

critical infrastructure



PROTECTION AND RESILIENCE NEWS

Official Magazine of



SPRING 2026

www.cip-association.org

FEATURE:

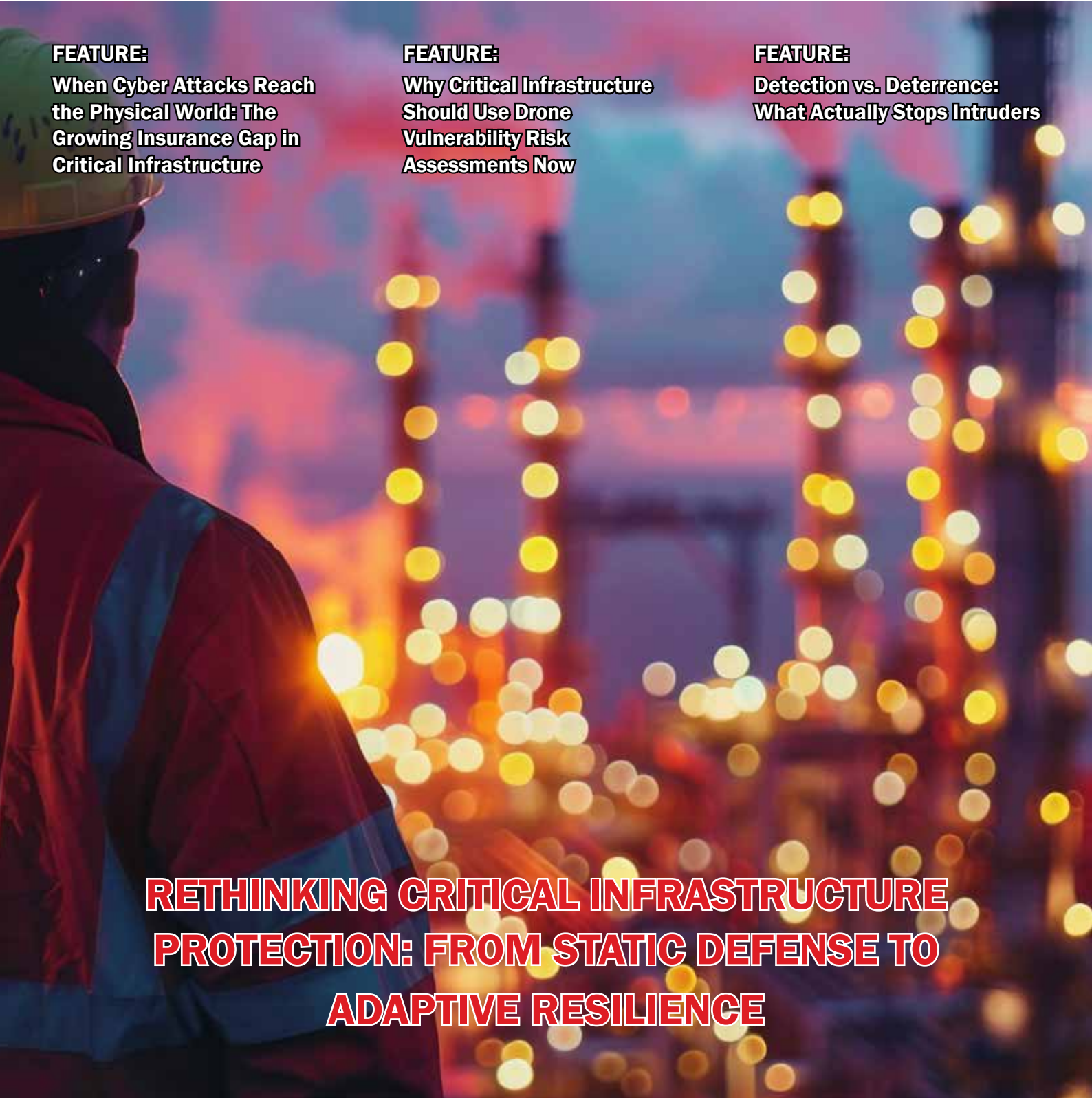
When Cyber Attacks Reach the Physical World: The Growing Insurance Gap in Critical Infrastructure

FEATURE:

Why Critical Infrastructure Should Use Drone Vulnerability Risk Assessments Now

FEATURE:

Detection vs. Deterrence: What Actually Stops Intruders



**RETHINKING CRITICAL INFRASTRUCTURE
PROTECTION: FROM STATIC DEFENSE TO
ADAPTIVE RESILIENCE**

critical infrastructure PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium

www.cipre-expo.com

The International Association for CIP Professionals (IACIPP) is proud to announce that CIP Week Europe 2026 will take place in Brussels, Belgium, in the heart that shapes policy for CIPR.

Invitation to Participate

As Europe's leading forum for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together senior leaders from industry, operators, agencies, and government to strengthen collaboration and drive innovation in protecting Europe's essential systems and services.

Register today — Early Bird rates end 20th September 2026.

Now in its 11th year, the conference addresses the most pressing challenges facing operators and agencies, including NIS2 and CER Directive implementation, business continuity, and the resilience of critical infrastructure and entities.

CIPRE features an outstanding international speaker faculty, delivering expert insight, practical experience, and valuable knowledge to support ongoing professional development.

For further information and registration, visit www.cipre-expo.com

Join us in Brussels and network with leading decision makers from corporate and government establishments, agencies and operators tasked with Critical Infrastructure Protection and Resilience.

Co-Hosted by:



Flagship Media Partner:



Global Cybersecurity Partner:



Silver Sponsor:



Supported by:



Help2Protect



THE CHALLENGING START TO THE YEAR LOOKS SET TO CONTINUE

As we move into the Spring edition of the magazine, hopes for a more stable and predictable global environment remain difficult to realise. Instead, the opening months of 2026 have continued to highlight just how interconnected, volatile, and fragile the world around us has become.

Ongoing conflict in Ukraine, instability across the Middle East, and growing geopolitical tensions involving China, North Korea, and other state and non-state actors continue to shape an increasingly uncertain global landscape. Alongside this, economic pressures, supply chain disruption, cyber aggression, and political instability are placing unprecedented strain on critical infrastructure and the organisations responsible for protecting it.

Recent incidents across energy, transportation, telecommunications, healthcare, and water systems have reinforced an important reality: disruption in one sector or region can now have immediate and far-reaching consequences elsewhere.

As we explored at the recent Critical Infrastructure Protection & Resilience North America (CIPRNA) in Baton Rouge, Louisiana, critical infrastructure no longer operates in isolation and increasing dependence on digital technologies, automation, cloud services, and artificial intelligence is transforming operations and creating major opportunities, but also introducing new vulnerabilities and dependencies that must be carefully managed.

The threat landscape is evolving rapidly, and as was highlighted at CIPRNA, awareness of resilience, security, and continuity planning has never been higher. Governments, regulators, and industry leaders increasingly recognise that resilience is not simply a technical issue, but a strategic necessity.

Collaboration across sectors and international borders continues to strengthen, driven by the understanding that no organisation can face today's threats alone. CIPR News exists to support that collective effort.

In this Spring edition, we explore the evolving threat and resilience landscape, examine the socio-economic impacts of infrastructure disruption, and highlight practical strategies organisations can adopt to strengthen both physical and cyber resilience. You will also find insights from practitioners across the sector, analysis of emerging trends, and lessons learned.

As 2026 continues, uncertainty may remain a constant. How we respond to it is not! By staying informed, connected, and proactive, we can continue to strengthen the systems and services society depends upon every day.

Thank you for reading, and thank you for the vital work you do in helping protect critical infrastructure across an increasingly uncertain world.

Ed.

Ed.

www.cip-association.org

Editorial:

Neil Walker

E: neilw@torchmarketing.co.uk

Design, Marketing & Production:

Neil Walker

E: neilw@torchmarketing.co.uk

Critical Infrastructure Protection & Resilience News is the newsletter of the International Association of CIP Professionals and distributed to over 80,000 organisations globally.



Rethinking Critical Infrastructure Protection: From Static Defense to Adaptive Resilience



By Prof. Ehab ElHegawy, Professor of Security Sciences | Head, Department of Security Crisis Management, Dubai Police Academy, UAE

The End of Predictability

Critical infrastructure is no longer operating in a predictable, linear environment. For decades, the global approach to infrastructure protection was built on a foundational assumption of stability: threats were generally discrete, identifiable, and could be kept at bay through robust

perimeter defenses. We built higher walls, thicker firewalls, and more rigid compliance frameworks. Today, however, these systems face overlapping disruptions driven by the convergence of climate pressures, sophisticated cyber-physical threats, and the exponentially increasing interdependencies between sectors.

The events of recent years have shattered the illusion of isolated failures. The global IT outage in mid-2024, triggered by a routine software update from a major cybersecurity vendor, demonstrated with chilling clarity how a single point of failure in the digital supply chain could cascade instantaneously across aviation,

healthcare, finance, and logistics worldwide. Similarly, the increasing frequency of extreme weather events intersecting with targeted cyber-attacks on energy grids has shown that risks are no longer isolated. They are connected, dynamic, and often simultaneous.

Traditional protection models were explicitly built to defend against known threats. They focus heavily on prevention, hardening of assets, and reactive response protocols. While these elements remain essential components of a comprehensive security posture, they are no longer sufficient on their own. The current risk landscape requires a fundamental paradigm shift—a transition that allows critical infrastructure to continue functioning even when disruptions inevitably bypass defensive perimeters.

This is where the concept of resilience becomes not just an academic theory, but an operational imperative. Resilience is not merely about stopping disruptions; it is about maintaining core operations despite them. It reflects a strategic shift from static defense toward adaptive performance. Instead of asking exclusively, 'How can we prevent failure?', the governing question for modern security leaders must become: 'How can our systems continue to operate, adapt, and deliver value under extreme stress?'

The Structural Limitations of Traditional Approaches

To understand why a new paradigm is necessary, we must critically examine the limitations of the traditional Critical Infrastructure Protection (CIP) models that still dominate national strategies.



One of the most significant vulnerabilities of traditional approaches is their entrenched reliance on sector-based, siloed thinking. Historically, energy, transport, water, telecommunications, and financial services have been managed, regulated, and secured as separate entities. However, modern infrastructure does not respect these artificial administrative boundaries. A disruption in the power grid immediately cripples telecommunications, which in turn blinds the logistics and transport sectors, leading to supply chain paralysis. This siloed management creates severe coordination gaps and exponentially increases the risk of cascading failures. When security teams only have visibility into their specific sector, they are effectively flying blind to the systemic risks building up in the interconnected web.

Another critical limitation is the over-reliance on static risk assessments. In many organizations, risk assessments are treated as compliance exercises—documents updated annually or bi-annually based on historical data and known scenarios. These static models are structurally incapable of keeping pace with

fast-evolving, asymmetric threats. They assume a static baseline that no longer exists. When a novel threat emerges—whether a zero-day exploit or an unprecedented climatic anomaly—static defense mechanisms are often paralyzed by the lack of a pre-defined playbook.

Furthermore, traditional models often equate security with rigidity. The assumption is that the more locked-down a system is, the more secure it is. However, in complex, interdependent networks, rigidity often leads to brittleness. When a rigid system is pushed beyond its design parameters, it does not bend; it breaks catastrophically. To address these systemic vulnerabilities, the global security community must move beyond the illusion of absolute protection and embrace a more practical, dynamic, and adaptive approach.

The Adaptive Resilience Paradigm: A Four-Capability Framework

Transitioning from static defense to adaptive resilience requires more than a change in terminology; it requires a fundamental restructuring of how infrastructure is designed, governed, and operated. A

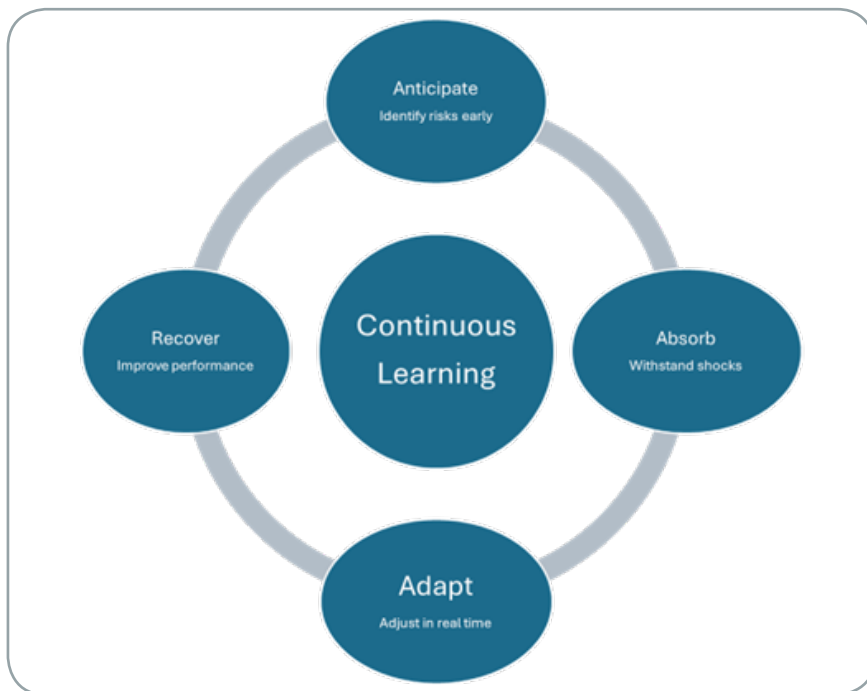


Figure 1: The Adaptive Resilience Cycle for Critical Infrastructure

practical and practitioner-focused way to operationalize resilience is through a continuous cycle of four core capabilities: Anticipation, Absorption, Adaptation, and Recovery.

Unlike traditional linear response models (Prevent - Respond - Recover), this framework operates as a continuous, dynamic loop — as illustrated in Figure 1 below.

1. Anticipate: Beyond Threat Intelligence

Anticipation goes beyond traditional threat intelligence. It is the ability to identify emerging risks, systemic vulnerabilities, and potential cascading effects before they materialize into full-scale crises. This requires moving from historical data analysis to strategic foresight. In highly interconnected environments, anticipation means mapping the hidden dependencies between your systems and third-party vendors. It involves continuous horizon scanning, utilizing AI-driven predictive analytics,

and understanding the ‘weak signals’ that precede a systemic shock. True anticipation means recognizing that the next major disruption will likely come from a vector you have not explicitly planned for.

2. Absorb: Designing for Graceful Degradation

Absorption is the capacity of a system to withstand a shock without experiencing total systemic collapse. In traditional models, systems are often binary: they are either fully operational or completely offline. An adaptive system is designed for ‘graceful degradation.’ This means that when a cyber-attack or physical disruption occurs, the system can isolate the damaged components and maintain essential, life-safety, or mission-critical functions, even at a reduced capacity. Absorption requires structural redundancy, decentralized architectures, and the deliberate engineering of ‘circuit breakers’ that prevent a localized failure from cascading across the entire network.

3. Adapt: Real-Time Operational Agility

Adaptation is the most critical differentiator between rigid defense and true resilience. Absorption buys the system time; Adaptation is what the system does with that time. It is the ability to modify operations, reallocate resources, and change decision-making structures in real-time as a crisis unfolds. When the operational environment changes drastically, static playbooks become obsolete. Adaptation requires empowered, decentralized leadership where frontline managers have the authority to make rapid decisions without waiting for top-down consensus. It also involves technical agility—such as the ability to dynamically reroute data traffic, switch to alternative energy sources, or utilize backup communication channels seamlessly.

4. Recover: Improving Future Performance

In traditional models, recovery means returning to the pre-crisis baseline—the status quo. In the Adaptive Resilience framework, returning to the baseline is considered a failure of learning. If a system recovers only to its previous state, it remains just as vulnerable to the next disruption. True recovery involves continuous learning and systemic evolution. It means analyzing the root causes of the disruption, identifying the friction points in the response, and integrating those lessons into the system’s architecture and governance. Recovery must result in measurably improved performance and enhanced resilience against future shocks.

Insights from the Gulf: The

Microcosm of Interdependency

The necessity of this adaptive approach is nowhere more evident than in high-density, technology-driven environments such as the Gulf region. Cities like Dubai and Abu Dhabi represent the vanguard of integrated urban environments, where the concept of the 'Smart City' has been fully realized. In these environments, critical infrastructure—water desalination, district cooling, automated transport, and digital governance—is hyper-connected through the Internet of Things (IoT) and centralized data hubs.

These regions serve as a critical microcosm for the future of global infrastructure. They highlight a crucial reality: resilience cannot be bolted on as an afterthought or activated only during a crisis; it must be built into the DNA of everyday operations. Systems that perform well under stress in these environments are those that are continuously monitored, regularly stress-tested through advanced simulations, and supported by robust, cross-sector governance frameworks.

A key insight from these hyper-connected environments is the critical importance of decision-making speed. In interdependent systems, the window for intervention is drastically compressed. A disruption in a smart grid can escalate into a multi-sector crisis in minutes, not hours. Delayed responses exponentially increase the likelihood of cascading failures. Therefore, real-time coordination, automated information sharing between public and private entities, and joint operational command centers are not optional luxuries—they are baseline requirements for survival.



Moreover, the Gulf region's experience with large-scale events—such as Expo 2020 Dubai, which brought together 192 nations across a hyper-connected physical and digital platform—provides a powerful case study in operationalized resilience. Security planners were required to protect an environment where cyber threats, physical security, health emergencies, and logistical disruptions could materialize simultaneously and at scale. The approach adopted was not one of absolute prevention, but of continuous anticipation and rapid adaptation. Dedicated cross-agency coordination centers operated around the clock, empowered to make real-time decisions across sector boundaries. The lesson was unambiguous: resilience is a governance model, not merely a technical solution. It demands that human systems—command structures, communication protocols, and leadership cultures—evolve in parallel with the technical infrastructure they are designed to protect. This is a lesson that applies equally to every infrastructure operator,

regardless of geography or sector.

Actionable Recommendations for Security Leaders

For professionals, site managers, and policymakers working in critical infrastructure, transitioning to this adaptive model requires deliberate, sustained effort. The following practical actions can significantly strengthen institutional resilience without requiring an immediate, ground-up redesign of existing systems:

- 1. Map Cross-Sector Interdependencies:** Move beyond internal risk assessments. Conduct rigorous mapping of your dependencies on external sectors (power, water, telecom, third-party IT vendors) to understand exactly how external failures will cascade into your operations.
- 2. Establish Real-Time Coordination Mechanisms:** Break down the silos. Create joint communication protocols and shared dashboards between infrastructure operators, government agencies, and emergency responders to



drastically reduce the time between detection and response.

3. Integrate Scenario-Based Planning:

Abandon static risk matrices. Implement dynamic, scenario-based wargaming that simulates complex, multi-hazard environments (e.g., a simultaneous cyber-attack during an extreme weather event) to test the limits of your absorption and adaptation capabilities.

4. Design for Operational Flexibility:

Engineer systems with the capacity for graceful degradation. Ensure that critical functions can be manually overridden or physically isolated from the broader network to maintain partial functionality under extreme stress.

5. Invest in Leadership Readiness:

Resilience is ultimately a human endeavor. Train leaders to make high-stakes decisions under conditions of extreme uncertainty and incomplete information. Empower frontline managers to adapt protocols dynamically when rigid playbooks fail.

6. Embed Continuous Learning:

Institutionalize the recovery phase. Create formal mechanisms to systematically extract lessons from every disruption, near-miss, and simulation, ensuring these insights are immediately integrated into future architectural and governance planning.

It is important to emphasize that these six actions are not isolated technical upgrades. They represent a coherent governance philosophy. Individually, each action strengthens a specific vulnerability. Collectively, they create a self-reinforcing cycle of institutional resilience. Organizations that have begun this transition report not only a measurable improvement in their crisis response capabilities, but also greater confidence among leadership in navigating uncertainty. In an era defined by permanent volatility, the ability to adapt is no longer a competitive advantage—it is the baseline requirement for continued operational relevance.

Conclusion: The New Foundation of Governance

The future of critical infrastructure protection will not be defined by who can build the strongest defenses, but by who can sustain operations through the most severe disruptions. The illusion that we can predict and prevent every threat has been definitively shattered by the complex realities of the modern, interconnected world.

Transitioning from static defense to adaptive resilience is no longer a theoretical debate; it is the new foundation for effective infrastructure governance. By embracing a continuous cycle of anticipation, absorption, adaptation, and evolutionary recovery, security leaders can ensure that our most vital systems remain functional, reliable, and capable of supporting society—no matter what shocks the future holds.

Resilience is no longer an option. It is the definitive metric of survival.

About the Author

Prof. Ehab ElHegawy is Professor of Security Sciences and Head of Security Crisis Management at Dubai Police Academy, UAE, with 30 years of operational and academic experience.

CISA, National Cyber Security Centre (NCSC) UK, and Global Partners Issue Advisory on Chinese Government-Linked Covert Cyber Networks

The Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC-UK), together with federal and international partners, have released a new cybersecurity advisory titled "Defending Against China-Nexus Covert Networks of Compromised Devices." This advisory equips network defenders with vital tools and resources to combat the threat posed by Chinese government-linked threat actors' use of covert networks of compromised devices.

"Working closely with U.S. and international partners, CISA continues to identify and warn organizations of Chinese state-sponsored cyber actors threatening critical infrastructure. This advisory informs organizations of how these actors are strategically using numerous, evolving covert networks at scale for malicious cyber activity," said CISA Acting Director Nick Andersen. "CISA strongly encourages organizations to review and implement appropriate mitigation measures to defend



their devices from this threat. Every day, CISA works to empower organizations with actionable information to strengthen their security and resilience against cyber threats."

The advisory explains how attackers create hidden networks by taking advantage of weak devices, like those used at home or in small offices, as well as Internet of Things (IoT) gadgets. It also describes how groups such as Volt Typhoon and Flax Typhoon use large groups of hijacked devices, called botnets, to hide who they are and carry

out spying, break-ins, controlling devices, and stealing data.

Cyber defenders are provided with comprehensive guidance to identify, baseline, and mitigate activity from dynamic and deniable covert networks, aimed at reducing the risk of organizational compromise.

To strengthen defenses, CISA and partners advise organizations to:

- Map and understand network edge devices, developing a clear understanding of organizational assets and what should be connected to them.
- Baseline normal connections, especially to corporate VPNs or other similar services.
- Maintain log collection and storage solutions to assist with detecting and responding to unauthorized access attempts.
- Implement multifactor authentication for remote connections.

CISA and U.S. Government Partners Unveil Guide to Accelerate Zero Trust Adoption in Operational Technology

The Cybersecurity and Infrastructure Security Agency (CISA), along with the Department of War (DoW), Department of Energy (DOE), Federal Bureau of Investigation (FBI) and Department of State (DOS) today published a joint guide to assist organizations with operational technology (OT) systems - including government systems - with applying Zero Trust principles. The guide, *Adapting Zero Trust Principles to Operational Technology*, provides OT owners and operators and Zero

Trust practitioners with practical insights on overcoming unique constraints, addressing potential challenges, and prioritizing key areas for integrating Zero Trust into OT environments.

New attack vectors, expanded attack surface and magnified cybersecurity risks are more prevalent because OT systems are becoming increasingly interconnected, digitally monitored, and remotely operated. Improperly secured pathways create opportunities for threat

actors to gain access to information technology (IT) and OT networks. Adapting and applying Zero Trust principles to fit the operational realities of the OT environment can help owners and operators close cyber risk gaps, however, it must be done carefully without disrupting their own systems in the process. Zero Trust strategies can prevent adversaries from compromising, manipulating, degrading, and disrupting the critical physical processes these systems control.

When Cyber Attacks Reach the Physical World: The Growing Insurance Gap in Critical Infrastructure



By Neil Arklie, Cyber Insurance Expert, DeNexus

Modern life depends on systems we rarely see. Power stations keep the lights on. Pipelines carry fuel across long distances. Chemical plants manage fast and complex reactions. Transport networks move people and goods every day.

Behind all of this sits Operational Technology (OT). These are the control systems, sensors and

safety tools that keep physical processes running safely.

For many years, these systems were built with one aim: to keep operations stable. Cyber security was not a priority. Most OT systems were isolated, used proprietary technology, and were run by engineers rather than IT teams.

That world has changed.

Industrial systems are now connected to corporate networks, cloud platforms, remote access tools and supply chains. This has improved efficiency, but it has also created a new kind of risk: cyber attacks that affect the physical world.

When this happens, the impact is very different from a typical IT breach. Instead of lost data or downtime, the result can be damaged equipment, fires, explosions, pollution or long outages.

These events are still rare. But when they happen, the consequences can be severe.

The Nature of OT Cyber Risk

OT systems operate under the laws of physics.

They are designed to keep things like pressure, temperature and flow within safe limits. If those limits are exceeded, equipment can fail, sometimes in dramatic ways. That is why safety systems are built into industrial sites.

Cyber attacks can interfere with these safeguards. Any programmable safeguard designed for an intended function, can be re-programmed to behave in an unintended way.

Attackers might change sensor readings so operators think everything is normal. They might alter controls to change how machines behave. They could disable alarms or safety shutdown systems. In some cases, they may lock operators out of the system altogether.

In many cases, small changes can have big effects. Adjusting a valve, motor speed or sensor reading can push a system outside safe limits. Once that happens, problems can spread quickly.

What matters most is this: once a system crosses a safety boundary, physics takes over. Equipment will behave according to physical forces, not human intent.



How Attacks Reach Physical Systems

Most cyber-physical incidents do not start in the control room.

They often begin with standard IT breaches. A phishing email, stolen login details, weak remote access or a third-party connection can give attackers a foothold. From there, they move through the network until they reach systems linked to industrial processes.

This pattern has been seen before.

A well-known example is the 2014 attack on a German steel mill. Reports suggest attackers entered through the corporate network using phishing. They then moved into the plant's control systems.

The disruption meant the plant could not safely shut down a blast furnace. This led to serious physical damage.

The lesson is clear: an IT issue can become a physical incident once attackers cross into OT systems.

Not all attacks are highly advanced.

In Australia, a former contractor used radio signals to control

sewage pumps, releasing waste into public areas. In Poland, a teenager reportedly used a simple device to interfere with tram systems.

These cases show that even basic weaknesses—like poor access controls or exposed systems—can lead to real-world damage.

Near Misses and Hidden Risks

Some of the most important warnings come from incidents where disaster was narrowly avoided.

The Triton malware attack in Saudi Arabia is a key example. The attackers targeted a system designed to prevent serious accidents, such as uncontrolled material release or unsafe conditions leading to fire/explosion.

A fault in the malware caused the plant to shut down before any damage occurred. No explosion happened.

But the message was clear. Attackers had reached the last line of defence.

From a risk point of view, a near



miss is still a serious warning. It may reflect strong safety design—or simple luck.

Rare Events, Severe Consequences

Confirmed cases of cyber attacks causing physical damage are still uncommon.

Over several decades, only a small number of such incidents have been publicly reported.

However, this can give a false sense of security.

Many events are never disclosed due to commercial or regulatory concerns. In addition, OT systems often lack detailed monitoring, so incidents may go undetected or misattributed as a systems malfunction.

At the same time, industrial sites deal with high energy processes and hazardous materials. If something goes wrong, losses can escalate quickly.

A single major event could cost billions, including repairs, lost production, environmental clean-up and legal claims.

The Insurance Challenge

While awareness of OT cyber risk is growing, insurance has struggled

to keep up.

Traditional policies were not designed for cyber-physical events. As a result, coverage often falls between two areas.

Property insurance usually covers physical damage, but many policies now exclude cyber-related causes.

Cyber insurance tends to focus on data breaches and IT disruption. It often excludes physical damage.

This creates a gap. If a cyber attack causes physical damage, it may not be covered by either policy.

For operators of critical infrastructure, this is a serious issue.

A single incident could lead to large losses that exceed cyber policy limits, while property insurers may reject the claim due to cyber exclusions. The risk owner pays the entire loss out of pocket.

When Cyber Stops the Physical World

Even without physical damage, cyber incidents can still have major effects.

The 2021 ransomware attack on Colonial Pipeline is a good example. The attack mainly affected IT systems, but the company shut down operations as

a precaution.

Fuel supplies were disrupted across large parts of the United States.

This and hundreds of ransomware incidents each year shows how closely digital systems are linked to physical operations.

More broadly, many manufacturers have found that IT failures can stop production entirely. In modern industry, the link between IT and OT is often economic as much as technical.

Why Insurers Find OT Risk Difficult

There are several reasons why this risk is hard to assess.

First, there is limited data. There are not many well-documented cases to analyse.

Second, every industrial site is different. Processes, equipment and safety systems vary widely, including the rigor of their engineering, making standard models difficult.

Third, this risk sits across several fields: cyber security, engineering, safety and finance. Each uses its own language and approach.

This can make it hard for insurers and operators to fully understand each other.

Closing the Gap

Addressing this issue will require closer collaboration.

One approach is to use more quantitative risk models (in this context, risk is \$\$). Instead of relying only on checklists or broad assessments, these models estimate the financial impact of specific cyber scenarios.

This helps organisations understand where to invest in security. It also helps insurers assess potential losses more clearly.

An Honest Way Forward

The truth is, this is still an evolving area.

Cyber-physical incidents are rare, and data is limited. No single group—operators, insurers or security experts—has all the answers.

What is clear is that cyber risk is no longer just digital. As systems become more connected, attacks will increasingly affect the physical world.

Dealing with this challenge will require engineers, cyber specialists, insurers and policymakers to work more closely together.

The aim is not only to prevent attacks, but also to understand and manage the financial impact when they happen.



Only by bridging the gap between cyber security, engineering and insurance can critical infrastructure remain resilient in a connected world.

DeNexus has combed through 40 years of cybersecurity incidents and have discovered only ~8 that have led to physical property damage due to malicious actors (e.g., Stuxnet). Consider there are thousands facilities globally and hundreds of ransomware driven

incidents annually, but on a tiny fraction in 40 years have actually gone beyond downtime, to incur physical damage (e.g., equipment damage, explosion, fire, flooding). Meanwhile, property insurance policies exclude damage triggered by cyber events, and cyber insurance policies exclude property damage. There is a gap where cyber-induced physical damage is not a covered peril for the majority of industry.

New 2026 'IOCTA' highlights sophisticated tactics and emerging challenges in the digital landscape

Europol has published the new edition of the Internet Organised Crime Threat Assessment (IOCTA) 2026, providing an in-depth analysis of the latest trends and developments in cybercrime affecting the European Union. The report, titled "How encryption, proxies, and AI are expanding cybercrime," underscores the accelerating pace and sophistication of cyber threats, emphasising the need for enhanced law enforcement capabilities and international cooperation.

The report offers a comprehensive overview of the key developments in cybercrime, online fraud, cyber-attacks, and online child sexual exploitation, along with actionable insights for law enforcement agencies and stakeholders.

The IOCTA 2026 underscores the dynamic and interconnected nature of cybercrime, highlighting how criminals continue to exploit technological advancements to perpetrate a wide range of illicit activities. The report reveals that the dark web remains a

critical enabler for cybercriminals, with marketplaces and forums demonstrating remarkable resilience despite ongoing law enforcement efforts. The fragmentation and specialisation of these platforms pose significant challenges for investigators, as criminals rapidly adapt and migrate to new, often more secure, environments. End-to-end encrypted (E2EE) platforms and anonymised services now connect the realms of surface and dark web communication channels, increasingly blurring their distinction.

Interdependencies - The hidden links between heat, water, and energy



Extreme heat exposes the deep interdependence between water and energy systems while revealing the limits of traditional sector-based risk management.

Heatwaves place sustained pressure on multiple systems simultaneously, creating cascading stresses that extend far beyond temperature impacts alone.

Rising pressure on water and energy systems

During prolonged heat events, electricity demand rises sharply as cooling needs increase across households, businesses and critical infrastructure. At the same time, power generation capacity often becomes constrained. Higher water temperatures, declining river flows and reduced thermal efficiency limit the ability of many power plants to operate at full capacity.

Water systems also come under growing pressure from increased household and agricultural demand, higher evaporative losses and expanding industrial cooling requirements. Because these stresses occur simultaneously, disruptions in one system can intensify

vulnerabilities in another, amplifying instability during extreme heat events.

Cooling constraints and energy insecurity

The risks to water and energy systems become particularly acute during compound heat and drought events. Thermoelectric power plants require large volumes of cool water to operate safely and efficiently, yet both water availability and cooling efficiency decline during periods of extreme heat. In some regions, environmental regulations restrict water withdrawals during drought conditions, constraining electricity generation precisely when cooling demand is highest.

This creates a critical paradox: water scarcity can restrict energy supply at the very moment when societies depend most heavily on electricity to cope with dangerous heat.

Cascading impacts across the food-energy-water nexus

These cascading dynamics are shaped not only by exposure to high temperatures, but also by how sectors respond to heat risks

and how those responses interact across the food-energy-water nexus. Agricultural adaptation strategies, for example, often rely on expanded irrigation to offset heat stress on crops. While this may help protect yields in the short term, it can also increase water withdrawals and electricity demand for pumping and distribution.

Meanwhile, energy systems operating under peak demand may implement load management or curtailment measures to stabilize the grid, disrupting water treatment systems, irrigation infrastructure and temperature-sensitive supply chains.

Governance trade-offs and maladaptation risks

These dynamics vary significantly across regions, governance systems and sectoral prioritization frameworks. In many countries, domestic water use is prioritised during extreme conditions while irrigation withdrawals are restricted, creating difficult trade-offs across food production, energy generation and water security.

Despite growing recognition of compound climate risks, many heat action policies remain organised along sectoral lines, focusing on maintaining stability within individual systems rather than coordinating risk reduction across them. Without integrated planning, interventions designed to protect one system may unintentionally increase vulnerabilities in another, exposing the fragile interconnections that underpin modern infrastructure systems.

Source: United Nations Office for Disaster Risk Reduction (UNDRR)



Are you sure your national infrastructure is secure?

The rapidly evolving threat environment—driven by climate change, geopolitical conflict, supply chain disruption, and increasingly sophisticated cyber and physical attacks—demands continuous modernization of policy, regulatory frameworks, operational practices, and protective technologies to address escalating and interconnected risks.

Invitation to Participate

The current Administration recently rolled out a new critical infrastructure memorandum, titled National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22) which is intended to set forth the role of the federal government, including responsibilities for specific federal agencies, in protecting U.S. critical infrastructure.

NSM-22 serves to supplant PPD-21, formally known as the Presidential Policy Directive – Critical Infrastructure Security and Resilience (pdf). PPD-21, a memorandum issued during the previous Administration, designated 16 critical infrastructure sectors that will be subject to additional oversight through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCA).

Are you prepared?

The Nation's critical infrastructure provides the essential services that underpin American society. Proactive and coordinated efforts are necessary to strengthen and maintain secure, functioning, and resilient critical infrastructure – including assets, networks, and systems – that are vital to public confidence and the Nation's safety, prosperity, and well-being.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery.

Join us in Lake Charles, LA for the leading forum dedicated to operators and government bodies responsible for advancing Critical Infrastructure Protection and Resilience across the region.

For further details visit www.ciprna-expo.com

The premier discussion for securing America's critical infrastructure

Co-Hosted by:



- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

To discuss exhibiting and sponsorship opportunities contact:

Bruce Bassin
(Americas)
E: bruceb@torchmarketing.co.uk
T: +1 702.600.4651

Paul Gloc
(Rest of World)
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270 820

Supporting Organisations:



Help2Protect



Flagship Media Partner:



Why Critical Infrastructure Should Use Drone Vulnerability Risk Assessments Now



By Kara Quesada, Senior Director of Marketing at Echodyne and William Edwards, Director of C-UAS Training – ENSCO

Drone incursions over critical infrastructure sites are no longer hypothetical—they are operationally relevant and escalating. Unauthorized incursions over the Salem and Hope Creek Generating Systems and River Bend Nuclear Power Plant highlight the issue, with reports suggesting some drones were up to five feet in diameter and capable of flying at more than 100mph. This is well

beyond the profile of hobbyist systems.

The exposure is not limited to energy assets. The Federal Aviation Administration (FAA) now logs 100 UAS sightings per month near airports. For operators of sites such as airports, prisons, ports, utilities, data centers, oil and gas facilities, it's already clear that dealing with the emerging drone threat is an

urgent priority, but the question is how to address it in a defensible and measurable way.

Despite this, many operators delay action, waiting for regulatory clarity or standardized counter-UAS frameworks. This is a mistake. Inaction does not reduce risk; it compounds it.

Drone Vulnerability Risk Assessments (DVRAs) offer an

immediate and practical path forward for critical infrastructure site operators. They enable operators to quantify exposure, identify detection and response gaps, and elevate the drone threat from a theoretical concern to a defined operational risk that can be communicated, prioritized, and acted on at the executive level.

Why DVRA's Matter

Conducting a DVRA provides a clear operational advantage by shifting organizations from reactive response to proactive risk management. Ideally implemented during the design phase and equally valuable in retrofit environments, a DVRA enables operators to identify vulnerabilities, evaluate threat scenarios, and integrate mitigation strategies before drone activity impacts service continuity, safety, or operations. This approach allows organizations to act deliberately, rather than under pressure, ensuring that counter-UAS measures are aligned with both mission requirements and site-specific risk profiles. A DVRA allows an organization to quantify their exposure in concrete terms, creating a defensible basis for budget allocation and prioritization of high-risk sites.

The assessment also translates emerging drone threats from a technical issue understood by specialists into something that leaders can evaluate. Detection of investment should be framed as a resilience and continuity measure, moving organizations from passive awareness to defensible, risk informed action. Early investment is critical, and a DVRA enables more disciplined capital allocation,



avoiding higher costs and inefficiencies of reactive response.

What a DVRA Actually Delivers

DVRAs are not simple site walk-throughs; they provide a multi-layered analysis that translates drone-related technical challenges into actionable risk management. A DVRA evaluates the specific threat profile of a site, including likely drone capabilities, attack vectors, potential consequences, and high-impact security gaps.

This analysis enables operators to prioritize sensor placement and account for environmental factors such as radio frequency interference, ensuring detection systems are appropriately selected and deployed. Radar plays a critical role, particularly in addressing "dark drones" that cannot be detected through RF-based methods.

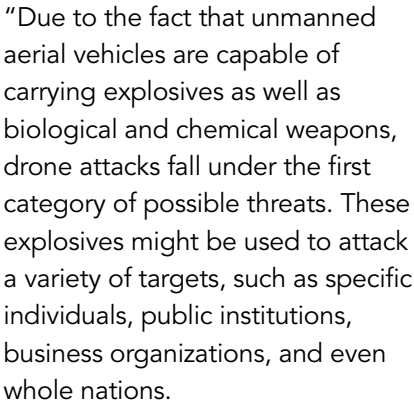
While some operators may wait for full counter-drone authorization, targeted detection remains an effective first layer of defense and supports soft mitigation strategies. A DVRA supports this approach by mapping risk across distributed assets and identifying the highest-consequence vulnerabilities requiring immediate attention.

The Scale of the Problem

The number of drones already in U.S. skies is staggering. The FAA has registered 420,825 commercial drones and 383,007 recreational drones in the U.S., ranging from hobbyist UAVs through to larger electric vertical takeoff and landing vehicles (eVTOLs). Threats range from hobbyists who may not mean to cause harm but do so accidentally (such as drones sighted over wildfires, which can cause a real threat to firefighting aircraft), through to those used for espionage and sabotage.

Drones present a unique threat to critical infrastructure. They can enter sites unnoticed, land undetected, and bypass traditional human security measures. As a result, locations once considered secure against ground-based threats are no longer assured in an era where modern drone technology has become a real and accessible risk.

Drones also pose very real threats to critical infrastructure. The scientific paper *Advances And Challenges in Drone Detection and Classification Techniques*, published by Purdue University researchers and researchers from Satbayev University, found:



Smuggling is the second-leading threat category for drone use. For border patrols and jail staff, drone drug smuggling has grown to be a serious issue. Sometimes weapons or other illegal items are smuggled beyond the reach of ground-based security. Border locations have a wide range of weather; therefore, smuggling drones need to be able to operate in adverse weather conditions.

Accidentally or purposefully
launching a remote-controlled
drone near an aircraft or in its flight

The Drone Threat Is Here Now-An Ideal Time for DVRA

The sightings of drones in New York, Pennsylvania and New Jersey spread over 17 days, and led to the FAA issuing 'special security' flight bans over parts of New York and New Jersey to protect critical infrastructure. The saturated attack had significant impacts, including preventing a medical helicopter from transporting a car crash victim due to a drone sighting near Raritan Community College.

Beyond coordinated incursions, drones are now a leading source of disruption in the aviation sector. UAS incidents have become the primary cause of non-weather-related flight delays, with 749 flights disrupted across the United

Internationally, the patterns are similar. At Sweden's Stockholm Arlanda Airport, sightings of UAS forced full suspension of air traffic for two-and-a-half hours, with fears that the incursion could be linked to heightened geopolitical tensions following Sweden's accession from NATO. In the United States the risk profile continues to expand. Recently, a United Airlines pilot reported colliding with a drone at 3,000 feet above San Diego, California. And in Nashville, a man with extremist beliefs who wanted to collapse the U.S. power grid attempted to weaponize a drone with explosives.

The Limits of Legislation

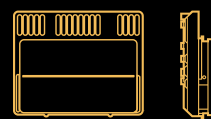
One key issue is that it's still unclear how legislation will change to allow site owners to respond to drone threats. At present, drones enjoy protected status as 'aircraft', making it a federal felony to disable, damage or destroy them, under FAA rules. The Cybersecurity and Infrastructure Security Agency's (CISA) 'Be Air Aware' guide, published late in 2025,

Improve Security Resilience with Radar

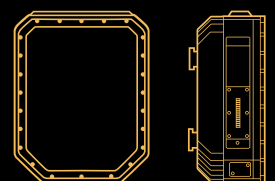
Fill security gaps and improve operational efficiency. Accurately detect and track ground and air threats, including dark drones.



EchoGuard®



EchoShield®



Radar for Critical
Infrastructure
Protection

ECHODYNE
RADAR REINVENTED™



raises awareness around the threat of drones both at infrastructure sites and at public gatherings, and highlights detection, rather than mitigation. The CISA guide advises, “If you witness a UAS operation that appears dangerous or is being used to commit a crime, report it immediately to local law enforcement first responders.”

The SAFER Skies Act, enacted as part of the FY2026 National Defense Authorization Act in December 2025, expands U.S. counter-drone authority by allowing qualified state, local, tribal, and territorial agencies- not just federal agencies - to detect, track, identify, and mitigate drones that pose credible threats to people at major public events, and critical infrastructure including correctional facilities. It also establishes federal training, certification, approved technology standards, reporting requirements, and funding pathways to help local agencies respond more quickly and lawfully to growing drone risks.

With infrastructure operators still constrained by regulatory and legal limitations, many continue to delay

investment in drone detection capabilities.

Reactive Spending After an Incident Costs More

Investing in drone defense early—through a DVRA and a structured approach to threat mitigation—is often the most cost-effective long-term strategy. Reactive spending after an incident is typically more expensive, particularly when factoring in the direct and indirect costs of operational disruption.

The 2018 Gatwick Airport incident provides a clear example. Reports of drone activity led to a full airport shutdown, with estimated economic losses of £50 million. Emergency response measures added further cost, including the rapid deployment of military-grade tracking equipment. In the aftermath, Gatwick implemented counter-drone technology at an estimated cost of £4 million.

While the post-incident investment was necessary, the scale of disruption and financial impact underscores the value of earlier, proactive measures.

Making the Final Case Against Waiting

Critical infrastructure security can no longer stop at the fence line. It must extend into the low-altitude airspace above the site, where commercially available drones can create real consequences for operations, safety, continuity, and sensitive data.

Conflicts in Ukraine, the Middle East, and other contested environments have demonstrated how inexpensive, commercially available, and rapidly modified drones can produce outsized effects. Those tactics will not remain confined to conflict zones. They are already informing criminal activity, extremist planning, and unauthorized incursions near sensitive facilities.

For infrastructure operators, the case for waiting is collapsing. Regulatory uncertainty may limit mitigation options today, but it does not prevent organizations from understanding their exposure, deploying detection, and building a defensible response plan.

A DVRA is the practical first step. It gives operators a clear view of their vulnerabilities, their highest-consequence gaps, and the investments needed to reduce risk before an incident forces action under pressure.

This ties back much more cleanly to the introduction: drone threats are urgent; waiting is not a strategy, and DVRAs are the most practical path forward now.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

Help2Protect.info
Protect your company from Insider Threats

In Collaboration
with:



See below for
20% Off Special
Offer

THREE TYPES OF INSIDERS - ONE TOOL TO DETECT THEM

Insiders may be involuntarily helping by not being sufficiently aware and trained about the potential impact of their actions, or they may be negligent. Only a small proportion of Insiders are malicious and have the intentional aim to damage the organisation. The Help2Protect program covers all 3 categories of Insiders: accidental, negligent and malicious. It also includes all types of crimes, including theft, espionage, sabotage, violent activism and organised crime, including terrorism.

BE PROACTIVE AWARENESS TRAINING



How to help to protect you, your
organisation and your colleagues.

BE READY PROGRAM DEVELOPMENT TRAINING



How do you develop an effective Insider
Threat Program for your organisation

An eLearning Platform dedicated
to Security and the Insider Threat

www.help2protect.info

SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE

IACIPP are offering you a 20% discount off this Insider Threat Detection and Prevention online course.

Register at: www.cip-association.org/help2protect - Promo Code: 7UATQW7M



Critical Infrastructure Protection & Resilience North America

10th–12th March 2026

Baton Rouge, Louisiana

www.ciprna-expo.com

Co-Hosted & Supported by::



The Critical Infrastructure Protection and Resilience North America (CIPRNA) conference and exhibition took place in the beautiful city of Baton Rouge, Louisiana, between the 10th and 12th March 2026.

This was the 8th CIPRNA event in the United States, our 4th visit to Louisiana and the 2nd time we have been hosted in Baton Rouge.

The conference had a very patriotic start with members of the Louisiana State Police Honour Guard presenting the American flag to the audience whilst the national anthem was played. This led us into our Keynote Session where senior leaders from both State Government, State Police and Industry security professionals delivered a compelling deep dive into the pressing challenges facing today's critical infrastructure sectors. Their insights set the tone for a day focused on collaboration, resilience, and forward thinking solutions.

The event consistently underscored the importance of communication, collaboration, and cooperation. Speakers frequently highlighted local, state, and national efforts aimed at strengthening relationships and building trust to support more effective coordination. Several strong examples of statewide initiatives were showcased—most notably InfraGard—which were presented as models

of best practice. This emphasis on unity was captured particularly well by Colonel Robert Hodges of the Louisiana State Police, who remarked that everyone was working toward “one team - one dream - one Louisiana.”

Over the course of the event, it became increasingly clear that not all were completely satisfied with the current connectivity between certain government agencies and the private sector. There were numerous references to what was perceived as a reduction in the interaction between such agencies and the private sector. Numerous speakers referenced what they observed as a decline in meaningful engagement, noting a noticeable drop in the amount of relevant information being shared. As one delegate put it, we now find ourselves in a situation where information seems to flow in only one direction — “it streams up but only trickles down.”

It was unfortunate that several key speakers from the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Emergency Management Agency (FEMA) were unavailable due to current funding challenges. Ultimately, the political and congressional factors behind the situation were way outside of our control.

The plenary session following the keynotes cantered on National and Regional Emergency Management Preparedness. With an impressive lineup of speakers representing a wide range of expertise, the session fully lived up to expectations. Real world examples drawn from highly challenging situations were woven together with theoretical perspectives, creating a compelling and balanced discussion.

A particularly powerful moment came during the presentation “The Challenges of Critical Infrastructure Protection: Lessons from Ukraine.” Oleksandr Sukhodolia delivered a striking account of the immense difficulties faced during a period of intense conflict. He outlined a broad spectrum of issues, focusing especially on the continual need to reengineer responses to the relentless waves of drone attacks targeting Ukraine's infrastructure. He concluded by posing a thought provoking question

to the audience: Do you believe you are prepared to face such a scenario?

The session generated considerable debate and prompted thoughtful reflection among attendees.

After such an intense and engaging session, everyone was ready to unwind. Delegates made their way to the Networking Reception, where they enjoyed refreshments and took the opportunity to connect with colleagues and explore the wide range of exhibitors.

Day 2 marked the start of our twin track sessions, offering a wide range of topics for attendees to explore. One of the most well attended discussions focused on Emerging Threats, featuring representatives from the Federal Bureau of Investigation (FBI), the state's Office of Homeland Security and Emergency Preparedness, as well as experts from the private sector. As expected, cybersecurity dominated both the presentations and the subsequent Q&A, reflecting its growing importance across all areas of security and preparedness.

Interestingly, there was little discussion about the growing concerns surrounding Insider Threats, and only limited reference to ongoing terrorism challenges. Terrorist incidents were addressed more fully in other sessions,

which felt particularly relevant in light of the New Year's Day attack in New Orleans.

Day 2 also included a series of infrastructure focused symposiums covering key sectors such as Communications, Transport, Power and Energy, and Maritime, Ports & Pipelines. As expected, a wide range of issues surfaced across these sessions, with several strong examples of preparedness and resilience highlighted by the presenters.

Information sharing remained a recurring point of debate, alongside the familiar executive level message heard in some sectors: the expectation to "do more with less." The term security exhaustion was used to describe the growing strain this dynamic places on infrastructure organisations as they work to meet expanding demands with limited resources.

The final morning of the conference continued with the twin track format, moving into sessions on Strategic Resilience Planning, Technologies to Detect and Protect, and Secure by Design. A particularly engaging discussion focused on Drones and Unmanned Aerial Systems (UAS), highlighting both their effective operational use and the growing range of technologies available to detect and counter criminal activity involving these systems.



One standout presentation came from Sheriff Joseph P. Lopinto III of Jefferson Parish, who demonstrated how law enforcement agencies are expanding their proactive use of drones across multiple areas of policing. We also heard from George Ray, whose leadership has positioned Louisiana as the most advanced state in the U.S. in the field of Unmanned Vehicle Systems.

The final session of the event returned to the theme that had resonated throughout the three days: Collaboration, Information Sharing, and Strengthening Public-Private Partnerships. It proved to be an ideal topic on which to conclude the conference. A diverse range of presentations explored the subject from multiple angles. The U.S. Treasury Department offered an international perspective, while InfraGard provided a statewide view of current and future initiatives, clearly demonstrating the ongoing efforts across both public and private sectors to build trust and deepen cooperation.

Similar messages came from the City of Henderson and the Parish of St. Charles, each placing particular emphasis

on community connectivity. The National Weather Service added further insight by outlining how it supports both public and private organisations through its outreach and communication strategies.

Interest in this session was so strong that the conference ran slightly over time, leaving me—as Conference Chair—to deliver a shortened version of my closing remarks, much to the audience's relief. I did, however, have the opportunity to thank our many presenters, exhibitors, sponsors, and, most importantly, our attendees for their active engagement throughout the three days.

Our next CIPRNA Conference and Exhibition will take place in Lake Charles Louisiana between the 16th and 18th March 2027 and our European event, CIPRE will be in Brussels in October this year.

John Donlon QPM FSI
CIPRE Conference Chair

Global Cybersecurity Partner:



Supporting Organisations:





Detection vs. Deterrence: What Actually Stops Intruders



By Jonathan Ratledge, Strategic Account Director, Critical Infrastructure & Government, AMAROK

Across critical infrastructure sectors such as energy, transportation, water, utilities, and other facilities, physical security threats are increasing in frequency and complexity. Assets are more distributed, sites are often remote or unstaffed, and essential operations cannot afford disruptions. Meanwhile, many organizations continue to rely

on security frameworks focused primarily on detection rather than prevention.

The common approach is familiar: detect an intrusion, verify the threat, and initiate a response. Cameras, alarms, analytics, and monitoring centers form the backbone of this model, providing visibility into events as they unfold. In many cases, these systems are

well-integrated and operationally necessary. However, detection-led security is inherently reactive. It assumes an intrusion attempt will occur and focuses on managing the outcome rather than reducing the likelihood of the event. In environments where response times vary and sites span large geographic areas, even rapid detection is unlikely to prevent loss, damage, or disruption.



This raises a broader strategic question for global infrastructure leaders: Is it enough to recognize when a breach occurs, or should the primary goal be preventing the attempt altogether?

The Structural Imbalance Between Detection and Deterrence

Detection and deterrence are not competing concepts, but in practice, they are often treated disproportionately. As industry threats evolve and expectations for resilience rise, that imbalance is becoming harder to ignore.

Most physical security strategies are built around detection. According to the Physical Security Market 2025-2030 report, video surveillance systems dominated the global market, accounting for more than 50.5% (Grand View Research). This includes systems that detect activity once it has begun and trigger a response, such as cameras, motion sensors, alarms, and monitoring centers — tools that provide visibility into events as they occur.

- Detection systems answer necessary questions: What is happening? What happened? What response is required? They provide situational awareness to support incident verification and create a record for investigation, compliance, insurance, or operational review. In well-designed environments, they can be integrated into response protocols that guide how teams react once a threat is identified.
- Deterrence systems, by contrast, focus on influencing behavior before an intrusion attempt occurs. These include visible barriers, controlled access points, lighting, active perimeter security, signage, and environmental design that signal a higher level of risk, effort, and consequence to potential intruders.

The critical infrastructure industry continues to prioritize detection over deterrence. The global video surveillance market is projected to grow from \$95.1 billion (USD) in 2026 to 261.65 billion (USD) by 2034 (Fortune Business Insights).

The issue is not that detection is unnecessary. It is that a detection-first approach can create a security gap when visibility and response are emphasized more heavily than perimeter-based prevention strategies.

The Reality of Infrastructure Intrusions

To develop effective security strategies, it is necessary to understand how most violations take place in practice. While high-profile incidents may be sophisticated or targeted, most security breaches across critical infrastructure are less complex.

Many crimes are opportunistic, driven by theft, vandalism, trespassing, or easy access rather than coordinated attacks. The continued rise in material theft, such as copper, components, and equipment, reflects this pattern. These incidents typically occur where assets are visible, access is predictable, and resistance is low. In this context, intruders tend to follow a straightforward logic: they weigh effort against reward and choose the path of least resistance. Therefore, sites with inconsistent perimeter control, limited deterrents, or predictable operating patterns are more likely to be targeted.

For infrastructure operators, the consequences often extend far beyond the value of the stolen material or damaged asset. A single intrusion can create emergency repairs, downtime, safety concerns, crew diversion, insurance involvement, regulatory scrutiny, and operational disruption. For electric utilities, water providers, transportation operators, and other critical

infrastructure organizations, the incident itself is often only the beginning of the cost.

When applied to security design, systems that primarily detect activity after entry can still leave infrastructure exposed. When the environment signals low resistance, the likelihood of an attempt remains high — even if detection capabilities are strong.

Where Detection-First Systems Fall Short

Detection systems identify events effectively, but once someone initiates an intrusion that triggers the system, the damage may already be done, and an unavoidable gap remains. Because these systems depend heavily on post-alarm intervention, monitoring teams — even those with AI — must assess alerts, filter out false alarms, and determine the appropriate response. In the United States alone, 94-98% of police alarm calls are false alarms, costing the public about \$1.5 billion per year in police time (U.S. Department of Justice). Over time, delayed escalation or false calls can lead to a lack of response, especially in highly distributed areas.

The operational and financial impacts extend beyond the incident itself. A single breach can cause downtime, safety issues, and regulatory scrutiny, diverting resources and straining teams. From a financial perspective, downstream expenses such as replacements, insurance, and productivity losses tend to rapidly surpass prevention costs.

For many infrastructure sites, the issue is not whether detection works. The issue is whether detection happens early enough,



and whether the response can arrive quickly enough, to prevent meaningful loss or damage.

How Deterrence Influences Behavior

A prevention-focused approach shifts the point at which security is activated. It moves the risk outward to the perimeter, where decisions are made and potential threats can be deterred from escalating.

At its core, deterrence operates on perception. Visible security measures create clearly defined boundaries and alter how a potential intruder evaluates risk versus reward. When effort increases and uncertainty rises, the likelihood of an attempt decreases. Essentially, security begins as a psychological barrier before any physical action is taken; it begins in the decision-making process. This premise also aligns with principles in criminology. Individuals seeking opportunity tend to favor environments with lower resistance and higher predictability. When those conditions change, behavior changes with them. In most cases, the outcome is not confrontation

but displacement; intruders will move on to less-protected sites.

For critical infrastructure, many assets are located in remote or minimally staffed environments where response times are inherently constrained. In these settings, visible deterrence and clear boundary enforcement must be foundational measures. Physical barriers and well-defined perimeters heighten avoidance instincts and reinforce a simple message: access is controlled, and intrusion carries consequences. When security is designed with human behavior in mind, it reduces the likelihood that unlawful activity progresses in the first place.

The Case for a Layered Security Approach

Detection and deterrence should work together, not compete; relying on only one creates gaps. A more effective approach is organized, multi-layered, and aligned with how intrusions occur and how human behavior responds.

This model organizes security into three functional layers at critical infrastructure sites:



- **Outer layer: Deter.** Establish visible boundaries through barriers, active perimeter deterrence, lighting, signage, and controlled access gates to discourage intrusion attempts before they begin.
- **Middle layer: Delay.** Introduce intrusion sensors, lighting, audible alerts, secondary barriers, and other physical obstacles that slow or complicate movement, increasing the time and effort required to proceed.
- **Inner layer: Detect and Respond.** Use cameras and real-time monitoring systems to identify activity and initiate an appropriate response in the event of a confirmed breach.

In this framework, detection remains essential, but it is no longer the first or only line of defense. Its role is to reinforce a system designed to prevent intrusion, not simply manage it after the fact. For infrastructure operators, the objective is to align these layers with asset value, operational scale, and acceptable risk levels. A well-designed

multi-layer approach minimizes perimeter exposure while enhancing response effectiveness and supporting continuity across critical systems.

Operational Considerations for Infrastructure Leaders

For industry leaders, the shift from detection toward layered deterrence is strategic. It requires moving from a reactive posture to proactive risk mitigation, with the objective of reducing exposure before incidents happen. This shift also changes how security effectiveness is evaluated. The focus moves beyond response capability to include prevention, visibility, and resilience across the entire operating environment.

A few questions can help assess whether your current strategies are aligned:

- Are we primarily reacting to incidents, or preventing them?
- How visible and defined is our security posture at the perimeter?
- Would a potential intruder view this site as difficult, risky, and time-consuming to enter?

How does our anticipated response time compare to the speed of a typical intrusion?

Are cameras and alarms being used as part of a layered strategy, or are they carrying most of the burden?

What is the full cost of an incident beyond replacement material or repair expense?

- Can the current model scale across distributed assets without creating unnecessary operational complexity?

At the same time, practical constraints remain. Security decisions must balance cost, coverage across distributed assets, and the ability to maintain and scale systems over time. The most effective strategies integrate these considerations without introducing unnecessary complexity or operational burden.

Selecting a partner that can manage all aspects of compliance, risk management, and connectivity for multi-site operations within a layered security strategy can reduce the need to juggle multiple vendors.

The Evolving Threat Landscape and Industry Expectations

The responsibilities assigned to critical infrastructure operators are expanding. Security is no longer evaluated solely on the ability to detect and report incidents, but on the ability to maintain continuity under increasing pressure. Regulatory scrutiny is intensifying, public safety expectations are rising, and insurance and liability considerations are becoming more closely tied to how risk is managed — not just how it is documented.

In response, there is a broader shift toward proactive risk mitigation. Resilience frameworks emphasize reducing exposure and ensuring operational stability rather than relying solely on post-incident reporting. Therefore, a perimeter-first, layered approach is a strategic foundation for addressing risk at the boundary, reducing the likelihood of intrusion, and limiting the need for downstream response. This shift also reflects a closer integration between physical security and operational resilience. Protection strategies are no longer isolated functions; they are part of a connected effort to safeguard uptime, reliability, public safety, and trust across critical systems.

As these expectations evolve, so must the standard for what constitutes effective security. Monitoring alone cannot secure critical infrastructure. The outdated sequence of detect, verify, and respond is no longer sufficient on its own. A more comprehensive model prioritizes deterrence and

delay immediately, with detection and response as needed. As a result, success depends not only on how incidents are handled, but more importantly, on how often they can be avoided entirely.

Redefining Effective Security in CIP

Detection answers an important question: "What happened?" Yet deterrence addresses a more consequential one: "How do we reduce the likelihood that it happens in the first place?"

The most effective security strategies recognize this distinction. They prioritize preventing incidents where possible, while maintaining the ability to detect, verify, and respond when necessary. For infrastructure leaders, this requires a shift in how success is defined.

Success should not be measured only by how efficiently incidents are managed after they occur. It should also be measured by how effectively a security posture

discourages attempts, delays escalation, reduces preventable losses, and supports operational continuity.

Detection will always matter. But detection alone is not prevention.

As threats evolve and expectations for resilience increase, the strongest critical infrastructure security strategies will be those that move risk outward, strengthen the perimeter, and combine deterrence, delay, detection, and response into a coordinated model designed to prevent more incidents from happening in the first place.

Jonathan Ratledge leads AMAROK's Critical Infrastructure and Government strategy, helping utilities, public agencies, and infrastructure operators strengthen perimeter security across high-value sites.

Locked Shields 2026 united the power of 41 nations to defend cyberspace

The world's largest live-fire cyber defence exercise Locked Shields 2026, organised by NATO Cooperative Cyber Defence Centre of Excellence, concluded on Friday, 24 April. The exercise brought together over 4,000 participants from 41 nations to practise protecting critical infrastructure and military systems against real-time cyberattacks.

"At Locked Shields, the teams must put their skills to the test, protecting the IT systems that keep our everyday life running—including critical infrastructure, air defence and e-voting. The teams demonstrated strong capabilities in detecting

and responding to malicious cyber activities. The key now is to take the lessons identified from the exercise and translate them into real-world readiness, particularly as AI capabilities continue to transform both the defence and attack sides of the cyber domain," said Tõnis Saar, Director of the NATO Cooperative Cyber Defence Centre of Excellence.

"Our ultimate goal at Locked Shields is to enhance collaboration between nations, and build trust and a shared understanding of how to strengthen resilience in cyberspace," said Dan Ungureanu, Exercise Director of Locked Shields 2026. "I thank all

participants, organisers, and partners – nearly 5,000 people worldwide – for contributing to this shared goal."

"As cyber threats continue to grow in complexity and scale, exercises like Locked Shields play an important role in helping us stay prepared. This year's focus on crisis management and the protection of critical systems reflects the kind of challenges we increasingly face in reality. Estonia is proud to host this exercise and to bring together experts from across the Alliance," concluded Estonian Minister of Defence Hanno Pevkur.

Algorithmic Amplification Is Now a Critical Infrastructure Risk



Critical infrastructure incidents no longer unfold only across physical assets and cyber systems. They also unfold in an infospace shaped by digital platforms whose algorithms favour speed, emotional intensity, and visibility over verification. For operators, this means that rumour, distortion, and misleading narratives can become part of the incident environment before the first official statement is issued. That is no longer just



Antonio Scala, Research Director at CNR-ISC

a communications issue. It is a resilience issue.

The problem is not limited to deliberate disinformation campaigns by hostile actors. A significant part of the risk arises from the normal operation of large social media platforms. During an outage, transport failure, communications disruption, or industrial accident, there is almost always an early information

vacuum. Official facts are incomplete, technical assessments are still underway, and restoration timelines remain uncertain. Into that gap flows the content platforms are most likely to amplify. In practice, that often means the most dramatic, emotionally charged, or speculative interpretation of events.

The consequences are operational, not merely reputational.

First, algorithmically amplified misinformation can distort public behaviour. False or exaggerated claims about the scale of an incident, the existence of secondary hazards, or the reliability of official updates can influence how people respond in real time. In an infrastructure emergency, resilience depends partly on public cooperation: passengers need clear guidance, consumers may need to reduce demand, and affected communities need to know which channels to trust. Confusion in the information environment weakens that cooperation.

Second, it can place additional strain on response systems. When misleading narratives spread quickly, emergency services, customer contact centres, and public authorities may face surges of enquiries, complaints, or panic-driven reactions that do not correspond to the technical reality of the event. This diverts attention and capacity at precisely the moment when disciplined prioritisation matters most.

Third, it can damage trust in ways that outlast the incident itself. Even where restoration is technically successful, the dominant online narrative may frame the event as evidence of incompetence, secrecy, or negligence. Once that

framing becomes established, later incidents become harder to manage because the baseline level of trust has already been weakened.

For this reason, critical infrastructure operators should stop treating the infospace as a downstream issue to be handled only after the technical response is underway. In the platform age, the narrative environment develops in parallel with the operational incident, and often faster than formal communication processes can respond. The information dimension therefore needs to be built into resilience planning in advance.

Three practical steps would make a real difference.

The first is to treat narrative monitoring as part of situational awareness during significant incidents. Operators already monitor technical status, cyber indicators, and service impacts. They should also have a structured way to assess what claims are circulating online, which narratives are gaining traction, and whether those narratives are affecting behaviour. While this is established practice in advanced crisis communication teams, it remains rare in CIP incident management structures — and that gap needs to close.

The second is to invest in trusted communication channels and pre-prepared messaging frameworks before a crisis occurs. Credibility cannot be improvised in the middle of a major outage. Organisations that have already established visible, consistent, and recognisable public channels — whether through direct social

media presence, relationships with local authorities, or pre-agreed communication protocols with emergency services — are in a much stronger position to reach the public quickly with accurate information when it matters. Equally important is preparing draft holding lines and narrative frameworks for the most foreseeable incident types: a grid outage, a transport disruption, a communications failure. When the information vacuum opens, the difference between responding in minutes and responding in hours is often the difference between shaping the narrative and chasing it.

The third is to update crisis training and exercises. Tabletop exercises should not simulate only the technical disruption. They should also simulate the platform dynamics surrounding it: rumour cascades, miscaptioned images, false attributions of cause, and competing unofficial narratives. That is now part of the real operating environment, and preparedness should reflect it.

Critical infrastructure protection has always required attention to the wider conditions that shape disruption. Today, one of those conditions is the infospace. Algorithmic amplification is not an abstract media issue or a secondary public relations concern. It is part of the environment in which incidents are interpreted, escalated, and managed. Resilience planning should reflect that reality.

Antonio Scala is a physicist and Research Director at CNR-ISC. His research focuses on complex networks, information dynamics, and critical infrastructure resilience.

Link11 Identifies Five Cybersecurity Trends Set to Shape European Defense Strategies in 2026

When the Morrill Fire ignited on March 12, 2026, it quickly grew into the largest wildfire in Nebraska history. As the fire rapidly burned across the state, NOAA's Next Generation Fire System (NGFS) provided the critical eye-in-the-sky perspective for the massive response to the record-breaking fire.

The up-to-the-minute guidance from the NGFS provided essential information for Watch Duty, a non-profit organization dedicated to providing real-time, human-validated wildfire information to the public and first responders.

"For our team, NOAA's NGFS serves as a critical early-warning tool, particularly for initial detections in rural areas," said Liam Winstead, the manager of operational intelligence and mapping at Watch Duty. "In many cases, NGFS is our first—and sometimes only—signal that a fire has ignited, often alerting us before firefighters are dispatched."

NOAA's NGFS is an experimental online tool that pairs NOAA's Geostationary Operational Environmental Satellite (GOES) data with AI-enhanced algorithms to automatically detect near-real time information about active wildfires, such as new ignitions and fire intensity.

"Geostationary satellites are constant sentinels," said Mike Pavolonis, NGFS developer and wildland fire program manager at NOAA's Satellite and Information Service. "They enable detection of fires within 5 to 30 minutes of ignition. The NGFS is a force-multiplier that helps human decision-makers sift through enormous volumes of satellite imagery."

In January 2026, the science team



behind the NGFS announced the debut of the Wildland Fire Data Portal, which now provides responders with more robust access to NGFS information. One indispensable feature of the Data Portal is how it provides Watch Duty the ability to pan back and forth through time to visualize how quickly wildfires are evolving.

"The Morrill Fire is a perfect example of how NOAA's Wildland Fire Data Portal is a game changer for public safety," Winstead said. "On March 12, the NGFS detection came in around 1:40 pm MT. At that stage, we did not have eyes on the ground or radio traffic to monitor. Within 10 minutes, additional NGFS detections showed the heat spreading rapidly in alignment with the wind, providing the confirmation that this was a fast-moving vegetation fire. We posted the incident and alerted the county just 13 minutes after the initial detection."

One challenge for responders and firefighters was how quickly the Morrill Fire spread due to low humidity and high winds. Red Flag Warnings, which mean that critical fire weather conditions are either occurring or are imminent, were in effect for much of the state when the fire ignited. By 9:00 pm that day,

the fire had traveled more than 65 miles across Nebraska.

When fires quickly engulf the landscape, fire analysts with the U.S. Forest Service and other agencies use the satellite heat detections from the NGFS to estimate the extent of those fast-moving wildfires. Typically, a fire's perimeter is mapped using a combination of satellite data, aerial imaging, and ground-based GPS tracking, but those methods may not be promptly available for all fires, especially wind driven wildfires in the Plains like the Morrill Fire.

Later that evening, when the winds shifted, NGFS detections showed the southern edge of the Morrill Fire flaring up and advancing toward populated areas of the state. With that information, responders were able to communicate to partners exactly where the fire was moving in near real-time.

Nearly two weeks after it ignited, the National Interagency Fire Center declared the Morrill Fire 100% contained on the evening of March 24, though engine crews stayed alert for scattered flare-ups within the burn scar. The total area burned was 642,029 acres – almost equal to the land area of Rhode Island.

With a massive, fast-moving fire like this, NOAA's NGFS provided both a big-picture view and the finer details crucial to monitoring and responding to this historic blaze.

"Having minute-by-minute access to wildfire data is critical during an active fire," Pavolonis emphasized. "The NGFS provides the situational awareness that wildfire response teams need to protect lives and property, and the Wildland Fire Data Portal ensures quick and consistent access to this information."

Join the Community and help make a difference

Dear CIP professional

I would like to invite you to join the International Association of Critical Infrastructure Protection Professionals, a body that seeks to encourage the exchange of information and promote collaborative working internationally.

As an Association we aim to deliver discussion and innovation – on many of the serious Infrastructure - Protection - Management and Security Issue challenges - facing both Industry and Governments.

A great website that offers a **Members Portal** for information sharing, connectivity with like-minded professionals, useful information and discussions forums, with more being developed.

The ever changing and evolving nature of threats, whether natural through climate change or man made through terrorism activities, either physical or cyber, means there is a continual need to review and update policies, practices and technologies to meet these growing and changing demands.

Membership is open to qualifying individuals - see www.cip-association.org for more details.

Our overall objectives are:

- To develop a wider understanding of the challenges facing both industry and governments
- To facilitate the exchange of appropriate infrastructure & information related information and to maximise networking opportunities
- To promote good practice and innovation
- To facilitate access to experts within the fields of both Infrastructure and Information protection and resilience
- To create a centre of excellence, promoting close co-operation with key international partners
- To extend our reach globally to develop wider membership that reflects the needs of all member countries and organisations

For further details and to join, visit www.cip-association.org and help shape the future of this increasingly critical sector of national security.

We look forward to welcoming you.



John Donlon QPM, FSI
Chairman
IACIPP



The Unblinking Eye: Advancing Critical Infrastructure Security through GDPR Friendly Iris Recognition



Seyit Ali Kaya, Regional Manager for Iris ID systems, Inc.

Critical infrastructures are high-value targets. The “insider threat”—whether malicious or negligent—remains one of the most difficult vectors to mitigate. Traditional access control mechanisms, such as proximity cards (RFID/NFC) or PIN codes, rely on possession or knowledge. These systems verify the credential of something you know, or you

have, not the carrier-real person. A lost keycard can be found and used by an adversary; a PIN can be shared or observed. In a nuclear facility or a bio- containment lab, the ambiguity of “who holds the card” is an unacceptable risk.

True identity authentication requires a shift to inherence—verifying True identity

authentication requires a shift to inherence—verifying who the person is. This is where biometrics bridge the security gap. By binding access rights to immutable physiological characteristics, security administrators ensure that only authorized personnel can enter sensitive zones, creating an irrefutable audit trail of physical movement.

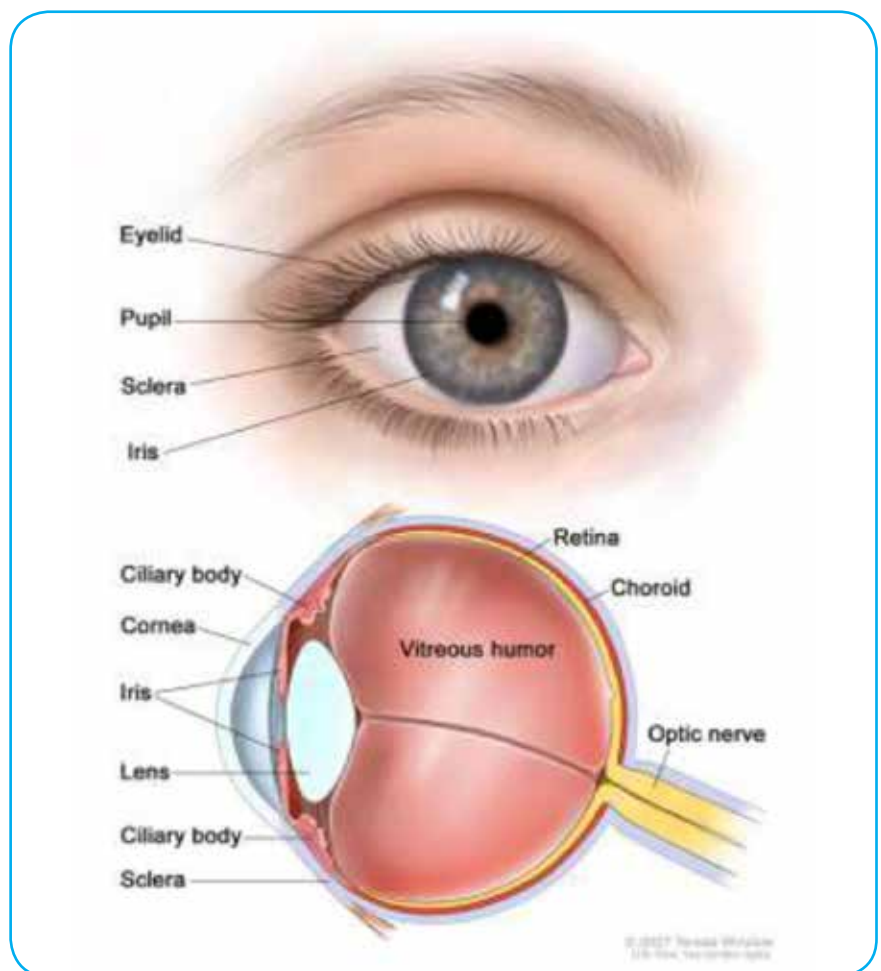
The Biometric Hierarchy: Why Iris Recognition Prevails

While fingerprints and facial recognition have seen widespread commercial adoption, critical infrastructure demands a higher standard of precision and reliability. Fingerprints can be worn down by manual labor or obscured by grease and dirt—common conditions in industrial CI environments. Facial recognition, while convenient, can struggle with lighting variations, facial hair changes, or high-security masking requirements, and is occasionally susceptible to sophisticated “presentation attacks” (spoofing).

Iris recognition addresses these limitations, positioning itself as the gold standard for high-security facilities.

1. Unmatched Entropy and Accuracy: The human iris—the colored ring around the pupil—is an internal organ protected by the cornea. Its pattern is formed by chaotic morphogenetic processes during embryonic development, resulting in a texture of extreme complexity. The mathematical probability of two irises being identical is virtually zero (even between identical twins or a person’s left and right eye). This results in the lowest False Acceptance Rate (FAR) of any biometric modality, a crucial metric when protecting dangerous or classified assets.

2. Stability and Longevity: unlike faces which age or fingerprints which scar, the iris pattern remains stable from infancy to old age. This stability reduces the administrative burden of frequent re-enrollment, a significant logistical advantage for large-



scale infrastructure operations.

3. Liveness and Anti-Spoofing: Modern iris scanners utilize near-infrared (NIR) light to capture the rich texture of the iris, which is invisible to the naked eye. Advanced systems incorporate “liveness detection” that measures the natural dilation and constriction of the pupil in response to light. This makes it exceptionally difficult to spoof using high-resolution photographs or contact lenses, ensuring that the system is interacting with a living, present human.

Operational Suitability in Critical Environments

Beyond raw security metrics, iris recognition offers operational benefits tailored to the realities

of critical infrastructure. Users do not need to touch anywhere. Iris recognition is contactless and its speed does not compromise security, having security and comfort at the same time. Also, only iris recognition can work with full personal protective equipment.

- **Contactless Hygiene:** In bio-secure environments or during health crises, the contactless nature of iris scanning is vital. Users do not need to touch a sensor, reducing the risk of pathogen transmission.

- **Speed and Throughput:** High-end iris systems function at a distance. Personnel can be authenticated less than a second even in large databases (including millions of people),



preventing bottlenecks at shift changes in large power plants or refineries.

- Integration with Personal Protective Equipment (PPE): In many critical infrastructure sectors, workers wear gloves, masks, or full protective suits. Fingerprint scanners are useless with gloves, and masks confound facial recognition. The eyes, however, are almost always visible, making iris recognition the most practical modality for industrial compliance.

GDPR Friendly Biometric Modality: Iris Recognition

Under GDPR, iris recognition is classified as biometric data used for unique identification, which makes it special category personal data (Article 9). Iris recognition supports GDPR compliance because it enables highly accurate identity verification with minimal data usage and strong protection against fraud. When implemented with privacy-by-design principles—such as on-device processing, encryption, template storage instead of raw images, template

on card match on device, and clear user consent, it helps ensure data minimization, security, and purpose limitation as required by GDPR. Its high accuracy also reduces false matches, limiting unnecessary processing of personal data and supporting lawful, fair, and transparent data handling.

- Privacy by design and by default (Art. 25): Iris templates are generated and images are processed locally on the device for template generation, no cloud or central storage are required. It minimizes data exposure and breach impact.
- Biometric Template Protection (Art. 32): Irreversible template generation. One-way transformation from the raw image and it is impossible to reconstruct the eye image. If data leaks, it cannot be reused or reverse-engineered.
- Data Minimization (Art. 5(1)(c)): No raw iris image is stored. Raw images can be discarded immediately after template creation and only mathematical feature vectors retained so

the minimum data required for identification/verification is stored.

- Purpose and Storage Limitation (Art. 5(1)(b) and (e)): Single purpose biometric use and automatic template lifecycle management is ready to use. Iris recognition can be used only for authentication-access control and cannot be re-used for analytics, surveillance, or profiling. Also, systems can be designed to prevent indefinite biometric storage. Autodeletion can be done after employee termination, contract expiration and/or inactivity threshold.
- Template on Card-Match on Device: In addition to above, users can easily bypass the regulation by writing their iris templates to a smart card which is already used in conventional access control systems. When iris image is captured and irreversible iris templates are created those templates can be written into a smart card with the GDPR's "state of the art" security requirement, AES256 or more complex encryption at rest and in transit. Personal data is only stored in the card memory neither in device nor a central database. During verification, user first tap the card to reader, and it immediately fetches the iris templates to temporary memory then asks the user to show eyes then re-create templates from the live user. At the final stage iris recognition device compares templates whether there is a match or not and memory is cleared.

Conclusion

The resilience of a critical infrastructure is defined by its

weakest entry point. As physical and digital threats converge, the reliance on distinct tokens or passwords is a liability that security directors can no longer afford.

The most GDPR-compliant biometric modality is iris and iris recognition systems are those that process biometrics locally, store only encrypted and irreversible templates, require explicit consent, offer non-biometric alternatives, and allow immediate deletion

of biometric data while users can benefit from iris recognition without sharing any data with template on card match on device mode.

The adoption of iris recognition represents a paradigm shift from probable authentication to definite authentication. By leveraging the unique, stable, and spoof-resistant nature of the human iris, critical infrastructure entities can achieve a level of physical

security that matches the gravity of their mission. In the defense of essential services, knowing exactly who is walking through the door is not just a security protocol; it is a fundamental responsibility to public safety.

CoESS and UNI Europa: EU Preparedness requires engagement with private security and strong Social Partner involvement

The Confederation of European Security Services (CoESS) and UNI Europa have adopted a joint statement on the EU Preparedness Union Strategy, highlighting the role of private security in Europe's crisis response systems. The statement underlines a clear message: without quality jobs and stable working conditions in essential services, Europe cannot ensure effective preparedness. It calls for stronger recognition of private security as part of Europe's internal security and civil protection architecture.

Private security workers protect citizens, safeguard Critical Infrastructure and support public emergency services every day, including in times of crisis. However, the statement points out that their contribution is still not fully reflected in EU policy and preparedness planning.

Europe cannot build a credible Preparedness Union while essential security functions are governed by market rules that undermine

workforce stability, service quality and ultimately Europe's security.

A central concern is the impact of lowest-price public procurement on the sector. According to CoESS and UNI Europa, current practices undermine working conditions, reduce job attractiveness and weaken service quality, contributing to labour shortages. This directly affects Europe's ability to respond to emergencies.

To address this, the statement calls for a revision of the EU Public Procurement Directive to promote quality-based awards and fair competition. It proposes that contracts should be awarded based on a balanced price-quality ratio and

only to companies that comply with labour and sectoral rules.

The EU sectoral Social Partners also stress that preparedness depends on a stable and trained workforce in normal times. Rapid mobilisation during crises is only possible if sufficient qualified personnel are available and properly trained.

In addition, CoESS and UNI Europa call for closer cooperation with sectoral Social Partners to improve career attractiveness in security services, address labour shortages and support training and skills development. They recently concluded the EU-funded project "INTEL", looking into attractive careers in security and expectations of young security workers (www.securityskills.eu).

The joint statement concludes that private security should be recognised as an essential partner in Europe's preparedness efforts, with a stronger role in policy, planning and coordination.



New report maps critical vulnerabilities in the world's interconnected systems

Are we ready for solar storms, submarine cable cuts, satellite disruptions, and extreme weather to disrupt communication networks and potentially trigger a “digital pandemic”?

A new report – “When digital systems fail: The hidden risks of our digital world” – outlines risk scenarios on Earth, at sea, and in space, analysing the fragility of interconnected digital systems and offering a roadmap for preparedness.

Experts brought together by the International Telecommunication Union (ITU), the United Nations Office for Disaster Risk Reduction (UNDRR), and Sciences Po, call for coordinated action between countries to improve digital resilience and protect essential services like healthcare, finance, and emergency response.

“Resilience must be built into the DNA of the technologies we depend on,” said Doreen Bogdan-Martin, ITU Secretary-General. “This report urges us to consider the systemic nature of risks and rethink how we protect the systems that connect and empower humanity.”

“As our societies become more reliant on digital technologies, disruptions caused by disasters can cascade across systems and borders, triggering far-reaching and potentially catastrophic failures,” said Kamal Kishore, Special Representative of the United Nations Secretary-General for Disaster Risk



Reduction and Head of UNDRR. “We must plan, build and maintain digital infrastructure with systemic risk in mind - now and for the future. Digital infrastructure must be resilient infrastructure”.

The risks of digital dependency

Digital technologies have revolutionized how we live, connect, and work, yet our growing reliance on these systems has created risks that often go unnoticed.

A severe solar storm could disable satellites, disrupt navigation systems, and destabilize energy grids, with recovery times measured in months. Extreme temperatures could overwhelm data centers, leading to mobile service outages, as well as failures in healthcare systems and financial transactions. In the meantime, earthquakes or other natural hazards can sever vital Internet connections, slowing business operations and leaving entire nations offline for weeks.

Any specific scenario may seem isolated and unlikely,

not alarming enough to prompt a timely global response. Yet digital vulnerabilities are real, and unexpected incidents are bound to happen.

The report highlights another vulnerability: societies have grown dependent on digital systems without maintaining analogue skills and ensuring adequate fallback options. When big systems fail, offline alternatives are not always available anymore.

“Facing systemic risks means looking beyond data and working across disciplines,” said Arancha González, Dean of the Paris School of International Affairs at Sciences Po. “This report shows how evidence-based policymaking can help us build resilience in an increasingly interconnected world.”

Turning knowledge into action

The report calls on policymakers, the private sector, and civil society to act now to prevent these risks from becoming a “digital pandemic”, urging for global commitment and coordinated action.

Authors suggest considering six priorities for safeguarding critical digital infrastructure:

- **Deepen knowledge:** Identify vulnerabilities, map cross-sector dependencies, develop models for potential chain reactions, and maintain analogue skills.
- **Modernize risk management:** Treat non-intentional digital disruptions as a core risk by updating legal and disaster-risk frameworks and incentives.
- **Strengthen standards and planning:** Establish robust fallback systems and conduct joint multi-sector scenario planning.
- **Improve coordination on critical risks:** Proactively coordinate on high-impact risks affecting space weather, submarine cables, satellites, and data centres.
- **Build societal resilience:** Equip communities and organizations to withstand and recover from digital disruptions by fostering adaptive capacities.
- **Foster trust and collaboration:** Build capacity, convene stakeholders, and promote shared awareness and accountability across sectors and borders.

The findings are the result of a collaborative process involving experts from 12 countries, representing national authorities, the private sector, academia and international organizations.

HSCC Unveils 3rd-Party AI Risk & Supply Chain Transparency Guide

To close that gap, the Health Sector Coordinating Council (HSCC) Cybersecurity Working Group (CWG) today published its AI Cyber Glossary. The CWG also released the “Health Industry Third-Party AI Risk and Supply Chain Transparency Guide.” The 109-page resource addresses cybersecurity risks in AI-driven supply chains.

The glossary establishes governance-ready definitions that clinical, operational, compliance, and technical stakeholders can apply with confidence. Greg Garcia, Executive Director of the HSCC CWG, noted that the resource fills a critical need. Healthcare has lacked shared, sector-specific language for AI. As a living document, the glossary will serve as the terminological foundation for all HSCC AI Task Group guidance materials.



Drawing from established frameworks such as the NIST AI Risk Management Framework (NIST AI RMF) and the joint HSCC-HHS Health Industry Cybersecurity Practices (HICP), the Guide adapts best practices to reflect the realities of AI-driven supply chains in healthcare—including data lineage tracking, model auditability, embedded third-party dependencies,

and post-deployment monitoring. It outlines critical control areas such as vendor security attestations, model explainability thresholds, and fail-safe requirements for AI-enabled clinical and operational systems. The Guide enables organizations to define accountability expectations and drive performance standards across their extended AI ecosystem.

Crucially, the Guide addresses the growing gaps in discovery and disclosure processes that make AI supply chain risk so difficult to manage. Many HCOs operate with incomplete or outdated vendor inventories, while AI-specific cybersecurity risks—such as synthetic data misuse, training data leakage, and adversarial inference—go unreported by vendors. To counter this, the Guide promotes proactive due diligence, dynamic risk profiling, and contractual transparency. It equips risk managers, compliance teams, and procurement officers with scalable tools to surface hidden dependencies, identify cascading failure points, and align third-party AI vendors and products with missioncritical safety, privacy, and resilience goals.

Updated State aid paves the way for EU Space for rail

The European Commission has introduced new State aid rules to make it easier to invest in sustainable transport across Europe. By removing the need for prior approval for certain types of funding in rail, inland waterways and multimodal transport, the new framework helps speed up deployment where it matters most.

For EUSPA, this is a welcome step forward—especially when it comes to integrating space into rail.

A key element in the new



rules is the recognition of satellite navigation in railway signaling: “As regards interoperability investments related to the European Rail Traffic Management System (ERTMS), costs related to

the integration of European Global Navigation Satellite System (EGNSS) functions within the ERTMS shall be eligible.”

This means that EGNSS-enabled functionalities within

ERTMS can more easily benefit from public funding.

The provision supports the development of a more cost-efficient, EU Space-enabled ERTMS and facilitates its wider deployment across the European rail network, including regional and secondary lines.

By reducing financial and administrative barriers, the new framework helps create favourable conditions for innovation and strengthens collaboration across the rail sector.

TIA Advances AI Ready Data Centers with New ANSI/TIA 942 Addendum, Global Certification Leadership, and Expanded Industry Quality Initiative

As artificial intelligence (AI) workloads drive unprecedented changes in data center design, performance, and operational risk, the Telecommunications Industry Association (TIA) today announced a coordinated set of actions to help the industry meet AI-era infrastructure requirements. These include the launch of a new Artificial Intelligence addendum to the ANSI/TIA-942 data center standard, continued global leadership in independent third-party data center certification, and expanding participation in TIA's new Data Center Excellence Quality Standard (DCE 9000) initiative.

Together, these efforts reflect TIA's end-to-end approach to strengthening AI-ready digital infrastructure—from defining infrastructure requirements for high-density, high-performance computing environments, to validating reliability through globally recognized certification, to improving quality and consistency across the data center supply chain. As AI accelerates data center scale, complexity, and deployment timelines, TIA's standards and certification programs are providing the industry with a common, credible framework to manage risk, improve predictability, and support resilient digital infrastructure worldwide.

Advancing ANSI/TIA-942



to Address AI Data Center Requirements

To support the next generation of AI-driven data centers, TIA Engineering Committee TR-42.1 (Premises Telecommunications Infrastructure) has initiated a project to develop Addendum 1: Artificial Intelligence to ANSI/TIA-942-C, focused on the unique infrastructure demands of AI and HPC environments.

AI workloads—characterized by dense GPU clusters, extreme bandwidth requirements, and new power and cooling models—are placing unprecedented demands on data center infrastructure. The addendum will focus on high-density, high-speed cabling for AI and HPC environments, along with cooling and electrical systems, including liquid cooling, to support reliable, scalable data center and digital infrastructure deployments.

The project is being

developed through TIA's voluntary consensus-based standards process with participation from data center owners and operators, designers, manufacturers, and other stakeholders supporting digital infrastructure. Publication of the addendum is targeted for mid-2027.

"This work reflects direct input from across the data center ecosystem," said Cindy Montstream, Chair, TIA TR-42 Engineering Committee. "By evolving ANSI/TIA-942 to address AI-specific infrastructure needs, we're aligning real-world operational experience with globally recognized standards that support scalable, reliable data center design and operation."

Global Data Center Certification Supporting Proven Infrastructure Performance

In parallel with standards development, TIA continues to support the global data center community through its ANSI/TIA-942

Certification Program, which validates facilities against the standard's infrastructure requirements and four rated levels of reliability.

To date, over 1,000 certifications in more than 800 data centers across 60+ countries have earned ANSI/TIA-942 certification, demonstrating predictable availability and resilience across diverse operating environments. As AI workloads accelerate new data center construction worldwide, certification provides operators, customers, and investors with independent validation that facilities are designed to meet defined reliability objectives critical to digital infrastructure performance.

Strengthening the Data Center Supply Chain with DCE 9000

Recognizing that reliable data center operations depend not only on facility design but also on the quality and consistency of the infrastructure supply chain, TIA launched the Data Center Excellence Quality Standard (DCE 9000) initiative. As announced on February 25, 2026, DCE 9000 is a collaborative effort to establish the first quality management system (QMS) standard purpose-built for data center physical infrastructure, supporting reliable, scalable digital infrastructure deployments worldwide.

Airbus Protect selected by EASA for EASA Higher Airspace Operations

Reinforcing the long-standing commitment to European institutional excellence, Airbus Protect, has secured a landmark tender with the European Union Aviation Safety Agency (EASA). By delivering critical expertise to shape the regulatory foundations of the EU's aeronautical future, our specialists are spearheading the integration of safety, cybersecurity, and sustainability standards to ensure the resilience of the European aviation ecosystem.

Leading a high-profile consortium alongside Deep Blue and the German Aerospace Centre (DLR), Airbus Protect will provide scientific



foundation and risk-driven insights required to regulate "Higher Airspace Operations" (HAO). This quasi-virgin territory, located above FL550, is quickly becoming a hub for next-generation technology, from slow-moving High Altitude Platform Systems (HAPS) to high-speed hypersonic aircraft. To meet this challenge, we are deploying an integrated strategy where our three

core pillars operate in total harmony.

In the realm of safety, our teams are developing specialised "Target Levels of Safety" and performing rigorous risk assessments to ensure that operation of these novel vehicles happens in a safety continuum with classical airspace users. This work goes hand-in-hand with building robust cybersecurity resilience, where we

define the critical security requirements and risk methodologies to protect HAO assets from evolving digital threats. Simultaneously, our sustainability experts are conducting in-depth impact assessments on CO2 and non-CO2 atmospheric effects of HAO to ensure innovation remains aligned with Europe's ambitious environmental goals.

Through this partnership, Airbus Protect will provide EASA with concrete regulatory framework proposals, ensuring the European sky remains safe, secure, sustainable, and at the global forefront of aerospace innovation.

New NATO CCDCOE policy brief explores Ukraine's cyber defence transformation and lessons for Allies

Ukraine's ability to defend itself against cyber threats since Russia's full-scale invasion in 2022 is offering valuable lessons for NATO and its allies, according to a new policy brief by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). The research highlights several key policy implications, including the need to develop pre-crisis partnership frameworks, formalise the role of non-state actors in cyber defence, and address the digital sovereignty

implications of deep dependencies on foreign technology companies.

Titled "Ukraine's Cyber Defence Evolution: The Role of Non-State Actors and Public-Private Partnerships," the report is based on interviews and surveys with 39 respondents from 21 Ukrainian organisations across government, military, private sector, and civil society organisations.

The findings show that Ukraine's cyber resilience is built on

four interconnected pillars: the government's innovative approach, expanded roles for private sector actors, intensive international partnerships, and integration with multinational technology companies. While vital for survival, these arrangements have created strategic dependencies that may impact sovereign decision-making and raise questions about their long-term sustainability.

The brief reveals that more than 85% of surveyed

Ukrainian organisations rely heavily on US-based technology providers, creating a vulnerability where operational continuity could depend on the political and financial alignment of foreign entities.

At the same time, the research underscores the importance of informal personal networks have frequently proven more effective than formal coordination channels during a crisis, providing the agility that rigid structures lack.

University of Alabama Names D-Fend Solutions as Counter-Drone Technology Supplier for Campus and Game-Day Airspace Security

D-Fend Solutions, the leader in field-proven radio frequency (RF) cyber-driven, non-kinetic, non-disruptive counter-drone takeover technology, today announced that the University of Alabama has selected and adopted D-Fend as a counter-drone technology supplier.



Deploying EnforceAir, the University has established a pioneer model for higher education airspace security, protecting campus operations, critical infrastructure, and major public events.

As a Tier One R1 research institution, the University of Alabama operates as a "small city," spanning 3.5 square miles with 330 buildings and nearly 50,000 students, faculty, and staff. During football season, the campus becomes one of the largest population centers in the state. Saban Field at Bryant-Denny Stadium hosts over 100,000 fans, while the "sea of humanity" on the campus Quad and surrounding areas can draw an additional 70,000 tailgaters.

Following a comprehensive evaluation of leading technologies, including season-long live performance trials against other systems, the University selected EnforceAir for its unique technical capability to support controlled mitigation, an option to be utilized by authorized, trained personnel in accordance with evolving regulatory frameworks, without the risks associated with kinetic measures or jamming, which can cause collateral damage or disrupt campus communications.

The University recognized that unauthorized drones present risks ranging from accidental collisions and falling debris to the disruption of high-level research and athletic events.

Electrosoft Secures Position on \$500M CISA Digital Transformation Support Services BPA

Electrosoft Services, LLC, a leading provider of federal cybersecurity and digital transformation services, is one of only four awardees on the \$500 million Cybersecurity and Infrastructure Security Agency (CISA) Digital Transformation Support Services (DTSS) Blanket Purchase Agreement.



As a BPA awardee, Electrosoft may secure task orders to deliver enterprise IT governance and delivery services across CISA's operations over a five-year period.

"CISA is a pioneer and continues to lead the way in digital transformation for federal agencies," said Dr. Sarbari Gupta, CEO of Electrosoft. "We are grateful for the opportunity to provide our expertise in cybersecurity, digital engineering and intelligent automation in support of the agency's critical mission. We're honored to be part of CISA's digital transformation effort."

Under the DTSS BPA, CISA is seeking support in multiple areas, including

digital solution development and automation, enterprise data management and analytics, DevSecOps maturity and automation support, and transformation strategy and enablement. These services seek to advance CISA's enterprise IT governance, accelerate digital transformation and enhance mission effectiveness across the agency.

This award reinforces Electrosoft's commitment to advancing federal cybersecurity, digital engineering and enterprise AI capabilities, supporting agencies as they modernize to enhance efficiency and strengthen their security posture.

Emerging AI-Driven Threats Prompt Renewed Focus on Enterprise Cybersecurity

Anthropic just proved that even the company building the most powerful offensive cyber tool ever created can't keep its own front door locked. A CMS misconfiguration exposed Claude Mythos, a frontier AI model that autonomously finds and exploits zero-day vulnerabilities across every major operating system and browser.



A Trusted Computing Group survey found 91% of businesses still lack a formal roadmap for quantum-safe encryption migration, even as NIST deprecation timelines and NSA compliance deadlines narrow the window to months. The 2026 Thales Data Threat Report sharpens the picture: only 47% of sensitive cloud data is encrypted today, down from 51% a year ago, while 61% of organizations rank harvest-now-decrypt-later attacks as their top quantum concern.

Quantum Secure Encryption recently launched QPA v2, an enterprise platform that helps large organizations find the weak spots in their encryption and build a clear plan to upgrade before

quantum computing turns those weak spots into open doors.

The Vancouver-based company says QPA v2 moves the conversation from 'we know there's a problem' to 'here's how we fix it.' The platform includes a planning wizard for governance, budgets, and migration timelines, AI-powered modules that evaluate how ready an organization's cryptography actually is, and inventory tools that scan software, hardware, and encryption components to flag what needs replacing.

"Organizations are now moving from understanding quantum risk to actively planning for it," said Ted Carefoot, CEO of QSE.

Siemens Industrial Edge ecosystem strengthens data and AI integration

Siemens has announced significant expansions to its Industrial Edge ecosystem, accelerating data and AI integration and releasing enhanced cybersecurity functionalities. These enable a seamless integration of IT and Operational Technology (OT) environments, optimize processes and reduce operational disruptions.



The Industrial AI Suite, based on Industrial Edge, is now generally available. It simplifies the entire AI lifecycle and enables embedding industrial AI via a complete infrastructure, easily scaling AI models and managing them across locations. The Industrial AI Suite supports a wide range of AI-based applications such as predictive maintenance and visual inspection to reduce downtime and sustainably increase production quality. In the latest version, the Industrial AI Suite also enables significantly more effective AI model retraining by allowing customers to combine image data with production data from MES systems or controllers.

Monitoring and data acquisition with SCADA systems is now possible in a decentralized manner via Industrial Edge: WinCC Unified is now generally

available, and WinCC Open Architecture is now available as an Edge App and for the virtual PLC (SIMATIC S7-1500v).

Industrial Edge Management version 2.0 combines a redesigned, more user friendly and efficient user interface with enhanced data management and security for distributed infrastructures. At the same time, the platform now supports additional hypervisors such as OpenShift and Hyper-V, enabling Siemens Industrial Edge to be operated flexibly on existing IT infrastructures. Siemens thus bridges the requirements of both the IT and OT worlds. IEC 62443-4-2-certified security functions for critical infrastructures, including air-gapped operation in which systems are physically isolated from external networks, are targeted for release in the second half of 2026 and are expected to provide enhanced cybersecurity.

Spirent Announces Landslide M6 Platform for Validating Next-Generation Mobile Core Networks at Scale

Spirent Communications, now part of Keysight Technologies (NYSE: KEYS), today announced the availability of Spirent Landslide C100-M6, the next generation of its market-leading validation platform for mobile core networks.



Engineered for the increasingly complex and high-volume traffic demands of 5G Standalone (SA) deployments, AI-driven services, and encrypted traffic at operator scale, Landslide M6 provides the increased performance required to validate and accelerate the next phase of network growth.

As 5G SA networks grow more complex with service-based architectures, testing labs have struggled to keep pace with new traffic patterns generated by network slicing, encrypted signaling, and AI-driven applications. To help operators meet these challenges, the Landslide platform has evolved with the M6 capable of delivering up to 3x faster activation rates than its predecessor, 10x more encrypted traffic capacity, and, for the first time, the ability to handle TLS acceleration.

Landslide M6 is available as both a high-performance hardware appliance and a virtual test server, giving teams flexibility in deployment. It introduces dedicated AI application traffic emulation capabilities, including traffic libraries and workload modeling designed to replicate the behavior of AI and machine learning services on live networks. As operators prepare to support AI-native applications and services, this capability ensures they can validate performance under realistic, next-generation traffic conditions before those services reach subscribers.

M6 hardware is already being utilized in Tier 1 operator lab environments, with the M6 Virtual test server option providing an additional deployment path for organizations moving toward cloud-aligned and flexible lab strategies.

FirstEnergy Names Brian Harrell to Lead Enterprise Security

As U.S. utilities confront an increasingly complex landscape of cyber and physical security threats, FirstEnergy Corp. has appointed Brian Harrell, a former senior U.S. homeland security official, as Vice President and Chief Security Officer.



Agency (CISA), where he frequently testified before Congress on countering domestic terrorism and protecting critical infrastructure.

Toby Thomas, Chief Operating Officer, FirstEnergy: "Brian has led security programs that connect intelligence to action in complex, highly regulated environments. That experience will be critical as we strengthen protections across our system and ensure our teams in the field have the tools, training and clarity they need to respond to evolving risks."

In his role, Harrell will enhance the company's enterprise security posture by strengthening defenses, expanding intelligence-driven detection and response capabilities and embedding security more deeply into business and operational planning. His work will emphasize training, readiness and coordination across both corporate and field teams. Harrell's responsibilities span corporate and field security, 24/7 security operations, enterprisewide cybersecurity, threat intelligence, risk and compliance and security architecture and engineering. He will report to Chief Operating Officer Toby Thomas.

Harrell previously served in senior roles within the U.S. Department of Homeland Security, including at the Cybersecurity and Infrastructure Security

Brian Harrell, Vice President and Chief Security Officer, FirstEnergy: "Security only works when it's understood and practiced at every level of the organization. That foundation is essential to a resilient grid, which underpins the strength of our communities, the economy and national security. Sophisticated threats aren't slowing, so we will continue to invest in cybersecurity and risk reduction measures to maintain a reliable and secure system, while strengthening training and readiness for our teams in the field."



Critical Infrastructure Protection Week *in Europe*
20th-22nd October 2026 - Brussels, Belgium

 International Association of CIP Professionals

critical infrastructure
 PROTECTION AND
 RESILIENCE EUROPE



critical infrastructure
 PROTECTION AND
 RESILIENCE **N. AMERICA**
16th-18th MARCH 2027
LAKE CHARLES, LA, USA
www.ciprna-expo.com



World Border Security Congress
13th-15th April 2027 - Lisbon, Portugal
www.world-border-congress.com

ADVERTISING SALES

Bruce Bassin
 Americas
 E: bruceb@torchmarketing.co.uk
 T: +1-702.600.4651

Paul Gloc
 Rest of World
 E: paulg@torchmarketing.co.uk
 T: +44 (0) 7786 270820

critical infrastructure PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium

www.cipre-expo.com

The International Association for CIP Professionals (IACIPP) is proud to announce that CIP Week Europe 2026 will take place in Brussels, Belgium, in the heart that shapes policy for CIPR.

Invitation to Participate

As Europe's leading forum for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together senior leaders from industry, operators, agencies, and government to strengthen collaboration and drive innovation in protecting Europe's essential systems and services.

Register today — Early Bird rates end 20th September 2026.

Now in its 11th year, the conference addresses the most pressing challenges facing operators and agencies, including NIS2 and CER Directive implementation, business continuity, and the resilience of critical infrastructure and entities.

CIPRE features an outstanding international speaker faculty, delivering expert insight, practical experience, and valuable knowledge to support ongoing professional development.

For further information and registration, visit www.cipre-expo.com

Join us in Brussels and network with leading decision makers from corporate and government establishments, agencies and operators tasked with Critical Infrastructure Protection and Resilience.

Co-Hosted by:



Flagship Media Partner:



Global Cybersecurity Partner:



Silver Sponsor:



Supported by:



Help2Protect

