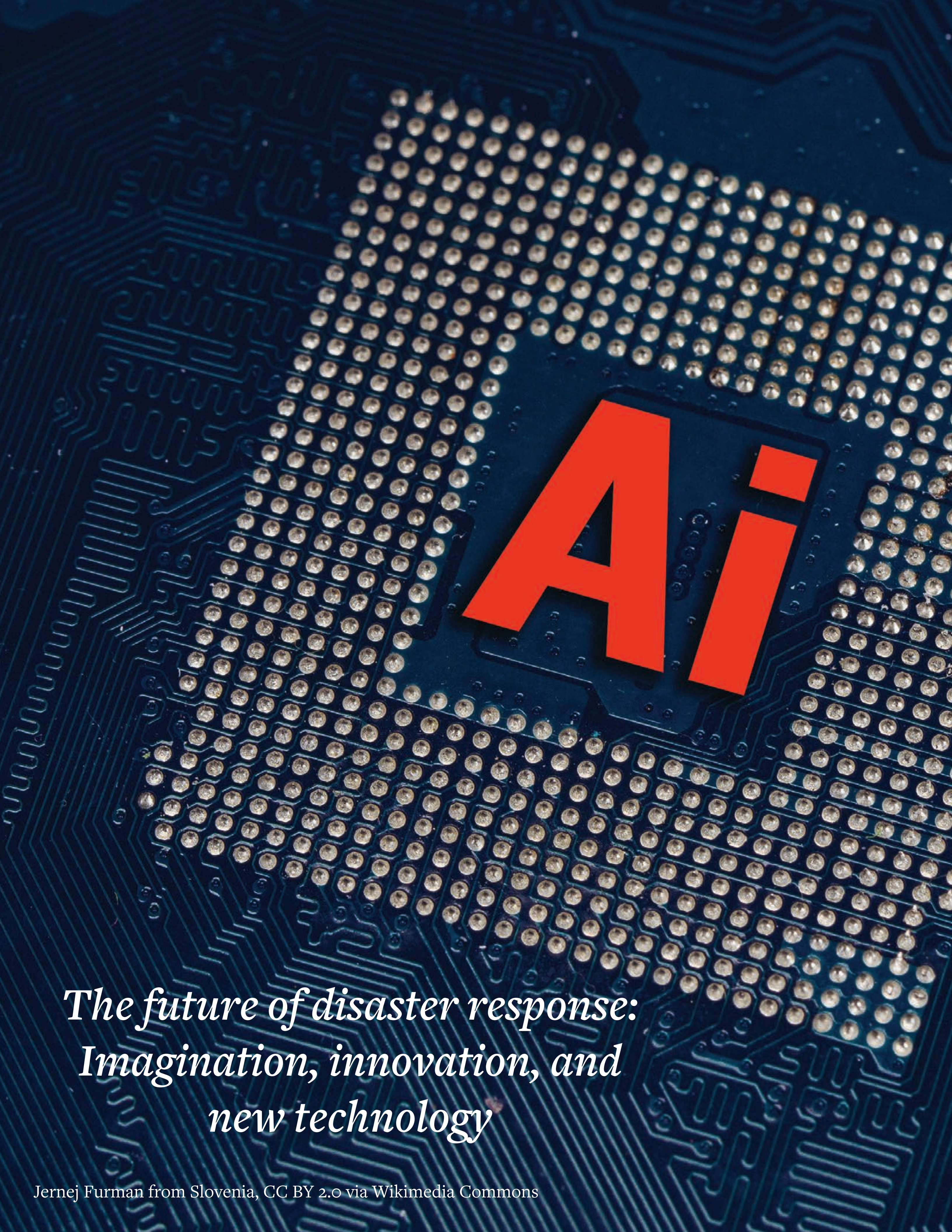
All is not lost. First, despite being overworked and under-resourced, the emergency management community is increasingly experienced and adept. The storms, fires, floods, pandemics, etc., have created a generation of well-trained emergency managers, though worn by these experiences. Second, the overlapping authorities and confusing policy guidance provide potential readymade solutions. However, they must be updated, deconflicted, and exercised before professionals employ them.

This alignment work should start at the top and work down. It is time to revisit EO 12656, including defining a national security emergency and the responsibilities assigned to each listed federal agency and their emergency coordinators. In addition, the revision should consider FEMA's role in supporting the overall preparedness and response to these incidents.

Next, more recent yet disconnected policy guidance developed since the establishment of DHS should be updated, including Homeland Security Presidential Memorandum 5, signed by President Bush in 2003. The document shares essential provisions, including what became the National Response Framework and National Incident Management System. However, incident management contradictions such as those that contributed to the poor response to Hurricane Katrina continue to distract DHS from core missions vital to national security and further complicate the response to large-scale incident management. The more recent Presidential Policy Directive 44 should also be implemented when complex incidents require additional coordination and proactive public messaging but not a massive mobilization of resources, such as COVID-19 or worse.

Finally, planning, training, and exercises should incorporate this organized and updated approach to address incidents up to and including national security emergencies. Should something catastrophic occur that threatens U.S. security, emergency managers would be ready to address this threat in parallel with the typical, yet growing, list of disasters and other emergencies.

Robert J. (Bob) Roller serves as the Federal Emergency Management Agency's (FEMA) National Planning Branch Chief and formerly served as the Planning Division Director within the DHS Office of Policy. He is a frequent contributor to Domestic Preparedness, and the views expressed here do not necessarily represent the views of FEMA or the United States government.



The future of disaster response: Imagination, innovation, and new technology

Jernej Furman from Slovenia, CC BY 2.0 via Wikimedia Commons

Needed: More Imagination for Countering Domestic Risks

By Jeanne Benincasa Thorpe

Two decades ago, the *9/11 Commission Report* stated that the most critical failure in preventing and preparing for the attacks was one of imagination. This practice seems to be a recurring theme in many major disasters up to the present day. Imagination is necessary for addressing challenges and incidents that threaten public safety. However, as *Lord of the Flies* author William Golding illustrates, people in crisis often lack imagination in considering potential threats, risks, and outcomes that they have not previously experienced.

Cultivating Imagination

Influential leaders should embrace a culture that values change, progress, and imagination. Homeland security and emergency management leaders who think bigger, broader, and bolder can develop new and unconventional strategies that address the vulnerabilities and threats of today and tomorrow. Public safety leaders who prioritize how they process and plan for all types of threats can fast-track their imaginative and creative planning and long-range vision for direct, indirect, and catastrophic threat scenarios. This step facilitates the mitigation of and response to disasters. Furthermore, industry leaders who become advocates can promote innovative strategies to address the new challenges and incidents – both natural and human-caused.

Communities across the United States are confronted with stronger and more destructive national disasters, escalating domestic and international conflicts, and complex cyberthreats. Senior leaders in the public and private sectors face a paradox that domestic preparedness expectations will continue to outpace investment. Therefore, it is important that leaders prioritize technological planning to integrate the most effective resources to combat these disasters. Furthermore, such prioritization helps leaders accelerate their interdisciplinary planning and long-term vision for catastrophic threat scenarios in imaginative and creative ways.

Finding Innovative Opportunities

On September 14, 2023, Secretary of Homeland Security Alejandro N. Mayorkas stated in a U.S. Department of Homeland Security press release, "Artificial intelligence is a powerful tool we must harness effectively and responsibly." He further remarked:

> *Our Department must continue to keep pace with this rapidly evolving technology, and do so in a way that is transparent and respectful of the privacy, civil rights, and civil liberties of everyone we serve.*

Artificial Intelligence (AI) has the ability to address the challenges of instantaneous sources of unvetted intelligence of the crisis and the streaming of endless data from sources that public safety and disaster management need to review, confirm, distribute, and act. This drain on time and resources can be significantly improved through the use of AI's capability of streamlining or scrubbing data and formulating effective responses based on the information processed.

Implementing AI and other innovative technologies that assess data quickly and accurately will improve response and mitigation tactics for any public safety agency. As with any revolutionary transformation, anticipated challenges can hinder the widespread adoption of public safety technology. Improper use poses additional risks. However, the benefits seem to outweigh the perceived drawbacks. The potential uses of AI for public safety technology solutions seems endless – from virtual and augmented reality for training simulations to drones with thermal imaging capabilities for fire response.

William Bratton, executive chairman of risk advisory at a global advisory firm, summarized his thoughts in a January 15, 2020, article in *American City and County*:

> *Technology is advancing so quickly that things we could only dream about a few years ago are a reality today, and with lives on the line, it is critical that public safety officials are equipped with the skills and the know-how to use them.*

Public safety has a foundation built on age-old traditions that can make them resistant to change or adopting new ideas. Leaders are responsible for instituting a culture that embraces change and sees the value in modernizing its processes to enhance public safety operations, create better outcomes, and make their communities safer places to live and work. However, leaders may resist trying new products and technologies for fear of low efficacy, reliability, and data security. In turn, this resistance can create a stagnant culture that dismisses new technology and cultivates comfort over creation.

Embracing New Ideas and New Technologies

Institutional resistance to new ideas can create a stale culture, preventing the opportunity to learn, evaluate, and test new technology like AI. Therefore, this may hinder public safety leaders, their resources, and their capabilities to respond to and mitigate disasters successfully and effectively. Adhering to tradition rather than striving for change is not a good reason to avoid technology. In today's rapidly evolving world, governments that adapt and embrace change can better serve their missions, protect citizens, and institute policies relevant to modern culture and solutions.

Agency leaders are crucial in instituting a culture that embraces change and values innovation and modernization. In such a culture, agencies can enhance public safety operations, create better outcomes, and make their communities safer places to live and work. Successful public safety agencies look toward the next potential natural disaster or public safety incident and consider the tools that could enhance their daily work. Even if existing equipment and devices have proven indispensable, technology continues to open new opportunities.

As the acceptance of AI rises worldwide, government bodies are learning how to capture its potential ethically and responsibly. AI is a powerful tool that can improve government processes and drive positive transformation. Careful consideration of critical factors such as security and privacy can ensure data access is limited to those possessing proper clearances and credentials. After addressing these concerns, public safety agencies can use AI and machine learning to analyze data, identify patterns, and predict future events. These actions could help them make better decisions and respond more effectively to emergencies.

From "Lord of the Flies" to the terrorist attacks of 9/11, significant consequences have been blamed on failures of imagination. Avoid repeating past mistakes and increasing risk through innovation, new technologies, and forward-thinking.

Looking Ahead

Technology is a part of daily life. It has transformed industries and redefined the world in ways that were unimaginable, even a few years ago. However, the failure of imagination is not new. It is part of the human condition. Many large-scale disasters, such as Pearl Harbor, 9/11, Hurricane Katrina, and the Maui wildfire, demonstrate a tendency to assign blame, miss some of the lessons learned, and fail to imagine that the disaster could happen again. There is a positive takeaway, though. By embracing AI and other new technologies, agencies and public officials could have abundant imagination and creativity at their disposal. These resources are ready to be tapped. The risk of not doing so could lead to a repeat of past mistakes and open the door to much more significant risks.

Jeanne Benincasa Thorpe is director of National Security and Resiliency for the law firm Nixon Peabody LLP. She works with the firm's attorneys to help clients anticipate potential challenges to ensure continuity in times of crisis.

Source: Tony Webster, CC BY-SA 4.0, via Wikimedia Commons.

Repeated Intelligence Failures – Not Connecting the Dots

By Robert Leverone and Darren Price

"The overriding conclusion was that the government's principal failure in 9/11 was a failure to 'connect the dots'." –Brookings Institute

Like 9/11, evidence suggests intelligence failures occurred during Pearl Harbor, the Boston Marathon Bombing, the bombing of the USS Cole, multiple active assailant attacks, and other incidents. These intelligence failures attain exponential levels of concern and consequence when they occur on a national level. Often associated with such events is the criticism that there was a "failure to connect the dots." Most recently, some have questioned if there was an intelligence failure (i.e., failure to connect the dots) before the October 7, 2023, Hamas attack in Israel. According to the National Counterterrorism Center, "HAMAS – the acronym for Harakat al-Muqawama al-Islamiya (Islamic Resistance Movement) – is the largest and most capable militant group in the Palestinian territories and one of the territories' two major political parties." The United States and several other countries have identified Hamas as a terrorist organization.

Erik Dahl, an assistant professor of National Security Affairs at the Naval Postgraduate School's Center for Homeland Defense and Security, posits in "Intelligence and Surprise: Failure and Success from Pearl Harbor to 9/11 and Beyond" that connecting the dots is understanding the importance of signals and warnings in the available information (i.e., intelligence) and parsing out that which is most relevant, connected, and able to be assimilated into a product for decision-makers willing to accede its content. Analyzing the enormous amount of data available often compounds this issue. Dahl cites Roberta Wohlsteter's book *Pearl Harbor*, which stated the ratio of noise to relevant signals made data analysis onerous before the attack on December 7, 1941.

In an October 30, 2023, edition of the podcast *Overheard*, entitled "Surprise Attack: Understanding the Challenges of Intelligence Analysis," Philip Wasielewski stated one commonality of surprise attacks has been preconceptions, which lead to ingrained biases. The idea that terrorists could fly hijacked airliners into the World Trade Center or that an irregular Hamas terrorist force could thwart the seemingly impregnable Israeli border defenses was inconceivable to many analysts and decision-makers. Wasielewski's guest, former Central Intelligence Agency (CIA) analyst Nate Dietrich, reinforced this viewpoint by stating that preconceptions and biases engender unalterable beliefs, which may lead to inaction.

Examples From the 9/11 and Hamas Attacks

Before the Palestinian-backed militant group Hamas attacked Israel on October 7, 2023, signs of an impending attack, including training with paragliders, military-style drills, and a professional-quality video of attacks on mock Israeli targets, were apparent. However, the "dots" were not collected and analyzed sufficiently to connect them.

According to a New York Post article, Hamas hid its preparations for the October 7 attack in the open. In that article, Michael Milshtein, a former Israeli Army intelligence officer, stated he was aware of Hamas' preparations but never conceived of their ability to coordinate such an ambitious, large-scale operation. Milshtein's observation appears to mirror that of the Israeli intelligence apparatus in that there was much thinking about what an adversary was, not what it could become. In addition, recent reports suggest that Israeli intelligence officials dismissed intelligence information, including a copy of the Hamas attack plan, obtained well in advance of the attack because the information was considered "aspirational."

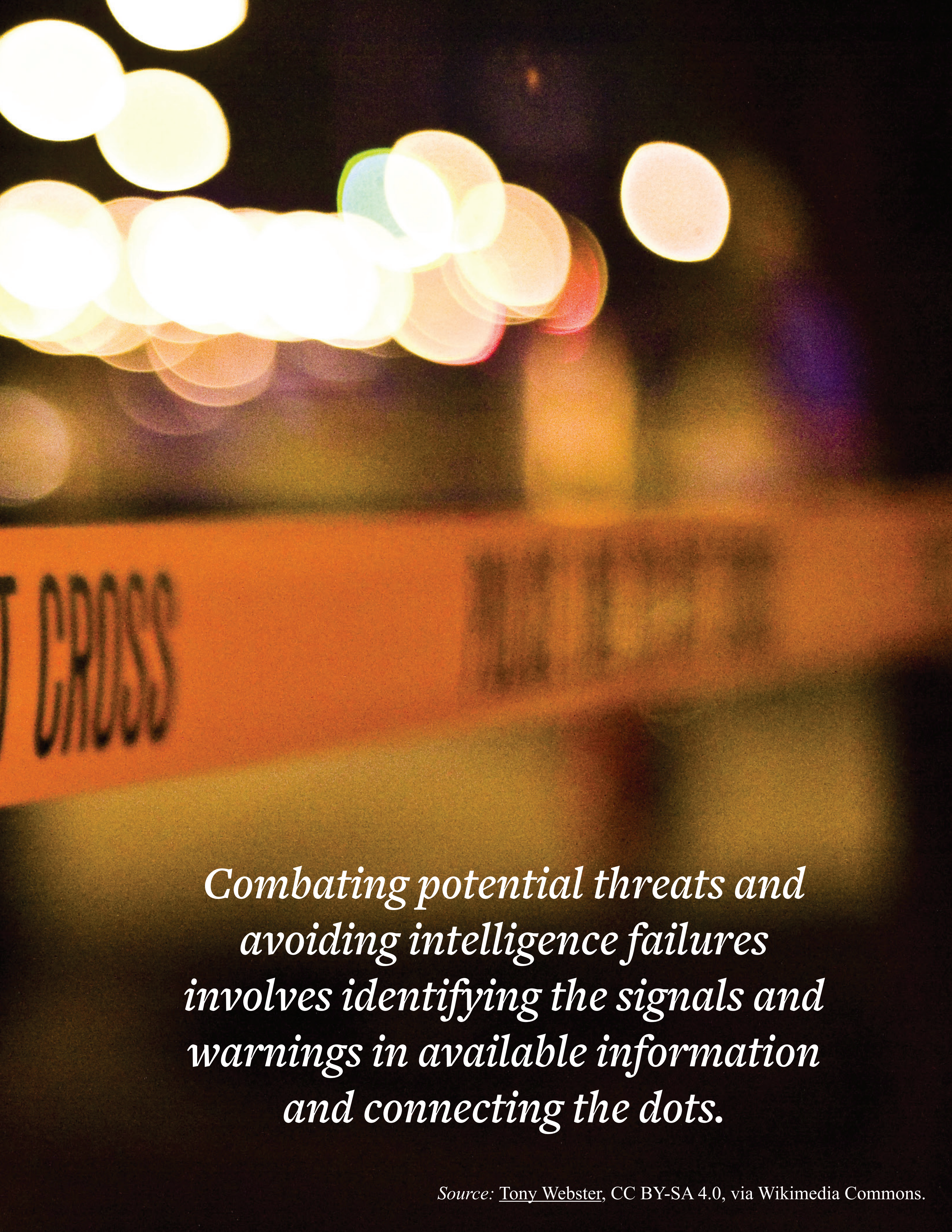
The 9/11 Commission Report similarly concluded after the 2001 terrorist attacks that the U.S. intelligence enterprise was still squarely on a Cold War footing against an adversary (i.e., the Soviet Union) that no longer existed. As a result, U.S. intelligence failed to give credence to the many data points indicating the emergence of a new threat (e.g., al-Qaeda). Siloed thinking and institutional (i.e., bureaucratic) policies that limit intelligence sharing are two impediments to preventing surprise attacks. Without information sharing across intelligence services, generating a compilation of data points to indicate a potential incident, especially a surprise attack, is challenging at best.

Conclusions from *The 9/11 Commission Report* led to the creation of the Office of the Director of National Intelligence to coordinate data collection and analysis among U.S. agencies. In *The Conversation*, Javed Ali of the Gerald R. Ford School of Public Policy postulates Israel's intelligence agencies – Shin Bet, Mossad, and its military intelligence agency – would benefit from a similar coordinating entity in their ongoing national defense. However, even if the abovementioned obstacles are overcome, some, including Dahl, suggest surprise attacks are inevitable.

The Challenge of Connecting the Dots

Failing to make the connections between intelligence gathered from various sources can have catastrophic impacts. While often asked, determining the root cause of why the dots were not connected is not a simple task, as there are ultimately many "whys" that contribute to how these catastrophic surprise attacks continue to happen despite the employment of robust intelligence and military systems. As such, post-incident reviews and analyses cannot cease when answering the first "why." For example:

- Military commanders in Pearl Harbor decided not to accept warnings of a pending attack because they had not completely deciphered the Japanese code;
- The CIA did not hand off information regarding the 9/11 hijackers to the Federal Bureau of Investigation for follow-up;



Combating potential threats and avoiding intelligence failures involves identifying the signals and warnings in available information and connecting the dots.

Source: Tony Webster, CC BY-SA 4.0, via Wikimedia Commons.

- The Israeli intelligence officials did not recognize the threat contained in pre-attack intelligence.

In addition, an Arab country, purportedly Egypt, reportedly warned Israel about Palestinian anger reaching a dangerous point before October 7. Yet, it appears Israel did not take significant action to address this warning. The public impression that Hamas was not willing to get into a large-scale confrontation with Israel may have played a role in the dots not being connected in advance of the October 7 attack. This perception extended beyond Israel as a national security advisor in the Biden Administration noted just days before the attack "that the Middle East was the calmest it had been in two decades." Some, such as retired Lieutenant General William G. "Jerry" Boykin, advance that internal issues within the Israeli Knesset not only created a strategic weakness their enemies could exploit but resulted in Israel missing opportunities to connect intelligence leads.

Reevaluating to Not Repeat the Cycle

Indefinitely maintaining a maximum readiness level in security and special operations is impractical from a financial or staffing perspective. As society moves farther away from a critical incident, it becomes even more challenging to maintain support for maximum readiness. That being said, when dealing with an adversary or adversaries possessing an avowed hatred that calls for eliminating people or nations, there is no room for complacency. As such, the "it won't happen here" mentality must change.

It is easy to analyze an incident afterward and point out what a given organization(s) failed to do to prevent a surprise attack. Rather than criticize or pass judgment after an incident, there must be a concerted effort to glean the root causes and consistencies across surprise attacks, whether local, regional, national, or international. It is short-sighted to reason that decision-makers failing to recognize the commonalities (i.e., pre-incident indicators), using siloed information sharing, not taking a threat seriously, or being complacent that it cannot happen here are the only contributing factors that need to be addressed to avoid a repeated cycle of surprise attacks.

Key Takeaways and Recommendations

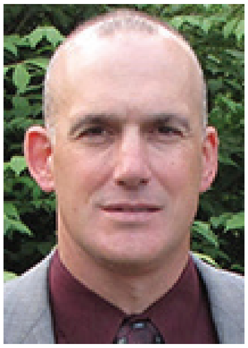
Following are some recommendations from the authors to avoid common themes evidenced in surprise attacks:

- Do not lose sight of the adversary's overall goals and intent. The original Hamas charter called for Israel's elimination. Although Hamas modified its charter in 2017, the intent has not changed, as evidenced by the October 7 attack on Israel.
- Create a culture of cooperation, not competition, among intelligence services. For nations like the United States and Israel that maintain robust intelligence operations across multiple agencies and organizations, competition and information silos can occur due to existing bureaucracies. Culture and laws can create bureaucracies that silo intelligence (e.g., the CIA is responsible for international intelligence operations, the FBI is the lead agency for domestic intelligence operations). Even with conscious efforts to share information, having multiple agencies with different intelligence responsibilities delays information- and intelligence-sharing processes.
- Expect the unexpected when it comes to asymmetrical warfare. Agencies should consider "red teaming" to

identify vulnerabilities in their defenses. With the approval of an organization's leadership, red teaming for a nation-state threat could involve a group (i.e., red team) pretending to be an opposing force to create a physical or cybersecurity intrusion. The red team then reports the vulnerabilities it identified back to the organization's leadership to address. However, costs and other concerns often limit or prevent using this tactic. Think tanks exist in topical areas, but the number of organizations engaging in red teaming for threats and vulnerabilities is assuredly low for many reasons (e.g., cost, perception, safety concerns). Yet, the factors limiting red-team use seem minor when a surprise attack occurs and lives are lost.

- Reduce or eliminate personal, institutional, and political biases in prioritizing security vulnerabilities. Unalterable beliefs engendered by biases regarding the capabilities of an adversary can skew effective measures at preventing an attack.
- Review the successful steps employed in previous interdictions to prevent future surprise attacks. This includes identifying what commonalities existed to provide sufficient credibility of the connected dots to equip decision-makers with a clear enough picture of the looming threat to initiate preventative measures.

Regardless of whether the actions outlined in this article for mitigating future surprise attacks or other steps are taken, one thing is certain. The consequences of repeating the cycle of failing to connect the dots are too high to ignore. Communities, friends, and families expect more, and rightfully so.



Robert Leverone, M.A., retired as a lieutenant from the Massachusetts State Police (MSP) after thirty-one years of service. He was the commander of the MSP's Special Emergency Response Team, an arm of the agency tasked with crowd control and homeland security-related missions. Robert holds a Bachelor of Science degree in Business Administration from Northeastern University, a Master of Science degree in Criminal Justice from Westfield State University, and a Master of Arts degree in Security Studies (Homeland Security and Defense) from the Naval Postgraduate School, where he authored his thesis, Crowds as Complex Adaptive Systems: Strategic Implications for Law Enforcement. Robert is the owner and president of Crowd Operations Dynamix, Inc., specializing in training and consulting for law enforcement and private industry organizations in crowd management and control issues.

Darren E. Price, M.A., retired in 2020 after over 34 years of government service. He currently consults for public and private sector clients on various homeland security-related projects across the United States. In addition, Darren serves as an adjunct professor in the Homeland Security/Emergency Management Program at Idaho State University and Mount Vernon Nazarene University. He is a graduate of the Naval Postgraduate School's Center for Homeland Defense and Security Master's Program with a Master of Arts degree in Security Studies (Homeland Security and Defense). Darren is also a U.S. Army veteran, where he served as an intelligence analyst in Germany and the United States.

Cargo shipping ports are highly visible and vulnerable targets for cybercriminals. The Port of Los Angeles combats millions of cyber-intrusion threats each year.

Port of Los Angeles, California (*Source:* Downtowngal, CC BY-SA 4.0, via Wikimedia Commons, September 18, 2021).

Fighting Cyberattacks at the Western Hemisphere's Busiest Port

By Gene Seroka

Ports worldwide are responsible for moving billions of dollars of cargo annually, making them highly visible and vulnerable targets for cybercriminals. For example, in 2023, a port in Japan was the victim of an alleged Russian cyberattack, which disrupted cargo flow and caused shipping delays for nearly two days. In November 2023, one of Australia's largest port operators suspended operations for three days after hackers accessed their files. These were just two in a series of such attacks against ports and shipping lines over the past several years.

Fighting Attacks at the Busiest Port

As these types of cyberattacks have escalated, the Port of Los Angeles (POLA) – the busiest container port in the Western Hemisphere – has prioritized cybersecurity and protection of its digital assets and infrastructure. POLA experienced about 754 million cyber-intrusion threats in 2023, or an average of approximately 63 million per month, the highest recorded ever. These intrusion threats are nearly double the level of cyberattacks since the onset of the COVID-19 pandemic in 2020.

Although POLA intercepted these cyber attempts, battling the constant barrage of reconnaissance, network exploitation, ransomware, malware, phishing, and credential harvesting has become a complex 24/7 operation. At a port that processes nearly 10 million units of cargo annually, any single and successful nefarious cyberattack could significantly disrupt operations and quickly extend to the broader supply chain.

Fighting cyberattacks is not a new challenge. Over the past decade, POLA has significantly expanded the digitization of its operations. Although this increased use of digital technologies has resulted in more efficiencies and cargo planning capabilities throughout the supply chain, it has also prompted the need to develop more sophisticated systems to protect against cybersecurity risks and disruption threats.

In 2014, POLA set the maritime industry standard for cybersecurity by establishing the nation's first Cyber Security Operations Center (CSOC) operated by a dedicated in-house cybersecurity team. For almost a decade, the CSOC – part of an overall network of threat intelligence communities, the Multi-State Information Sharing and Analysis Center, and the Federal Bureau of Investigation's Cyberhoodwatch program – served as a centralized location to proactively monitor network traffic to prevent and detect cyber incidents under port control. In establishing the CSOC, POLA became the first port to earn the certification of ISO 27001 information security management systems (ISMS). The ISO 27001 standard provides companies of any size and from all sectors guidance for establishing, implementing, maintaining, and continually improving an ISMS.

Rolling Out the Cyber Resilience Center

With cyberattacks becoming increasingly frequent and more sophisticated, POLA and IBM rolled out the Cyber Resilience Center (CRC) in 2022. The innovative platform, a first-of-its-kind automated port community cyberdefense solution, allows expanded coordination against cyberthreats among POLA and its supply chain partners.

Envisioned as a "system of systems," the $6.8 million CRC enables participating stakeholders – such as cargo firms, terminal operators, shipping lines, longshore labor, as well as truck and rail companies – to automatically share cyberthreat indicators and potential defensive measures with each other in real-time. The CRC also allows POLA to receive, analyze, and share information with other cross-sector stakeholders who provide essential support services within the port complex.

Before the CRC, actionable cyberthreat information often took hours, days, weeks, or months to obtain because most data were collected and processed manually. A key benefit of the new platform is its ability to collect and share data in real time within the POLA ecosystem automatically and more accurately.

The CRC's collaborative approach also has the additional benefit of centralizing threat information for stakeholders, allowing for early detection of potential attacks that otherwise might inadvertently spread and propagate across the supply chain. Participating stakeholders can also use the platform and its information to restore operations following a cyberattack and, as an additional resource, to advise and assist with recovery efforts. The CRC is designed to not be intrusive, disruptive, or burdensome to the stakeholders' existing security operations and systems.

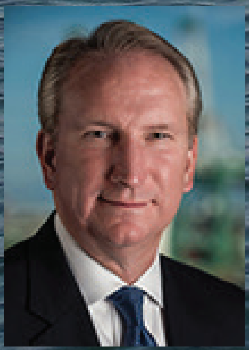
When a threat by the same threat actors, malware, or techniques may affect two or more stakeholders, the CRC immediately informs all stakeholders. The synthesized and anonymized information provides actionable intelligence for stakeholders to utilize. As an advisory unit, the CRC offers on-demand enriched intelligence and research to assist stakeholders during incidents.

The CRC was a substantial investment and a significant next step in POLA's cybersecurity strategy, building upon the port's earlier data protection safeguards. Since its rollout in 2022, it has provided platform users with a new level of awareness and enhanced intelligence, better collective knowledge sharing, and heightened protection against cyberthreats within the supply chain community.

Increasing Need for Cybersecurity Collaboration

As with many issues facing ports and their maritime industry partners worldwide, the need for more collaborative cybersecurity efforts across the supply chain is critical. Adversaries coordinate and share attack tools and information every day. Only through collective and shared knowledge around the issue – including cross sectors of stakeholders that support cargo movement – can ports achieve the necessary cyber readiness and preparedness required in a fast-paced digital world.

The past several years have shown the vital role of ports in the nation's economy, making it paramount that the digital infrastructure of all ports be kept as secure as possible to ensure no disruptions in cargo flow. Building collective knowledge and working together is how that goal can be achieved.



Gene Seroka is the executive director of the Port of Los Angeles, which has experienced a series of historic, record-breaking performances since his appointment in 2014. A respected global trade expert, Seroka has distinguished himself as a leader throughout his illustrious career in shipping, global logistics, and executive management. As executive director of the busiest container port in North America, Seroka is responsible for managing a $2 billion budget, advancing major capital projects, growing trade volume, and promoting innovative, sustainable practices that strengthen the region's economy. Prior to joining the Port, Seroka held several key positions – nationally and internationally – in sales and management for American President Lines (APL) Limited. He holds an MBA and Bachelor of Science in marketing from the University of New Orleans.

Source: Downtowngal, CC BY-SA 4.0, via Wikimedia Commons.

The Impact of Misinformation on Community Resiliency

Damage in the harbor of Lahaina on the island of Maui (*Source:* U.S. Coast Guard Hawai'i Pacific District 14, Public domain, via Wikimedia Commons).

A Foreign Government, Oprah, and Fires in Maui

By Marek N. Posard and Jessica Jensen

Soon after wildfires ripped through the island of Maui in August 2023 – causing more than $5 billion in damage – reports of online trolls, possibly backed by the Chinese government, used social media to spread falsehoods. Among the misinformation were a secret "weather weapon" test, space warfare, and even Oprah Winfrey causing the fires.

One reason a foreign government would bother pushing such ridiculous claims is simple. Crises and disasters are opportunities to undermine the national unity that forms in response to tragedy. U.S. adversaries, including China, Russia, North Korea, Iran, and others, may gain an advantage when there is discord among the American public.

Misinformation – Motivations and Consequences

The Soviet Union perfected this technique, and Russia seems to have revived this playbook, as evidenced by their interference during the presidential elections and recent disasters, like the Ohio train derailment where reports of pro-Russian trolls claimed that authorities were lying about the impact of this chemical spill. Specifically, Russia or other foreign actors identify deep-seated group differences in the country and release a "firehose of falsehood" to prevent the naturally prosocial, unified efforts that often form following crises.

Two things make these types of misinformation operations attractive. First, it is relatively easy to do via social media. TikTok, Instagram, and Twitter provide a direct pipeline to millions of Americans. Second, these operations are inexpensive.

While mis- and disinformation campaigns are low-cost to deploy, emergency management professionals and the disaster-impacted communities they serve can pay a high price. Fortunately, emergency management professionals can apply what they have learned from the field's decades-long efforts to combat disruptive rumors.

Response and recovery are periods when the public needs to receive important – perhaps lifesaving – information dealing with heightened stress and uncertainty. Rumors have long challenged these efforts, whether spread through news outlets, word of mouth, social media, or foreign influence operations that prey on fear, mistrust, and confusion among the public.

The Federal Emergency Management Agency (FEMA) employs means of combating rumors and pushing accurate information. For instance, FEMA routinely releases fact sheets after disasters (like those in Alabama and Louisiana), maintains a common disaster-related rumor page, and frequently updates news outlets. Part of the Joint Information Centers and Public Information Officers' purpose is addressing concerns like this.

Efforts That Local Professionals Should Do

Be Ready – Preparation may produce large dividends during a disaster. The good news is that preparation is relatively inexpensive and can build on activities that communities already carry out. For example:

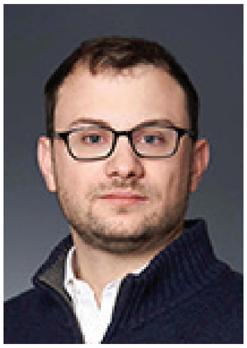
- Add social media and rumor monitoring and control techniques to the jurisdiction's response and recovery plans;
- Include foreign misinformation efforts in tabletop, functional, and full-scale exercises;
- Integrate the potential for foreign actor misinformation campaigns in any Public Information Officer training; and
- Work through how information regarding foreign actor involvement will flow from the federal government to the state and local levels.

Strike a Balance – During disaster response and recovery, take a balanced approach to addressing misinformation perpetuated by foreign actors. It is important to identify misinformation, but do not obsess over it either. It may be tempting to refute falsehoods during a crisis, but that could backfire by amplifying the falsehoods one seeks to minimize.

Focus on the Forest, Not the Trees – RAND research finds that Americans do not like foreign adversaries trying to influence them. Those who learn they are being manipulated act to debunk misinformation themselves. Instead of refuting (and thus repeating) a particular claim made by online trolls:

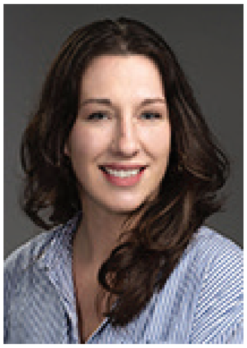
- Explain that nation-state actors may spread misinformation to create confusion and discord; and
- Empower residents with truthful and easy-to-access information.

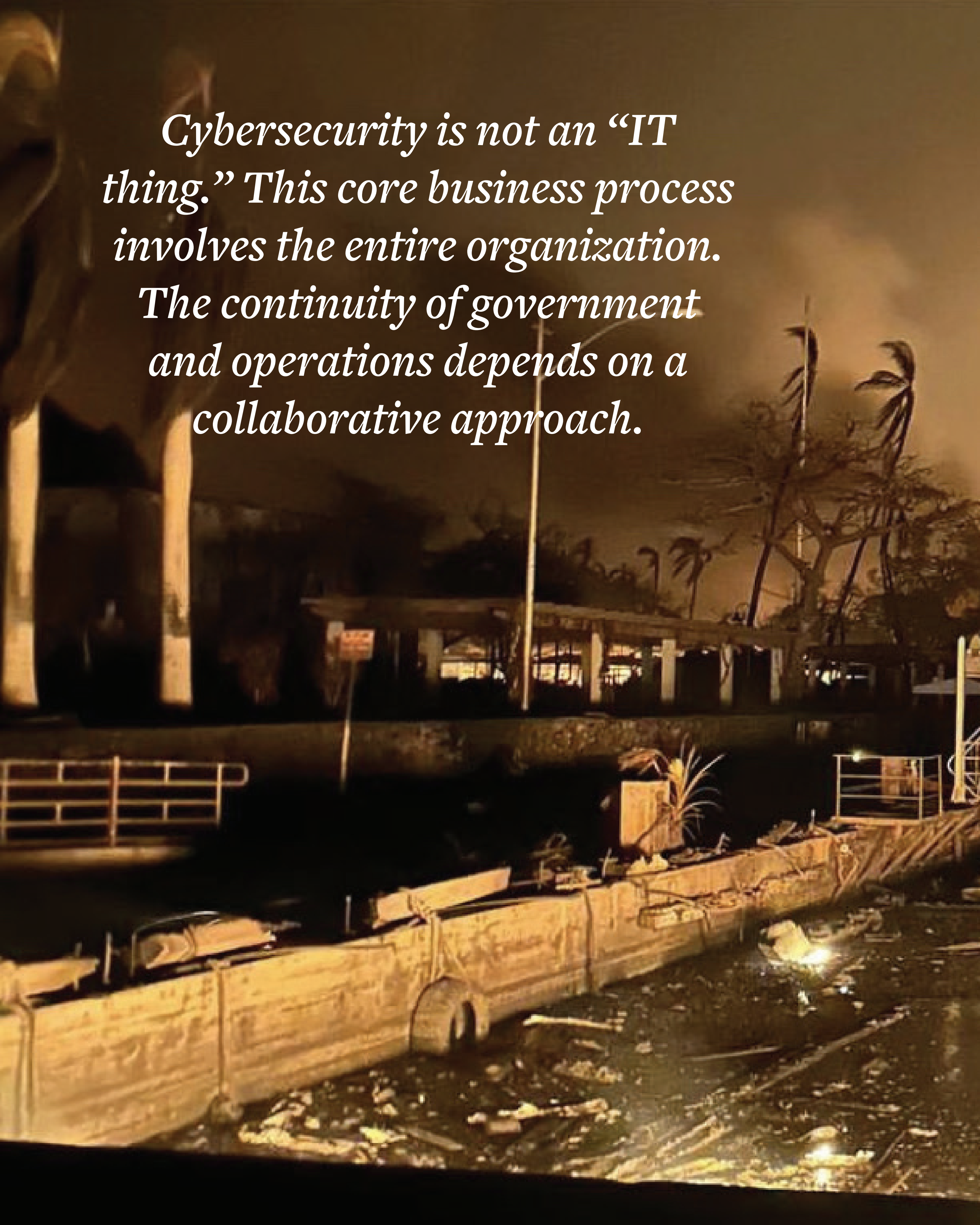
It might seem laughable that there are bureaucrats inside foreign governments creating claims about Oprah moonlighting as an arsonist in Maui, but the creation of these types of falsehoods does happen. Even if information operations are cheap for foreign governments to execute, they also can be simple to counteract effectively through routine emergency management preparedness activities.



Marek N. Posard is a military sociologist at the nonprofit, nonpartisan RAND Corporation and an affiliate faculty member at the Pardee RAND Graduate School.

Jessica Jensen is a policy researcher at the nonprofit, nonpartisan RAND Corporation and an affiliate faculty member at the Pardee RAND Graduate School.





Cybersecurity is not an "IT thing." This core business process involves the entire organization. The continuity of government and operations depends on a collaborative approach.

Source: U.S. Coast Guard Hawai'i Pacific District 14, Public domain, via Wikimedia Commons.

Source: Unsplash/Jason Richard.

Protecting Infrastructure – Cyber, Physical, and EMP Attacks

By David Winks

News feeds warn of cyberattacks on the infrastructure that underpins the U.S. economy, including electric, water, and gas utilities, data centers, cellular networks, and major food suppliers. Terrorists using exploding drones to destroy substations serving this infrastructure is a new tactic that could happen close to home. When the lights, Wi-Fi, and cellular services go out, it may not be as simple as waiting for them to come back on. When all the city noises and cars stop, that silence may indicate the occurrence of an electromagnetic pulse (EMP).

The Grid

Imagine 3,500 spiders, each with their own style, getting together to create a giant web. Now imagine that the web is the power grid, comprising thousands of power companies with thousands of generators, sensors, control and communication systems, trading and billing platforms, transmission and distribution systems, and 140 million customers. With this complexity comes vulnerability to combinations of cyber, physical, and electromagnetic attacks on the power grid.

Cyberattacks can cause regional or nationwide blackouts, as in Ukraine and India. When hackers weaponize substations to create large power spikes, they can induce physical damage to equipment such as motors and computers.

Physical attacks like shooting holes in transformer oil tanks have become frequent enough that utilities are erecting ballistic protection around substations. While this protection helps prevent rifle attacks, it does not contemplate the use of bomb-dropping drones attacking from above. These drones are being used extensively in conflicts globally and by criminal gangs in Mexico. Bomb-dropping drones used against substations or grid control centers are possible.

Electromagnetic attacks on the grid can come from solar storms, radio frequency weapons, and high-altitude EMPs from nuclear detonations in the upper atmosphere.

Impact and Outage Duration

Adversaries may attack when they have a high likelihood of success and a significant impact. Each type of attack has a different level of impact. Cyberattacks can create temporary outages for hours or days and induce physical damage to equipment. The damaged equipment could prolong the outage for weeks or months, depending on the equipment repair or replacement time. While cyberattacks are crafted for specific types of equipment, cyber weapons can have considerable collateral damage beyond the intended target. For example, Russian cyberattacks against Ukraine and Chinese attacks against India caused power outages from hours to days.

Physical damage to substations, such as the Metcalf substation attack, which caused $15 million in damage and shut down 17 transformers, can affect specific targets such as Silicon Valley. When a single site is attacked, power can often be rerouted from other substations to restore service. The attacked site may be down for months since the equipment replacement time for transformers is 18 to 24 months. Coordinated attacks on multiple substations could cause cascading grid failures.

Electromagnetic damage to equipment can be specific or nationwide. There are two types of EMP attacks. One type of attack uses a fast radiated pulse (called E1) from a detonation at an altitude of 46 miles, affecting an area 1,000 miles across. With this type of attack, at least two detonations would be needed to affect the entire U.S. The other uses a single detonation at an altitude of 75 miles to maximize the induced ground current (called E3) and can affect a 2,000-mile diameter.

Unintentional damage can occur from spikes on the grid caused by sudden changes in electrical demand. For example, the rapid charging of millions of vehicles at random times and locations could cause spikes in the power grid as the U.S. moves to electric vehicles. This concern will increase as 13 million commercial trucks, which require as much as one megawatt of power each, are connected to the grid. If not properly designed, spikes from large charging systems can damage nearby residential and business equipment.

Radio frequency (RF) weapons generate pulses through antennas targeted at specific sites. RF weapons can be hand-held or vehicle-mounted – on cruise missiles or drones. The EMPs these weapons generate transfer energy into data cables, power cables, or metal pathways on printed circuit boards. The intent of RF weapons is to upset or damage computer chips used in control systems or data centers, causing the equipment to malfunction or shut down, possibly for weeks.

Solar storms can damage equipment by inducing ground currents, which couple into equipment power lines and coaxial cables. According to NASA:

> *In 2013, Lloyds of London predicted that the most extreme space weather storms could affect 20-40 million people in the U.S. and cause up to $2.6 trillion in damages, with recovery taking up to two years.*

Fortunately, disconnecting from long power lines and cable networks can minimize the effect of the solar storm on electrical equipment. Powering systems from microgrids provides effective mitigation for solar storms.

High-altitude EMPs from nuclear detonations in the upper atmosphere can affect entire continents. This means that EMPs can damage generators, transformers, control systems, and communication systems. They can also cause a collapse in demand by damaging equipment that uses electricity. It could take years to replace the heating, air conditioning, appliances, lighting, and computers across 140 million homes and businesses. Compared to the Lloyds of London estimate for the most extreme solar storm, the cost of an EMP event would be at least three times greater (140 million homes and businesses vs. 40 million people affected), or about $7.8 trillion in damages.

Prevention Beats Cure

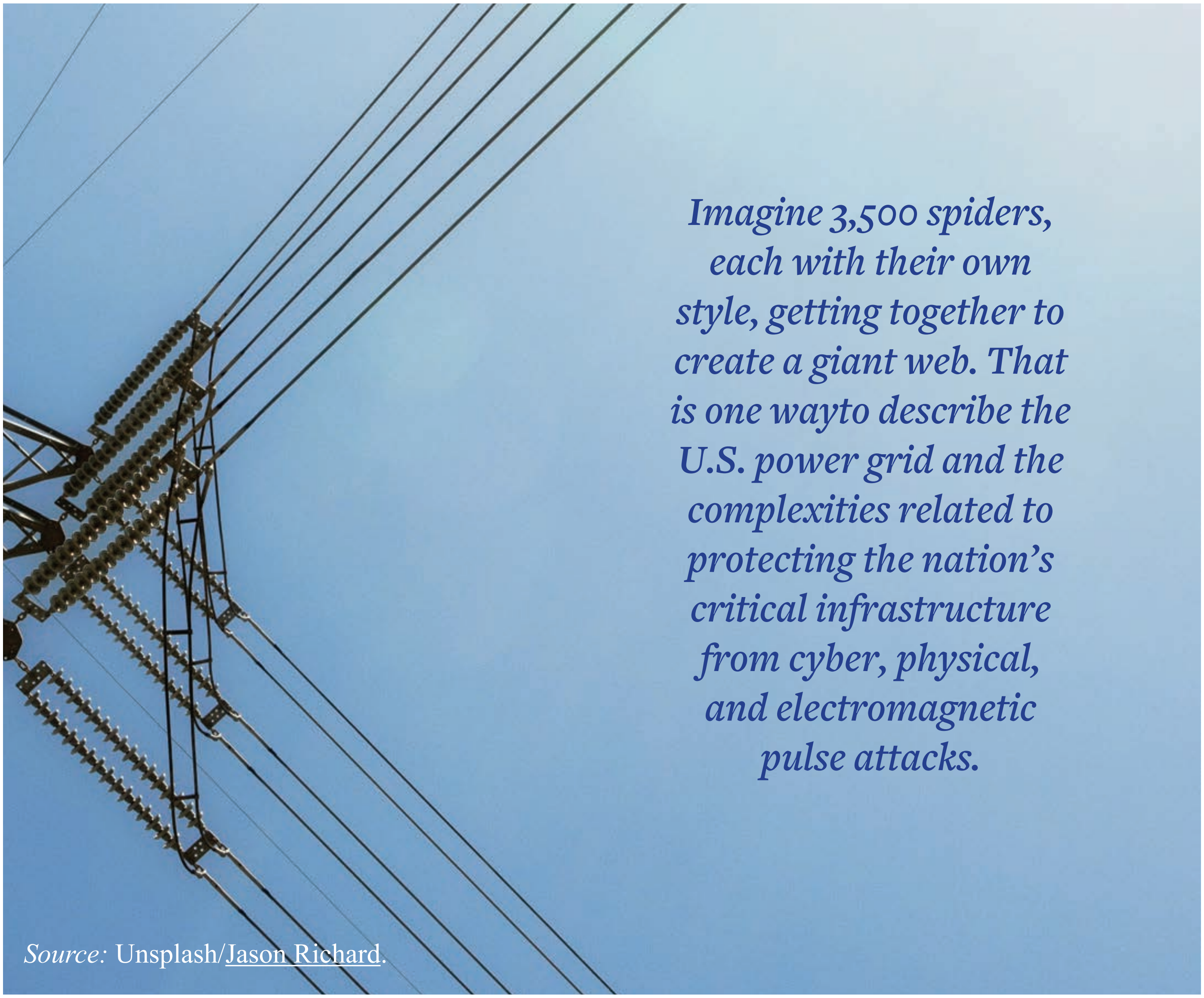
Although it is impossible to prevent all hostile actions, reducing the impact of attacks is possible. Protecting water, power, communications, computing, healthcare, first responders, and transportation systems will be important for the economy to continue functioning after a catastrophic grid outage. By protecting 20% of these infrastructures each year, starting with the most critical, the impact of an attack would continually lessen. Whether the critical infrastructure is owned by private companies, local municipalities, or the federal government, approval by public utility commissions to recover the costs from ratepayers will be critical for the implementation of these protections. The U.S. could be resilient in five years with the protection of the following infrastructure totals:

- 153,000 public water systems (1,560 provide over 10 million gallons/day)
- 25,378 electric generators power the grid
- 55,000 substations
- More than 1,200 natural gas main compressor stations
- 4,238 banks with 70,644 branches
- 4 credit card processing companies with redundant data centers
- 2,653 data centers
- 417,215 cell sites
- 45 undersea cable landing sites in the U.S.
- 10 satellite teleports
- 6,120 hospitals
- 52,291 fire stations
- 17,985 police departments
- 34,661 food and beverage plants
- 40,000 grocery stores
- 147,900 waste collection vehicles
- 13 million commercial trucks
- 38,453 locomotives
- 360 ports
- Department of Defense, Department of Homeland Security, and Federal Bureau of Investigation biometric repositories
- 5,193 public airports, 14,776 private airports

Protection Steps – The Convergence of Physical and Digital (Cyber) Protection

Cyber protection of critical systems starts with rethinking the design of computers and networks, which are built in layers, like a stack of pancakes. The lowest layer is the physical equipment, and the top layer is the application consumers use. By making the lower layers secure, it is possible to better protect the upper layers of the stack. One of the lower layers is the binary layer, which runs processes (subroutines) in memory. If hackers can determine the memory locations of the processes, they can bypass the security controls and make computers do things they were not intended to do.

Equipment manufacturers can randomize the locations of these processes in memory so they are not in the same place on every device. This device uniqueness helps prevent the spread of malware. Uniqueness can also be the basis of device identity for zero-trust implementations. As



> *Imagine 3,500 spiders, each with their own style, getting together to create a giant web. That is one wayto describe the U.S. power grid and the complexities related to protecting the nation's critical infrastructure from cyber, physical, and electromagnetic pulse attacks.*

Source: Unsplash/Jason Richard.

manufacturers use computer chips to build control systems, they can include additional protections. Just as there are physical stops on a dial, control system manufacturers can add hardware limitations to prevent systems from being reprogrammed to run outside of safe operation.

Physical protection of critical systems can be enhanced by realizing that the homeland is now a contested space where saboteurs can destroy equipment. A change in thinking to address these new threats can help envision ways to prevent saboteurs from disrupting systems. Instead of building substations that are defenseless to bomb-dropping drones, utilities could consider placing critical substations underground and disguising the surface to make it difficult for drone operators to identify their targets. Adding non-conductive netting (e.g., to keep quadcopters from landing on transformers with explosives or to prevent dropped munitions from reaching the transformers) and RF counter-drone systems to existing substations might be possible. Non-conductive netting is intended to keep quadcopters from landing on transformers with explosives or to prevent dropped munitions from reaching the transformers. Counter-drone systems prevent drones from reaching their target using one of several approaches. They can take over the drone's control channel, disable it, or use a defensive drone to physically capture it.

Protecting against high-altitude EMPs typically involves placing electronic equipment inside 1/4" thick, seam-welded plate steel enclosures with filter banks for the power connections. Filter banks use inductive and capacitive elements in a circuit to eliminate spikes by regulating both voltage and current (referred to as LC filters). As technology has advanced, there are additional options. Conductive materials made from nickel-coated carbon fiber can provide lightweight passive shielding. Advances have also been made in ultra-fast switching that can redirect EMPs on incoming power lines to ground before they can damage the equipment. EMP-shielded cabinets and surge suppression can protect control electronics, sensors for synchronizing the grid, operation centers, and communication systems. By installing low-voltage EMP surge suppression at business and residential meters, utilities can protect the end user equipment and preserve the demand for electricity so the grid can continue to function.

The Investment

Utilities and co-ops want to serve their customers and provide reliable service. Many are willing to install new technology, especially if it helps provide higher reliability and lower operating costs. Since utilities are rewarded with a return on assets, additional investment in infrastructure increases the utilities' overall returns. Public utility commissioners act as regulators of the utilities on behalf of ratepayers. They want reliable service but keep a close watch on spending to maintain rates as low as possible. Increasing resilience and lowering the impact of cyber, physical, and electromagnetic attacks on infrastructure requires educating the utilities, the public utility commissioners, and the ratepayers. They need to know how the threats have evolved. Educating policymakers is also important. New legislation could encourage and empower public utility commissioners to approve resiliency investments that minimize the consequences of adversarial-caused disasters.

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

Source: Vecteezy.com

A Holistic Approach to Cybersecurity Risk

By Ernesto Ballesteros

Information Technology (IT) enables government and private sector services at all levels to deliver healthcare, treat wastewater, facilitate the administration of government and emergency services, and more. It is difficult to find a facet of modern life that IT does not enable. Therefore, securing these technologically enabled processes is critical to operating business and government. Unfortunately, some may consider cybersecurity an "IT thing" rather than a core business process that involves the entire organization.

Cybersecurity may conjure thoughts of a room down the hall with the servers in it. General awareness about not clicking on phishing links seems to be increasing. However, those in leadership may not think about the consequences of the network going down. For example, consider the impact of a disruption at the local Public Safety Answering Point. Effective processes may or may not be in place to continue this critical function. This example is not merely theoretical. In 2016, Henry County, Tennessee, hackers shut down their computerized dispatch system, requiring all emergency calls to be tracked manually until the system could be restored. This was among the first known attacks on a 911 center, but others followed, including an attack that disrupted several 911 centers across the country.

Similarly, effectively delivering on an agency or department's mission would be challenging if ransomware locked up all records, data, and systems. These systems provide access to Internet Protocol-based cameras, communications devices, and access control devices. In one of the costliest cyber incidents to hit a municipality, the City of Atlanta experienced a ransomware incident in 2018 that disrupted utility payments, traffic tickets, business licenses, and several law enforcement functions, including writing incident reports, processing inmates, and issuing warrants.

Addressing Challenges

Federal, state, and local governments have established more robust cybersecurity postures to address these concerns. They are helping safeguard national, state, and local critical infrastructure from cyberthreats that could disrupt essential functions. However, as technological innovation and change advance, they must continue to advance their cybersecurity efforts proportionate to the risk. As a global challenge, vulnerabilities are increasing as communities continue to add network infrastructure, applications, Internet of Things devices, medical devices, industrial control systems, and other items

Cybersecurity is not an "IT thing."

Source: Vecteezy.com

on the network. These applications, devices, and systems may be layered on top of older, outdated, or more vulnerable technologies. Investments must continuously advance to keep up.

One of the primary challenges confronting state and local governments is that resources dedicated to cybersecurity often face significant competition for funding amid tight budgets. Despite having support sources like federal grants for state and local governments, states and localities often report having insufficient funding to keep up with the changing cybersecurity risk landscape. There are many ways to address these challenges, and many innovative approaches have been implemented. For example, the State of Texas Department of Information Resources provides cybersecurity services, including setting state information security policies, standards, and best practices, assisting with the improvement of cyber incident preparedness, and facilitating information sharing, among other resources. Similarly, the Cybersecurity and Infrastructure Security Agency (CISA) maintains the CISA Resource Hub and provides cyber and physical security assessments, cybersecurity workshops, and guidance on prioritizing vulnerabilities via the Known Exploited Vulnerabilities Catalog.

Asking the Right Questions

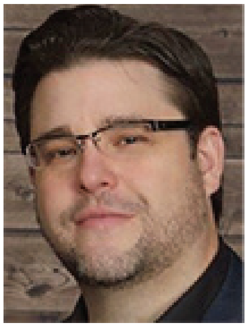
In an environment of limited resources, prioritization is essential. One key aspect of this prioritization is creating a collaborative environment where leadership and IT understand what cybersecurity efforts are integral to the continuing delivery of the most critical services. Following are some non-technical questions for leaders across jurisdictions to ask when prioritizing cybersecurity:

- *Interdependencies* – What IT-enabled business processes and services would most impact our mission if disrupted? What data is most critical to protect? What IT systems do that data reside on? Is there a complete inventory?

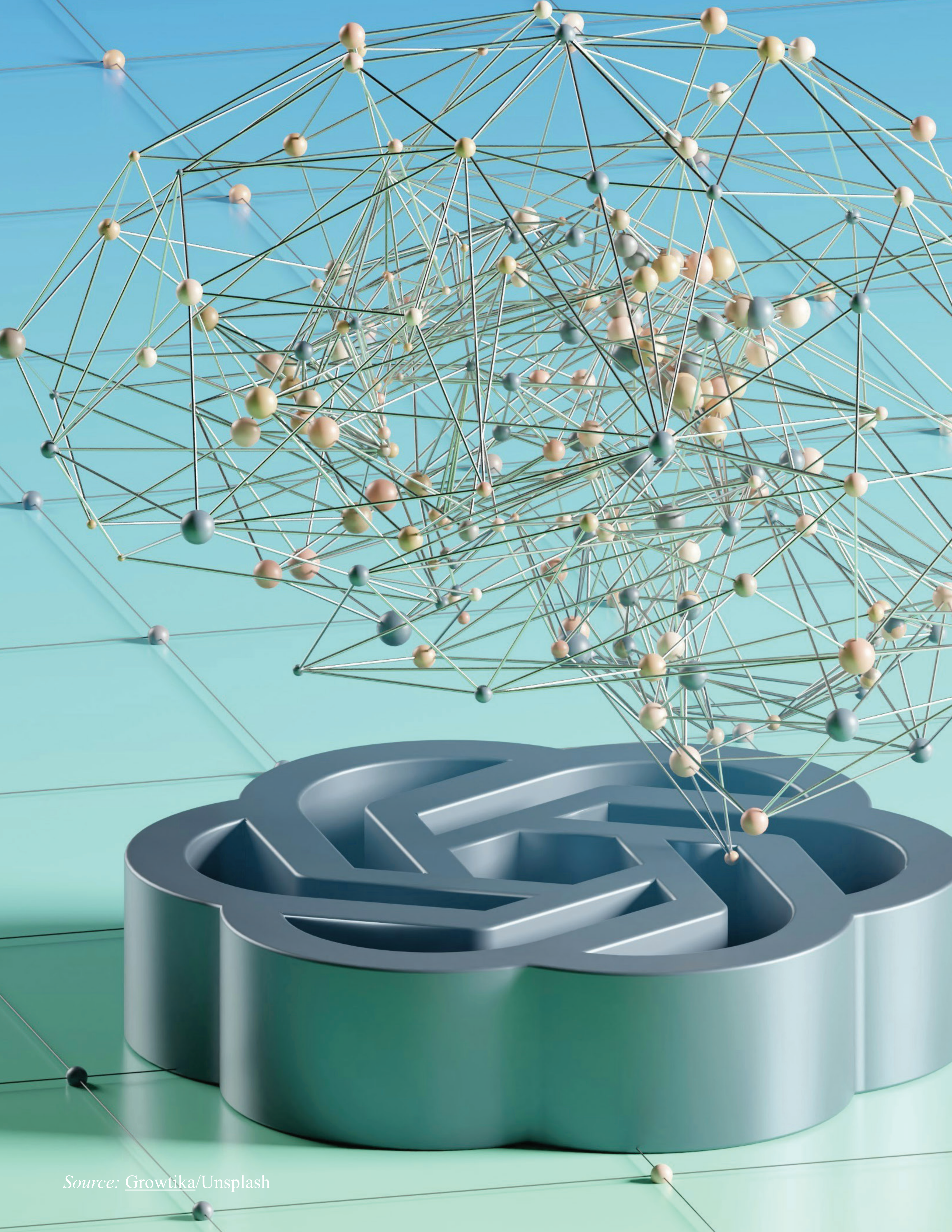
- *Security efforts* – How do we protect those processes, services, and data? Are the security controls we have in place working? Have we assessed them? How many of my systems and business services are currently vulnerable to disruption? Are we engaged in any "Bad Practices"?
- *Response capabilities* – How would we respond in case of a disruption? Do we have a cyber incident management plan? Have we tested it, and is it up to date? Does our continuity plan account for a cybersecurity disruption?
- *Preparedness* – Are we ready for ransomware? Do our backups meet our restoration needs? Are they securely stored offline?
- *Budget* – Given any identified gaps, is our budget adequate for the task of securing our most critical services? Where should we invest more?

Answering these and other questions provides a better understanding of the mission-critical disruption risks from a cybersecurity event. Prioritizing the most critical processes can assist in effectively leveraging services from sources like the Texas Department of Information Resources, the Multi-State Information Sharing and Analysis Center (MS-ISAC), and the CISA.

Cybersecurity challenges for governments in the United States are complex and multifaceted. Overcoming these hurdles requires a concerted effort focusing on prioritization, collaboration, and effectively leveraging resources from partners. As governments continue to adopt new technologies to serve their communities, safeguarding against cyberthreats becomes necessary to ensure the resilience and security of critical infrastructure and core services. By working together, decision-makers can better understand, strengthen, protect, and sustain essential services that impact daily operations.



Ernesto Ballesteros serves as the cybersecurity state coordinator for the State of Texas at the Cybersecurity and Infrastructure Security Agency Region 6. In this role, he builds strategic public and private sector relationships in Texas to facilitate the development and maintenance of secure and resilient infrastructure. Previously, he served the State of Texas, as the state cybersecurity coordinator and chair of the Texas Cybersecurity Council at the Texas Department of Information Resources. As the state cybersecurity coordinator, Ballesteros led the Texas Cybersecurity Council to collaborate on state cybersecurity matters. He contributed to the development and implementation of statewide initiatives, such as the Texas Information Sharing and Analysis Organization, the Statewide Cybersecurity Awareness Training Program, and more. Prior professional roles include: information security officer for the Alamo Colleges District (San Antonio, Texas); information security officer at Jefferson Bank (San Antonio); information security consultant at Omnikron Systems (Woodland Hills, California); assistant professor of Computer Information Systems and Security at Our Lady of the Lake University (San Antonio); director of the Center for Information Assurance Management and Leadership at Our Lady of the Lake University (San Antonio); and information systems auditor for CPS Energy (San Antonio). Ballesteros is an adjunct professor of Law at St. Mary's University School of Law (San Antonio), where he teaches cybersecurity, information systems, and law.



Source: Growtika/Unsplash

Nation-State Activity in the Age of Artificial Intelligence and Quantum Computing

By Margaret (Margie) Graves

Seldom has there been a simultaneous evolution of two powerful and complementary technologies – artificial intelligence (AI) and quantum computing (QC). AI refers to machines programmed to mimic human intelligence. These systems use algorithms to analyze data, recognize patterns, and make decisions. Generative AI is a subset of AI that creates new content from learned data. It generates original material across various mediums (text, images, audio, etc.). Traditional AI analyzes existing data, but generative AI goes beyond by generating new content. QC involves specialized technology, including computer hardware and algorithms, that harnesses the unique properties of quantum mechanics. Unlike classical computers or supercomputers, quantum computers can solve problems that are either impossible for classical machines to solve or would take an impractical amount of time.

Nation states are in a race to harness the power of these technologies for social good, economic advantage and growth, geopolitical influence, and cybersecurity. Many countries, whether allies or enemies, are investing in AI and QC capabilities and highlighting the adoption and use of these technologies in policies, legislation, and strategic imperatives.

For example, in 2015, China published its "Made-in-China" strategy, which states the strategic objective of becoming dominant in specific technology markets, including AI and machine learning, the Internet of Things, and chip manufacturing. The U.S. and its allies have considered this objective to be a threat not only to economic growth but also to national security. The U.S. has responded by using trade policy to limit the incorporation of products from China and other unfriendly nation states in the national technology ecosystem.

The CHIPS Act legislation addresses some of these challenges by offering approaches to reduce supply chain risk and investing in AI and QC technologies to increase the country's competitive edge. There also is an emphasis on strengthening the protection of intellectual property created in research and development centers. Aside from these measures, significant policies solidify the importance of the effective adoption, appropriate use, and vigilant cyber protection of AI technology, as evidenced by a comprehensive executive order.

Benefits of AI and QC

AI and QC offer significant benefits for executing private-sector business and government missions. The combination of AI and QC gives companies and governments the ability to curate large amounts of unstructured data (AI), find the "signal in the noise," and perform pattern recognition in such rapid computational timeframes (QC) that the outputs from the algorithmic analyses can help make strategic and operational decisions in real-time. In addition to providing powerful analytic support for decisions, AI and QC also offer organizations the ability to use predictive analytics to continuously improve resilience, especially during a crisis. A few of the most powerful use cases include:

- *Medical research* – AI and QC can assist in medical diagnostics for rare or critical illnesses, biomedical and genetic research, and pharmaceutical development. During the first phases of the COVID-19 pandemic, the OECD tracked and published on its website the use of AI in addressing the crisis. More recently, the Cleveland Clinic has deployed a QC capability, the first of its kind solely dedicated to biomedical research.
- *Climate resiliency and emergency preparedness* – According to the National Oceanic and Atmospheric Administration (NOAA) Center for Artificial Intelligence (NCAI) website, "NOAA has a long history of using AI in weather forecasting, climate modeling, and environmental monitoring," and the NCAI is its "conduit for artificial intelligence and machine learning for mission science initiatives." The Federal Emergency Management Agency (FEMA) is using AI to conduct geospatial damage assessments after a natural disaster. Disaster relief suppliers of goods and services use AI to optimize their supply chain and transportation networks to ensure rapid delivery.
- *Fraud risk reduction* – AI can identify patterns of fraud in benefit transactions. The Department of Health and Human Services uses AI to identify fraudulent pharmaceuticals and Medicare or Medicaid fraud. FEMA is using AI to identify fraudulent disaster relief applications.
- *Cybersecurity* – AI can enhance the effectiveness of cybersecurity operations and defense by identifying attack patterns, recognizing anomalous activity, performing predictive risk analysis that can help expand defenses and train cyber defenders, and automating a matching response based on defense approaches that have worked against past cyberattacks.

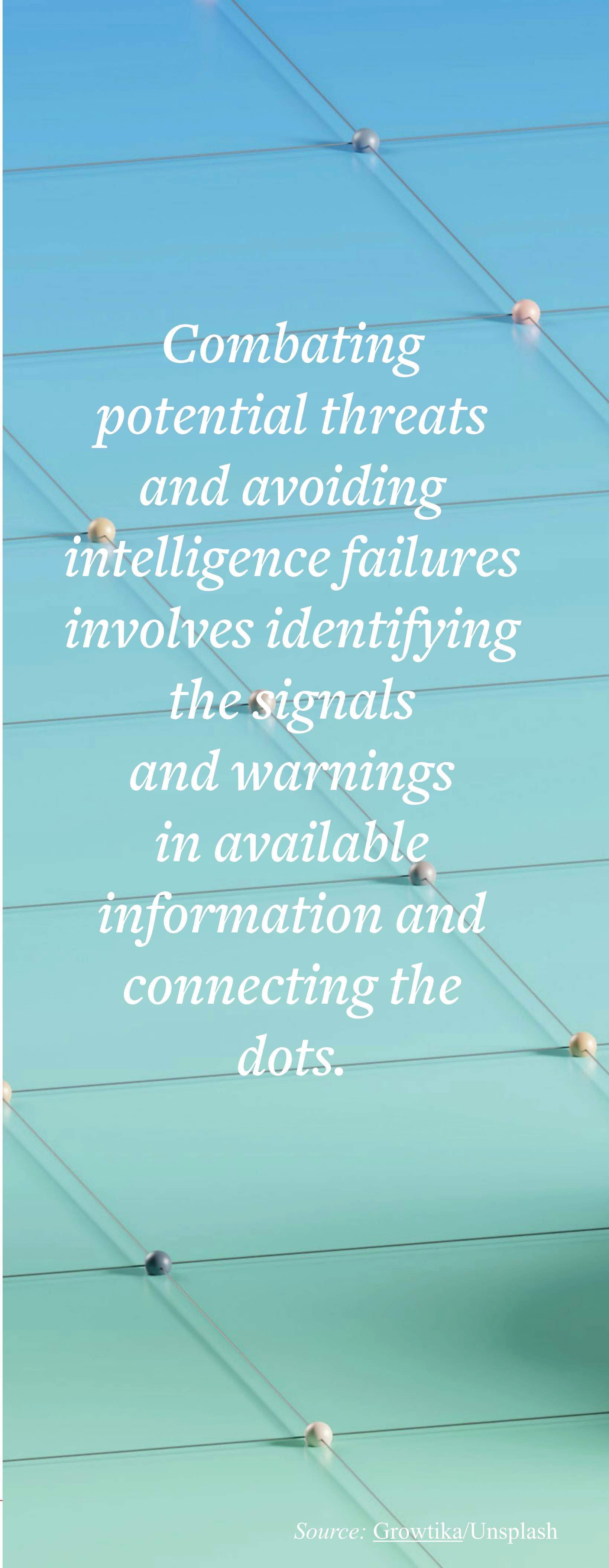
Dual-Use Technologies

Unfortunately, knowledge of these technologies leads to a point-counterpoint argument in which each capability that can be used for good can also be used by criminals or nation-state actors for nefarious purposes. Nowhere is this point-counterpoint phenomenon more evident than in the national security realm. For example, there is understandable excitement about the ability of AI to accelerate and enhance the development of valuable computer code. However, at the same time, an attacker could use this capability to create stronger self-healing malware in which multiple strains of malware are fed to an algorithm, thus creating strains that are harder to detect. This malware could subsequently be used in disruption or exfiltration of sensitive national security data.

Another risk arises by the very nature of AI's fundamental principles. AI uses massive amounts of data to feed machine learning. Having such a large amount of data in one system could present an attractive attack surface to adversaries. Designing and building these systems with that risk in mind is imperative. Generative AI also poses an emerging threat as it enables adversaries to create more dangerous phishing attacks by creating emails that are convincing in their content. Finally, developing deep fake identities provides an opportunity to create civil unrest and influence political outcomes.

Protective Steps That Organizations Should Take

Organizations should define practical steps that private or public sector organizations can take to ensure they derive the most good from these technologies while protecting their vulnerabilities. To that end, in the 2022-23 timeframe the National Academy of Public Administration and the IBM Center for the Business of Government conducted a series of roundtables with eminent executives from government, industry, and academia to openly discuss strategies for improving nation-state government resiliency in the face of "future shocks" in the areas of emergency management, cybersecurity, supply chain, climate resilience, and workforce development. These roundtables helped produce individual reports, a compendium, and a book with recommended actions for executives. These publications were released in November of 2023 and are referenced in this article.



Combating potential threats and avoiding intelligence failures involves identifying the signals and warnings in available information and connecting the dots.

Source: Growtika/Unsplash

Several reports indicated that thoughtful implementation and appropriate use of AI and QC can bring tremendous benefits. However, those implementations must be underpinned by a structure that at least recognizes the importance of the following elements:

- *Governance structure* – There should be recognition that AI and cybersecurity are risk factors to include in C-suite discussions. They are not simply technology issues. The appropriate implementation of AI includes ensuring that it is comprehensive, inclusive, unbiased, and secure. Proper use is the responsibility of the highest level of the organization.
- *AI literacy and workforce development* – All levels of the organization should know how to leverage these technologies to improve the mission and what risks they present. Role-based training is critical, from C-suite executives to practitioners.
- *Public, private, and academic partnerships* – There should be a constant exchange of information regarding the risk and threat landscape, successful use cases and implementations, and evolving research and development.
- *Investment in innovation and transformation* – Chief information officers, chief data officers, and AI executives must work together to address all elements of quality AI implementations, including infrastructure, tools, and data strategies supporting mission- or business-driven use cases.

In conclusion, using AI and QC for business and mission results presents promise and peril. Critical missions such as national defense and public health and safety will benefit from real-time enhanced situational awareness and the ability to optimize predictive analysis, defense, response, and recovery. Additional benefits include the support of fair trade and commerce by creating economic stability in global markets to reduce the possibility of geopolitical destabilization. A business result is providing services to the population that are delivered in a more transparent and accelerated fashion, thereby enhancing the customer experience. Staying abreast of the evolving landscape and remaining vigilant will ensure that organizations protect against unintended consequences and take the right pathway into the future.

Margaret (Margie) Graves is a senior fellow with the IBM Center for The Business of Government and the IBM Partner for Digital Transformation Strategy. She serves as a senior advisor to IBM's Federal Services practice and is a member of IBM's Former Government Executives Council. As the former federal deputy chief information officer, she led the Office of the Federal Chief Information Officer efforts to drive value, deliver digital services, protect federal IT assets through cybersecurity, and develop the technology workforce. Before her role as federal deputy chief information officer (CIO), Margie served as the deputy CIO at the U.S. Department of Homeland Security, overseeing an IT portfolio of $5.4 billion in programs. Margie also has held numerous leadership positions in nonprofit organizations, including the American Council for Technology-Industry Advisory Council (ACT-IAC), the National Academy of Public Administration, and the Partnership for Public Service. She also serves on the Board of the Northern Virginia Technology Council. Margie's private-sector experience in the management consulting industry has included holding executive positions and performing consulting engagements for clients. She holds an M.B.A. and a B.S. in Chemistry from the University of Virginia.