

critical infrastructure



PROTECTION AND RESILIENCE NEWS

Official Magazine of



International Association of
CIP Professionals

SUMMER 2026

www.cip-association.org

FEATURE:

The Preparedness Gap: From Capability to Coordination

FEATURE:

Human risk: why enterprise security must go beyond cybersecurity

FEATURE:

A Tale of Two SOC's: Insights From Two Red Team Assessments



critical infrastructure
PROTECTION AND
RESILIENCE EUROPE
20th-22nd October 2026
Brussels, Belgium
www.cipre-expo.com

**WHEN DEPENDENCIES BECOME CRITICAL: A
DEPENDENCY-CENTRIC PERSPECTIVE ON CRITICAL
INFRASTRUCTURE 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:



Global Cybersecurity Partner:



Gold Sponsor:



Silver Sponsor:



Executive Sponsors:



IT'S A MAD, MAD, MAD, MAD WORLD

Is it me, or does everyone feel like they're living in a dream (or perhaps nightmare!). Geopolitics appears to be taking a turn, and not for the better, with few signs the political will and capabilities are keeping pace to stem the decline.

The war in Ukraine continues to provide challenges to Eastern Europe's borders, Ukraine's critical infrastructure and Europe's supply lines for energy and agriculture.

The wars in the Middle East also continues to create global energy challenges, proxy terrorism threats and cyber attacks against our critical infrastructures. Let alone the many other regional and global threats that are keeping our intelligence and security services on their toes.

There are uncomfortable parallels with the security environment to the classic 1963 comedy, *It's a Mad, Mad, Mad, Mad World*. We seem to be descending into an increasingly chaotic race, with everyone trying to work out what is happening, who they can trust, where the real threat lies and, ultimately, how to get there first.

For those responsible for protecting critical entities, the challenge is no longer simply identifying individual threats. Cyber attacks, physical intrusion, sabotage, espionage, disinformation and other forms of hostile activity are increasingly interconnected, while the distinction between what is criminal, state-sponsored, opportunistic or deliberately ambiguous is becoming harder to establish (and don't get me started on AI!), and the task is to translate that intelligence into practical measures that protect increasingly interconnected systems and the services upon which society depends.

Perhaps the greatest risk is that we continue to approach these challenges as separate problems — cyber here, physical security there, resilience somewhere else — when the reality is increasingly one interconnected threat environment.

The answer will not be found in a single technology, organisation or security discipline. It requires greater collaboration, better intelligence sharing, stronger understanding of interdependencies and, above all, the ability to anticipate how apparently unrelated events may connect.

The race to understand the threat is already underway. The question is whether we are keeping pace. Well, these discussions will be covered during CIP Week in Europe in Brussels, Belgium on 20th-22nd October, with Critical Infrastructure Protection & Resilience Europe the premier conference where lessons can be learnt from sharing of information and experiences, as well as developing your network.

We hope you enjoy this month's read, and hope to see you in Brussels at CIP Week.

Ed.

www.cip-association.org

Editor:

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.



Copyright of Torch Marketing Co Ltd. All rights reserved. No part of this publication may be reproduced by any means whatsoever without the express permission from the publishers. While every effort has been made to ensure the accuracy of the information contained in this publication, the publisher cannot accept responsibility for any errors or omissions it may contain.

When Dependencies Become Critical: A Dependency-Centric Perspective on Critical Infrastructure Resilience



Michael Kolatchev, Principal, Managing Director & Lina Kolesnikova, Senior Consultant at Rossnova Solutions Belgium

Critical Infrastructure Protection (CIP) has traditionally organised resilience around identifiable assets and operators: determine what is critical, assess the risks they face, and strengthen their protection. This logic remains an important foundation of contemporary legislation, regulation and risk management.

The growing emphasis on essential services and functions has broadened this perspective. Their delivery increasingly relies on external platforms, suppliers, technologies and specialised capabilities that may lie beyond the ownership or direct control of the organisations responsible for them.

Contemporary resilience policy already reflects this broader perspective. The EU Critical Entities Resilience (CER) Directive focuses on the continuity of essential services and vital societal functions, while OECD work increasingly addresses resilience at the level of infrastructure systems and their interdependencies.

This article builds on these developments but asks a more specific question: what happens when the systemic significance of a dependency emerges across multiple organisations or sectors and may therefore not be fully visible from any single organisational perspective?

For the purposes of this article, a Critical Dependency is understood as a relationship, resource, service or capability whose disruption compromises the delivery of one or more essential societal functions, irrespective of its formal status within existing CI frameworks. The purpose of the category is not to rename dependencies, but to identify those whose systemic significance becomes visible only when reliance is considered across essential societal functions.

A dependency-centric perspective makes this intermediate level explicit: societal functions define what must be sustained; critical dependencies identify what must remain available; assets, services and capabilities determine how that availability is provided.

When Dependencies Become Systemic

Research on infrastructure interdependencies and systemic criticality has long demonstrated that the consequences of disruption are shaped by the position of assets within wider interconnected systems. A dependency-centric perspective builds on this insight by shifting attention to the relationship between a dependency and the functions that rely upon it.

Dependencies may acquire systemic significance through the



structure of reliance around them. Reliance may be concentrated around a common provider or capability, extend across sectors, or connect organisations responsible for essential functions to resources they neither own nor directly control.

Dependency criticality arises not from the characteristics of a resource, service or capability alone, but from what depends upon it.

A service may appear non-critical when considered within a single bilateral relationship, yet acquire systemic significance when multiple essential functions rely upon it. Conversely, even an important dependency may have limited systemic consequences where realistic substitutes or alternative pathways exist.

This creates a problem of perspective. Existing assessments often examine dependencies from the standpoint of an individual organisation, function or essential service. A dependency-centric perspective adds an aggregate view by considering patterns of reliance across multiple functions, operators or sectors. Each individual organisation

may reasonably conclude that a dependency is manageable, while the same dependency acquires systemic significance when these relationships are considered collectively. That significance may therefore exceed what is visible to any single participant in the system.

Asset criticality and dependency criticality are related but not identical. The systemic significance of a dependency derives from the functions that collectively rely upon it, rather than from its formal status or characteristics alone. Where that significance exceeds what individual actors can see, a dependency becomes more than an operational relationship: it becomes a distinct resilience concern.

What Makes a Dependency Critical?

The analytical challenge is to distinguish routine operational dependencies from those whose disruption could have wider societal consequences. Two considerations are particularly useful in assessing dependency criticality: how reliance is structured and what consequences disruption could produce.



The first concerns how reliance is organised around a dependency: how many essential functions depend upon it, how concentrated that reliance is, and whether realistic substitutes or alternative pathways exist.

The second concerns the consequences of disruption: the scale and severity of functional loss, and the potential for effects to propagate across infrastructures, sectors or societal functions.

These considerations interact. Concentrated reliance becomes more consequential where substitutes are limited and disruption can propagate across essential functions. No single characteristic is therefore sufficient to establish dependency criticality.

Dependency criticality is also contextual. The same service may be replaceable for one operator but indispensable for another. Its significance may change over time as technologies, markets, suppliers and operating conditions

evolve. A capability with several viable substitutes today may become critical following market consolidation, technological integration or vendor lock-in. A routine dependency may also acquire temporary systemic significance during an emergency when alternatives are not immediately available or demand changes sharply.

Capacity adds another dimension to this problem. A dependency may be adequately available to individual essential services under normal conditions yet become constrained when several services require the same resource or capability simultaneously. Criticality may therefore arise not only from the absence of alternatives, but also from whether those alternatives—or the dependency itself—can meet aggregate demand under disruption.

Criticality should therefore not necessarily be understood as a permanent attribute of a dependency. It may instead arise

from a particular configuration of reliance, substitutability, capacity and potential consequences. Identifying critical dependencies requires attention to how these patterns may change over time and under different operating conditions.

Taken together, these considerations provide a basis for identifying dependencies that merit systemic attention without treating every external relationship as a matter for critical infrastructure policy.

Reframing Infrastructure Analysis

Building on existing function-based approaches, a dependency-centric perspective makes explicit an additional level of analysis between essential societal functions and the arrangements through which they are sustained.

Each level addresses a different analytical question. Essential societal functions establish what must continue. Critical dependencies identify what must remain available for those functions to continue, while delivery arrangements determine how that availability is provided and protected. Distinguishing these questions matters because they cannot be fully answered at the same analytical level.

Essential societal functions provide a relatively stable point of reference. Infrastructure assets, technologies, suppliers and delivery arrangements may change, while the functions they sustain tend to be more persistent. Defining what must continue also makes it possible to specify required levels of availability, quality, timeliness and tolerable degradation.

Consider water. Infrastructure analysis examines the systems, organisations and dependencies required to maintain supply. At the level of the essential societal function, the requirement is simpler: water must remain available. The former addresses how this is achieved; the latter establishes what must be sustained.

The distinction matters because an organisation can assess the resilience of assets and services within its field of responsibility without necessarily seeing whether the combined delivery arrangements remain sufficient from the perspective of one or several societal functions. Starting from the function does not eliminate asset- or operator-level analysis; it provides a reference against which the adequacy of those arrangements can be considered.

This sequence can also reveal dependencies whose systemic significance remains less visible when assessment is confined to individual organisations or sectors. A service for which each operator has identified a substitute may, for example, have few realistic alternatives at system level if several operators would turn to the same substitute simultaneously during disruption. Substitutability assessed individually may therefore overstate substitutability across a system of essential functions.

Existing capabilities for identifying assets, tracing dependencies, defining service levels and tolerable disruption, and analysing unacceptable consequences remain indispensable. A dependency-centric perspective



adds a further analytical question: which dependencies acquire systemic significance because of the societal functions that collectively rely upon them?

Governing Critical Dependencies

Making critical dependencies visible analytically does not necessarily make them governable.

An infrastructure asset generally has an identifiable operator. A dependency may instead connect multiple operators, providers and sectors. Each actor may understand and manage its own relationship, while no single actor sees or is responsible for the aggregate dependence created by those relationships.

This creates a governance problem that bilateral risk management alone may not resolve. A provider may satisfy its obligations to every individual customer, and each operator may have assessed that provider within its own risk framework. Yet collective reliance by several essential functions may create systemic significance that

no bilateral assessment captures.

The problem becomes particularly visible where multiple essential services rely on the same digital platform, software ecosystem or specialised provider. Each organisation may have identified and managed its own dependency through contractual arrangements, service-level requirements or contingency measures. Those arrangements, however, do not necessarily reveal whether the provider (or available alternatives) could support simultaneous demand from multiple essential services during a large-scale disruption.

Bilateral assurance may therefore be insufficient where criticality is collective.

The problem is partly one of information rather than individual responsibility. Operators may understand their own dependencies but lack visibility of aggregate reliance. Providers may know their customer base without being positioned or expected to assess the societal significance of every function



those customers deliver. Sectoral regulators may see dependencies within their domains while missing concentrations that emerge across sectors. Systemic significance can therefore arise from information that exists in fragments but is not aggregated at the level at which the systemic nature of risk becomes visible.

The governance challenge is not simply to improve coordination, but to make aggregate reliance visible and actionable. This requires visibility beyond direct organisational dependencies, coordination where systemic significance crosses sectoral responsibilities, and continued reassessment as providers, technologies and substitutes change. Most importantly, assurance may need to reflect aggregate reliance rather than bilateral performance alone.

The relevant question is not only whether individual obligations can be met, but whether the dependency as a whole is sufficiently resilient given the combined importance of the

essential functions that rely upon it. This does not imply that providers should automatically bear responsibility for all possible societal consequences of downstream dependencies. Imposing such responsibility indiscriminately could itself create disproportionate or commercially unsustainable obligations.

Where, then, should responsibility for resilience reside when the systemic significance of a dependency exceeds its importance to any individual customer?

Formal designation is not necessarily the answer. Treating every systemically significant dependency as critical infrastructure could simply expand existing categories without resolving the underlying governance problem. Different dependencies may require different combinations of information sharing, assurance, contingency planning, coordination or regulatory attention.

Who should perform this aggregating function will vary across governance systems. What matters is that aggregate reliance becomes visible at a level where its systemic significance can be assessed and, where necessary, addressed.

Assets remain essential objects of protection. Critical dependencies should also become explicit objects of resilience governance.

Conclusion

The central issue is not whether critical infrastructure depends on external services, suppliers and capabilities. It is whether their systemic significance becomes visible before disruption reveals it.

A dependency-centric perspective connects what society needs to sustain with what else must remain available for those functions to continue. In doing so, it can reveal aggregate reliance that exceeds what any individual actor can see or manage through bilateral arrangements.

Such a perspective cannot resolve the resulting governance problem by itself. But it can make it visible.

The next step for critical infrastructure resilience may therefore be not simply to map more dependencies, but to recognise when and where they acquire systemic significance across essential societal functions—and to ensure that this significance can be identified, assessed and governed.

TSA Administrator Launches Horizon 25 Strategy

The Transportation Security Administration (TSA) today announced the Horizon 25 Strategy as the agency approaches its 25th anniversary and Administrator David P. Cummins looks ahead to TSA's next quarter century.

This strategic vision is designed to drive excellence and resiliency for many years to come. To achieve this, Cummins has defined three primary goals to deliver on our zero-fail mission. These priorities will modernize TSA's checkpoints, elevate the traveler experience, and harden multi-modal transportation security.

"President Trump and Secretary Mullin have entrusted me with the task of modernizing TSA," Cummins said. "In its first 25 years, this agency has performed its critical Homeland Security mission with dedication and excellence. As we look forward to the next 25 years, we must constantly work to stay ahead of evolving threats and deliver a Golden Age of Travel. Through the Horizon 25 Strategy, we will build a TSA that is agile, resilient

and ready for tomorrow's challenges."

To rapidly advance key strategic initiatives, Cummins will bring together innovators and groundbreakers from across the agency, including field and headquarters personnel, in September.

These initiatives include enhancing TSA PreCheck®, improving the passenger experience, streamlining the acquisition of new technology, expanding TSA's capabilities to counter the threat of unmanned aircraft systems and advancing other key priorities.

This strategy will accelerate public-private partnerships with industry leaders across sectors to expand modernization across TSA. An evolved Screening Partnership Program will replace TSA Gold+ to better harness the role of the private sector in delivering a safer, more secure, and more efficient aviation system.

Each initiative of this strategic vision reflects the core philosophy Cummins brings to the agency.

"TSA does not have to choose between a secure checkpoint, an efficient checkpoint, and an elevated passenger experience," said Cummins. "Through Horizon 25, TSA can, and will, deliver all three at once."

Over the past year, TSA has kept America's transportation systems secure through unprecedented travel events, partial government shutdowns, and record-breaking passenger volumes.

As a transportation executive in the private sector with extensive experience collaborating with federal agencies and private sector partners, Cummins has overseen strategy for transportation systems globally with an emphasis on innovation and forward thinking. He brings that same attitude to government service in advancing his priorities for TSA.

With Cummins now at the helm, TSA is ready to move forward and tackle the challenges and opportunities ahead with boldness, creativity and a commitment to innovation.

TSA installs new computed tomography screening technology at Juneau International Airport

The Transportation Security Administration (TSA) has installed two new state-of-the-art computed tomography (CT) checkpoint X-ray machines that enhance screening capabilities of carry-on items brought to the checkpoint by passengers ticketed to fly out of Juneau International Airport.

The new CT x-rays screen carry-on items at the checkpoint by applying a sophisticated algorithm as they generate a 3-D image of the contents of carry-on bags. This new technology creates such a clear image



of a bag's contents that the system can automatically detect explosives and other threat items by shooting

hundreds of images with an X-ray camera spinning around the items to provide TSA officers with a 3-D view of the contents of a carry-on bag. A TSA officer can view the 3-D X-ray image on a monitor and manipulate the image to get a better view of the bag's contents, ultimately reducing the number of carry-on bags that need to be opened and manually inspected.

However, if a bag requires further screening, a TSA officer will inspect it to ensure that a threat item is not contained inside.

Tailored cybersecurity at scale. Precision-built for complexity, compliance, and resilience.

ESET PRIVATE delivers tailored cybersecurity at scale. Engineered for complex environments, it brings together expert advisory, advanced threat protection, and custom services to safeguard critical assets.

Backed by strategic partnerships and intelligent technologies, it integrates seamlessly into operations and supports compliance. The result? Cyber resilience—purposefully aligned to your goals, sector, and growth.



Advisory



Delivery



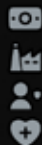
Operation

ESET PRIVATE key offerings



Air-Gapped Solutions

Multilayer, cutting-edge protection to secure restricted networks from known and evolving threats. Benefit from flexible deployment, compliance support, and full control over your security stack.



Client Shield

From service provider to customer — a multiplatform, white-label security offering. Boost customer confidence, reduce digital risk, and unlock new revenue by integrating advanced cyber protection into the customer experience.



Scanning Solutions

High-accuracy scanning for large volumes of inbound data—combining flexible deployment with advanced protection against never-before-seen threats. Ultra-fast and purpose-built for scale, it maintains throughput with minimal performance impact.



Threat Intelligence

Dedicated threat intelligence with geopolitical and sector-specific insights. Delivers early warnings, focused adversary monitoring, and exclusive research collaboration to strengthen proactive defenses.



Managed Security

End-to-end managed security operations with 24/7 monitoring and incident response across multiple perimeters. Custom-built for your environment, it includes dedicated SOC teams and compliance reporting.



Industrial Security

End-to-end protection across the entire IT and OT environment. Purpose-built for critical infrastructure and legacy systems, it secures connectivity and reduces cyber risk without disrupting operations.



Advisory

Custom cybersecurity strategies to strengthen readiness, compliance, and awareness. It helps organizations proactively anticipate, withstand, and adapt to threats, while protecting continuity and core business needs.



Industries

 Financial Services

 Utility

 Manufacturing

 Transportation, Logistics

 Government, Defense

 Digital / IT

 Healthcare

 Telco

This is ESET

Proactive defense. Minimize risks with prevention.

Stay one step ahead of known and emerging cyber threats - targeted attacks, zero-day threats, ransomware, phishing, and more - with our AI-Native, prevention-first approach. ESET combines the power of AI and human expertise to deliver easy and effective protection.

Experience best-in-class, science-driven security, backed by over 35 years of in-house global cyber threat intelligence. Our extensive R&D network, led by industry-acclaimed researchers, powers our award-winning, cloud-first cybersecurity platform. ESET solutions are highly customizable, include local support, and have minimal impact on performance. ESET protects your business so you can unlock the full potential of technology.



The largest global EU-owned & based company with over 35 years of experience in the cybersecurity industry



We work with four of the Magnificent Seven global tech companies



Long-term and consistent recognition by leading analysts for innovative and effective cybersecurity solutions

ESET IN NUMBERS

35+
years of
experience

1bn+
protected
internet
users

500k+
business
customers

178
countries

11
global R&D
centers

TRUSTED BY GLOBAL BRANDS



Google Play

Canon



intel.



LET'S DISCUSS
YOUR
CYBERSECURITY
CHALLENGES



Cybersecurity
Progress. Protected.

The Preparedness Gap: From Capability to Coordination



By Catherine Piana, Secretary General, Confederation of European Security Services (CoESS)

Europe's Preparedness Era

Europe's approach to security has undergone a profound transformation. For decades, policy debates concentrated on identifying threats, strengthening protective measures and developing the capabilities needed to respond to crises. While these priorities remain

essential, the focus has gradually shifted from resilience towards preparedness. The question is no longer simply whether Europe possesses sufficient capabilities, but whether it is prepared to organise and mobilise them effectively when they are needed most.

This evolution is reflected in recent

European initiatives, including the Critical Entities Resilience (CER) Directive, the NIS2 Directive and, more recently, the Preparedness Union Strategy. Together, they signal a broader understanding of resilience, one that extends beyond emergency response to encompass anticipation, coordination and the ability of

society as a whole to withstand, manage and recover from disruption.

Preparedness is therefore no longer solely the responsibility of governments or emergency services. It requires a whole-of-society approach in which public authorities, Critical Infrastructure operators, emergency responders, businesses and relevant regulated actors each contribute to a shared resilience architecture.

Yet despite this evolution, an important challenge remains largely overlooked.

Across Europe, many of the capabilities that would prove essential during a crisis already exist. Public authorities, emergency services, Critical Infrastructure operators, regulated private security providers, specialised technology operators and other essential actors protect critical infrastructure, monitor sensitive facilities, respond to alarms, secure transport networks, support business continuity and provide situational awareness around the clock.

However, these capabilities are still too often brought together only after a crisis has begun, in the absence of agreed governance arrangements, communication protocols, operational procedures and established coordination mechanisms.

This article argues that Europe faces not only capability gaps, but also what I describe as the Preparedness Gap: the gap between the capabilities and experience available within society and those effectively recognised, integrated and institutionalised as part of preparedness before a



crisis occurs.

Closing this gap requires more than additional investment or new technologies. It requires a shift in mindset: from viewing resilience as the accumulation of capabilities to understanding it as the organisation of capabilities.

Private security offers a compelling illustration of this broader challenge. With approximately two million licensed professionals operating across Europe, the sector contributes daily to the protection of airports, ports, energy facilities, hospitals, public institutions, transport networks and countless other critical assets. Yet despite this operational presence, the sector's capabilities, expertise and operational resources are frequently incorporated into preparedness arrangements only when emergencies are already unfolding. This is not simply a challenge for one sector. It reflects a broader governance challenge that is relevant to every organisation responsible for preparedness and the protection of society.

Preparedness therefore raises a

broader question than capability development alone:

How can existing capabilities become an integral part of resilience before, not during, the next crisis?

The Preparedness Gap

Public policy frequently refers to capability gaps, skills shortages or technological deficits. These concepts assume that resilience depends primarily on acquiring what is missing. While this remains true in some areas, it does not fully explain why well-equipped societies continue to encounter coordination challenges during major emergencies.

Increasingly, Europe's preparedness challenge lies elsewhere. In many cases, the necessary capabilities already exist, but they remain insufficiently recognised, connected and embedded within preparedness planning.

I therefore propose a complementary concept: the Preparedness Gap.

The Preparedness Gap is the difference between the capabilities



and experience available within society and those effectively recognised and fully integrated in governance, procedures and operational planning, as part of preparedness before a crisis occurs.

In practical terms, preparedness means that roles and responsibilities, communication protocols, standard operating procedures, information-sharing mechanisms, legal authorities and decision-making processes have already been agreed, tested and exercised before an emergency arises. It also means that procurement models are designed for long-term resilience, not short-term cost efficiency. And finally, it makes sure that valuable operational experience gained during previous crises is translated into permanent institutional practice.

In short, preparedness is about ensuring that every relevant capability, and every relevant lesson, has already been recognised, connected and embedded before the first alarm is raised. This saves precious time and energy in crises, during which these resources are most scarce.

Why the Preparedness Gap

Persists

The Preparedness Gap rarely results from a single policy failure. Rather, it emerges from the gradual accumulation of decisions taken across different policy domains, often with legitimate but disconnected objectives. Legal frameworks, procurement models, operational planning and institutional cultures have evolved in parallel rather than together, creating preparedness systems in which existing capabilities are not always fully connected.

Closing the Preparedness Gap therefore requires more than additional resources. It requires preparedness to be understood as a question of governance.

Four dimensions deserve particular attention.

Recognition

Preparedness begins by recognising which capabilities already exist within society.

Many preparedness frameworks understandably focus on public institutions and emergency responders. Yet resilience increasingly depends on a much broader ecosystem of stakeholders that contribute to the protection

of Critical Infrastructure every day. Recognition does not imply transferring public responsibilities or blurring lines of authority. Rather, it means acknowledging operational realities and understanding how existing capabilities can contribute more effectively before, during and after crises.

Recognition is therefore the first step towards integration. Capabilities cannot become part of preparedness if they are absent from preparedness planning.

Integration

Recognition alone is not enough. Capabilities become operationally meaningful only when they are translated into preparedness.

That requires more than acknowledging their existence. It means embedding them in contingency planning, governance arrangements, communication protocols, information-sharing mechanisms, joint exercises and clearly defined responsibilities before a crisis occurs.

In practice, however, cooperation often develops only out of operational necessity. Public authorities, Critical Infrastructure operators and private actors establish pragmatic, ad hoc working relationships because circumstances leave them little alternative. These improvised arrangements frequently demonstrate remarkable professionalism and commitment. They also consume valuable time and energy at precisely the moment when both are most limited.

The more fundamental challenge emerges after the crisis.

Once normality returns, temporary cooperation too often disappears with it. Operational experience is acknowledged, reports are produced and participants are thanked for their commitment. Yet valuable lessons are not always translated into revised governance, updated contingency plans, regular joint exercises or permanent cooperation mechanisms.

As a result, each new crisis risks beginning with many of the same conversations, uncertainties and organisational barriers as the previous one.

The issue is not whether societies learn from crises. It is whether institutions learn quickly enough to transform operational experience into permanent preparedness.

Preparedness should ensure that cooperation no longer depends on operational necessity alone, but becomes a permanent feature of resilience.

Governance

Preparedness also depends on clarity.

- Who has the authority to act?
- Who shares information, with whom, and under what conditions?
- Who makes operational decisions?
- Who assumes responsibility?
- How are roles and responsibilities coordinated across organisations?

These questions often prove more complex than the technologies themselves. Without clearly defined governance arrangements, even highly capable organisations struggle to



work together efficiently under pressure.

Governance is therefore not an administrative layer added to preparedness. It is the mechanism through which individual capabilities become collective resilience.

Sustainability

Preparedness cannot be separated from the long-term sustainability of essential capabilities.

Resilience depends on organisations being able to recruit, train and retain qualified professionals, invest in innovation and maintain operational readiness over time.

Procurement strategies that prioritise lowest price at the expense of quality may appear economically efficient in the short term, yet they can gradually erode the capabilities upon which preparedness ultimately relies. Workforce resilience, professional standards and sustained investment are therefore not simply economic concerns; they are integral components of preparedness itself.

Three Symptoms of the

Preparedness Gap

The Preparedness Gap is rarely visible during routine operations. It becomes apparent when crises expose the disconnect between existing capabilities and the governance arrangements needed to mobilise them effectively.

The following examples come from different operational domains. They involve different technologies, legal frameworks and stakeholders. Yet they reveal the same underlying challenge: the necessary capabilities already exist, but they are not always sufficiently integrated into preparedness before they are needed.

Symptom 1 – Emergency Planning

Perhaps the clearest illustration of the Preparedness Gap lies in emergency planning itself.

Across Europe, public authorities, emergency services, Critical Infrastructure operators and private security organisations routinely cooperate during major incidents. Terrorist attacks, natural disasters, industrial accidents and large public events have repeatedly demonstrated the professionalism and commitment



of all actors involved.

Yet this cooperation frequently develops under the pressure of events rather than through prior preparedness.

As situations evolve, communication channels are established, responsibilities clarified and practical solutions found. Organisations adapt remarkably well to circumstances that no contingency plan could fully anticipate.

This capacity to improvise is one of Europe's strengths.

It should not, however, become its preparedness model.

Improvisation inevitably consumes time, leadership attention and operational capacity precisely when these resources are most valuable. More importantly, once the crisis has passed, many temporary arrangements disappear. Relationships remain personal rather than institutional, while lessons identified are not always translated into revised procedures, regular joint exercises or permanent governance mechanisms.

The consequence is that each major crisis risks beginning with

many of the same discussions about roles, responsibilities and coordination.

Preparedness should ensure that these conversations have already taken place.

Symptom 2 – Counter-UAS

Counter-Unmanned Aircraft Systems (Counter-UAS) are frequently presented as a technological challenge.

In reality, technology is only one part of the equation.

Detection systems continue to improve. Artificial intelligence enhances identification capabilities, while mitigation technologies continue to evolve. Yet technology alone cannot determine how a drone incident is managed.

Who is authorised to detect?

Who validates the threat assessment?

Who decides whether intervention is justified and authorises it?

Who coordinates the operational response?

How are responsibilities allocated between public authorities, Critical Infrastructure operators and specialised security providers?

These are governance questions.

Without clear answers established before an incident occurs, even the most advanced technologies risk being deployed inefficiently or too late.

Counter-UAS therefore illustrates a broader lesson. Preparedness is not achieved simply by acquiring new capabilities. It depends on integrating those capabilities into coherent legal, operational and institutional frameworks long before they are required.

In many cases, the technology gap is smaller than the preparedness gap.

Symptom 3 – Critical Communications

Critical communications provide perhaps the most tangible illustration of the Preparedness Gap.

Across Europe, Monitoring and Alarm Receiving Centres continuously monitor sites, verify incidents and assess the credibility of alarms before emergency services are alerted. They already generate information that is filtered, verified and operationally relevant.

Yet in many cases, this information still reaches emergency services through traditional voice telephone calls. The capability to produce high-quality situational awareness already exists. Technologies capable of digitally transmitting structured, verified information also exist. What remains insufficient is their systematic integration into emergency communication architectures.

The result is not merely a technical inefficiency.

It is a preparedness issue.

Every additional telephone conversation introduces delay, increases the potential for misunderstanding and limits the ability to establish a common operational picture. During rapidly evolving incidents, these seemingly minor inefficiencies can accumulate into significant operational consequences.

The challenge is therefore not primarily one of digital innovation.

It is one of governance, interoperability and preparedness.

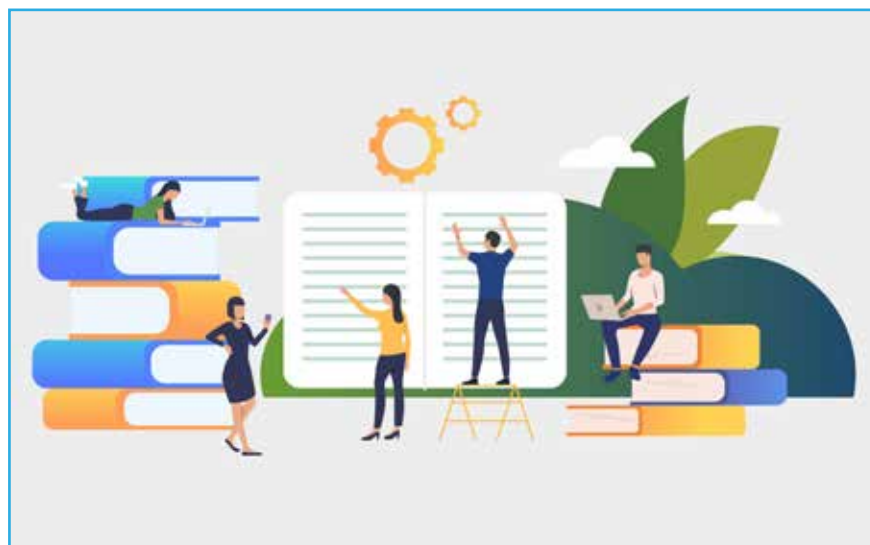
When existing capabilities remain disconnected, technology cannot fully deliver the resilience it promises.

From the Preparedness Gap to Preparedness by Design

Identifying the Preparedness Gap is only the first step. The more important challenge is to rethink how preparedness itself is conceived.

Too often, preparedness evolves reactively. Crises expose weaknesses, force organisations to cooperate and generate valuable operational experience. Some of these lessons become policy or practice. Many remain local, temporary or informal. As a result, familiar coordination challenges continue to reappear from one crisis to the next.

Preparedness by Design requires a different approach. Rather than relying on crises to create cooperation, it seeks to ensure that the relationships, governance arrangements and operational interfaces required during emergencies already exist before they are needed.



This approach rests on four principles.

Recognise capabilities

Preparedness should begin with a comprehensive understanding of the capabilities that already exist across society. Effective resilience depends not only on public institutions but also on the regulated private actors, operators and service providers that contribute daily to the protection of Critical Infrastructure and essential services.

Integrate before crises

Capabilities create value only when they are connected.

Emergency planning, communication protocols, information-sharing mechanisms and joint exercises should be established before an incident occurs, not developed under operational pressure.

Govern cooperation

Preparedness requires clear responsibilities, decision-making structures and legal frameworks that enable organisations to work together efficiently. Governance is what transforms individual

capabilities into collective resilience.

Institutionalise learning

Every crisis generates valuable operational experience. Preparedness by Design requires this experience to be systematically translated into revised procedures, permanent cooperation mechanisms, regular exercises and continuous improvement. Resilience should not depend on institutional memory alone; it should be embedded in institutions themselves.

Preparedness is therefore not simply the ability to respond effectively when a crisis occurs. It is the ability to ensure that existing capabilities, partnerships and lessons learned have already been transformed into a coherent system before the next crisis begins.

Closing the Preparedness Gap is ultimately not about creating more capabilities.

It is about designing preparedness so that the capabilities already available can achieve their full collective value.



Conclusion

Europe has entered an era in which preparedness has become as important as protection. This reflects an important recognition: resilience cannot be built during a crisis alone. It must be designed beforehand.

The concept of the Preparedness Gap offers a complementary way of understanding resilience. It shifts the debate from what is missing to what already exists but remains insufficiently connected. It reminds us that preparedness is not simply about acquiring new capabilities, but about recognising, integrating and institutionalising the capabilities and experience that society already possesses.

Private security is one illustration of this broader challenge. The same reasoning applies wherever valuable capabilities remain outside preparedness planning, where cooperation depends on personal relationships rather than established governance, or where operational experience is not systematically transformed into lasting institutional practice.

Europe's next step in strengthening preparedness

may therefore depend less on creating additional capabilities than on organising the capabilities it already possesses. In an increasingly complex risk environment, resilience will not be determined solely by the quality of individual organisations, technologies or regulations, but by the way they are designed to work together.

Closing the Preparedness Gap ultimately means making preparedness intentional rather than incidental.

Because preparedness should never begin when the first alarm is raised. It should already be embedded in the relationships, governance arrangements and capabilities that protect our societies every day.

Ultimately, Europe's resilience will depend less on the capabilities it possesses than on its ability to organise the capabilities it already has.



PROTECTING TO EMPOWER

Protecting what keeps Europe moving

Europe's critical infrastructure operates in increasingly digitalised and interconnected environments, facing threats that span both the physical and digital domains.

IndraMind connects data, systems and stakeholders to deliver a unified view of the situation, anticipate risks and ensure operational continuity—helping critical infrastructure stay ahead of emerging threats.

The Detection Gap: Why Distributed Infrastructure Operators Are Flying Blind Across Their Own Estates



By Ross Palmer, CEO, OpSiteAI

In 2024, a routine software update from a major cybersecurity vendor triggered a global IT outage that cascaded across aviation, healthcare, finance and logistics within hours. The incident was not the result of a sophisticated attack. It was the result of a change that nobody saw coming, and nobody detected fast enough.

The lesson was not primarily about cybersecurity. It was about visibility.

Across distributed infrastructure environments, from multi-site retail and forecourt networks to utilities, transport hubs and branch operations, the question that the 2024 outage exposed is one that most operators still cannot answer in real time:

What is happening across every site in your estate right now, and what is it costing?

For most organisations, the honest answer is: we do not know until something fails. And by the time we know, the financial exposure has already been building for minutes, hours, or in some cases, considerably longer.

The IT/OT convergence problem nobody is solving

The convergence of IT and operational technology has transformed how distributed infrastructure environments function. What were once isolated, proprietary OT systems now sit alongside corporate networks, cloud platforms, IoT devices, edge compute infrastructure, and remote access tools. The connectivity has driven efficiency. It has also created a category of risk that most monitoring frameworks were not designed to address.

Traditional monitoring tools are built around a binary state; a system is either online or offline, an alert fires when a threshold is crossed. A ticket is raised. A response is initiated.

But the most expensive operational failures in distributed environments rarely begin with a binary state change. They begin with degradation, a subtle, progressive decline in performance that falls below the threshold of standard monitoring but above the level at which the system is functioning acceptably.

A payment terminal is slowing down during peak trading hours. A network device drops and reconnects across multiple sites. A heating system is running outside scheduled hours because the scheduling configuration drifted after a firmware update. An access control system logs intermittent failures that nobody connects to a broader pattern.

None of these triggers a standard alert. None of them appears on a dashboard. But each one is a signal, and each one has a



financial exposure that accumulates silently while attention is directed elsewhere.

The most expensive operational failures rarely begin with a system going offline. They begin with a system quietly degrading, below the threshold of standard monitoring, above the level of acceptable performance.

The cost of not knowing

Quantifying the financial exposure of delayed operational detection is difficult precisely because most organisations have never measured it. The metrics that infrastructure operators track, such as uptime, incident response time, and mean time to repair, all begin at the point of detection. They say nothing about the time between when something starts going wrong and when anyone finds out.

That gap, what practitioners increasingly refer to as Mean Time To Detect, or MTTD, is where the highest and most avoidable operational cost sits.

In one analysis of a 346-site estate across retail and forecourt environments, that gap was responsible for:

- Delayed detection and

operational disruption cost the equivalent of more than half a million euros annually.

- Engineer call-outs are dispatched without adequate diagnostic information, requiring repeat visits and generating avoidable costs.
- Energy systems are running outside operational hours because no automated detection flagged the deviation.

Aggregated across the estate, the total financial impact of delayed operational detection approached € 1 million per year. Not from a single catastrophic failure. From the daily, quiet accumulation of issues that nobody saw.

The figure is not unusual. Across distributed environments of similar complexity, the pattern is consistent, and the number is almost always larger than operators expect when they first model it.

Why siloed systems make the detection gap worse

Most distributed infrastructure operators do not lack monitoring tools. They have them in abundance. Network monitoring. Device management platforms. Building management systems. SCADA infrastructure. Ticketing



systems. Energy management dashboards.

The problem is that these systems do not talk to each other, and crucially, none of them connects operational signals to financial outcomes in real time.

When an incident occurs across a distributed estate, the response typically looks like this: a site calls in to report a problem. The operations team begins checking systems, the network first, then devices, then the application layer, then third-party suppliers. Each check requires a different tool, a different login, a different data source. By the time a root cause is identified, the window for minimising cost has often already closed.

The 2024 global IT outage illustrated this at scale. The organisations that recovered fastest were not those with the most sophisticated individual monitoring tools. They were those with the most unified operational picture, the ones who could correlate signals across systems, identify the scope of the impact rapidly, and direct resources with precision.

The organisations that recover fastest from operational failures are not those with the most monitoring tools. They are those with the most unified operational picture.

In distributed environments, that unified picture is almost universally absent. Security teams have their tools. Facilities teams have theirs. Network operations has its own. Each sees one layer of the estate. Nobody sees the whole thing, and nobody has connected what they see to what it means financially.

The shift from reactive to operational intelligence

The framework that is emerging across critical infrastructure sectors, and which the NIS2 Directive accelerates for a wider range of organisations, is one that shifts from reactive detection to what practitioners are beginning to call operational intelligence.

The distinction is important. Monitoring tells you when something has failed. Operational intelligence tells you when something is about to fail, and what the cost of that failure will be if it is not addressed.

Practically, operational intelligence in a distributed environment requires three capabilities that traditional monitoring does not provide:

- **Correlation across systems:** the ability to connect signals from network infrastructure, OT devices, application performance and environmental systems into a single operational view
- **Anomaly detection before failure:** the identification of deviations from normal behaviour that precede incidents, rather than alerts that fire after they occur
- **Financial quantification:** the translation of operational signals into commercial impact, so that incidents can be prioritised by what they cost the estate rather than by the order in which they were reported

Together, these capabilities close the detection gap. They reduce MTTD from hours to minutes. They eliminate the diagnostic lag that results in avoidable engineer deployments. And they give infrastructure operators something they rarely have today, a real-time financial picture of what is happening across their entire estate.

Implications for NIS2 and distributed operators

The NIS2 Directive, which broadens the scope of critical infrastructure regulation across the European Union, requires operators to implement appropriate technical and organisational measures to manage cybersecurity and operational risk. Critically, it extends these requirements beyond the sectors traditionally classified as critical infrastructure



critical infrastructure

PROTECTION AND
RESILIENCE N. AMERICA

16TH-18TH MARCH 2027

LAKE CHARLES, LA, USA

www.ciprna-expo.com

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 (CIRCIA).

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:





to include a wider range of entities, including large-scale retail operators, forecourt networks and distributed commercial infrastructure.

For many of these operators, NIS2 compliance will require, for the first time, a formal approach to operational risk monitoring that connects their IT and OT environments. The directive's emphasis on incident reporting timelines and on the ability to demonstrate proactive risk management rather than reactive response aligns directly with the shift toward operational intelligence.

Organisations that invest in unified operational visibility ahead of compliance deadlines will find themselves better positioned to meet regulatory requirements. More importantly, they will find themselves better positioned operationally, with a demonstrably lower cost base and a more resilient estate.

NIS2 compliance will require many distributed operators to formally connect their IT and OT

environments for the first time. The organisations that do this ahead of the deadline will find they have solved a commercial problem, not just a regulatory one.

Closing the gap: what operational intelligence looks like in practice

Across live deployments in distributed retail, forecourt and infrastructure environments, the shift from reactive monitoring to operational intelligence has produced consistent and measurable outcomes:

- Issues detected before sites report them, reducing the detection gap from hours to minutes across complex multi-site estates
- Engineer deployments eliminated before dispatch, by providing complete diagnostic information remotely, allowing resolution without site visit
- Operational cost quantified automatically, giving infrastructure leaders a financial narrative to present to boards and regulators, not just a technical one

- Incidents resolved significantly faster, compressing the window between something going wrong and normal operations resuming

These outcomes are not the product of any single technology. They are the product of a fundamentally different approach to operational visibility, one that treats the estate as a connected system rather than a collection of independently monitored assets.

The detection gap is not a new problem. But the tools to close it are now mature enough to deploy at scale across distributed environments. The question for infrastructure operators in 2026 is not if the gap exists. It is whether they can afford to leave it open.

Ross Palmer is CEO of OpSite AI, an operational intelligence platform that helps distributed infrastructure operators detect, prioritise and resolve operational issues before they impact revenue or continuity. OpSite AI works with retail, forecourt and enterprise operators across Ireland and is expanding into the UK and Europe. opsiteai.com

Mid-America Transportation Projects Receive National Honors for Strengthening Communities

Twelve state department of transportation projects in Illinois, Indiana, Kentucky, Michigan, Minnesota, Missouri, Ohio and Wisconsin have won top regional honors in the 2026 America's Transportation Awards competition. From bridging safer connections for pedestrians and bicyclists to deploying innovative high-water warning systems that help protect motorists during flooding events, these projects are strengthening communities by bolstering safety, mobility, and quality of life.

Selected from 27 projects submitted by 10 states in the Mid America



Association of State Transportation Officials (MAASTO) region, these entries are part of a record 127 nominations from 45 state DOTs in this year's overall competition. Sponsored by the American Association of State Highway and Transportation Officials (AASHTO), the America's Transportation Awards honor transportation projects that

deliver meaningful benefits to communities. Projects compete in four categories—Quality of Life/Community Development, Operations Excellence, Best Use of Technology & Innovation, and Safety—showcasing the essential role transportation plays in improving mobility, safety, and quality of life for all users.

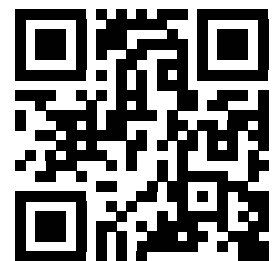
Many of this year's MAASTO regional winners benefited from IIJA funding, demonstrating the critical role the next federal surface transportation legislation will play in continuing progress toward safer communities and improving mobility and access for all.

FORTINET

The Highest Level of OT Security Assurance

FortiOS 7.6 achieves
IEC 62443-4-2 Security
Level 4 certification for
critical infrastructure protection.

Scan for more information:





Critical Infrastructure Protection & Resilience Europe

20th–22nd October 2026
Brussels, Belgium

www.cipre-expo.com

Co-Hosted & Supported by::



The International Association of Critical Infrastructure Protection Professionals (IACIPP) marks its eleventh year at a moment when the protection and resilience of Critical National Infrastructure (CNI) is being reshaped by a rapidly evolving threat landscape. Increasing interconnectivity, dependence on global technologies, complex supply chains, extreme weather, and rising geopolitical tensions have collectively heightened the vulnerability of essential services.

We are operating in an era defined by complexity, interdependence, and accelerating technological change. The resilience of critical entities has never been more important, or more difficult to achieve. Energy grids, water systems, transport networks, telecommunications, and financial services form the foundation of modern society. They enable economic stability, safeguard communities, and underpin national security. Yet as these systems advance, the threats confronting them grow in sophistication, scale, and persistence.

The risk environment continues to shift rapidly. Climate change is driving more frequent and severe extreme weather events, placing unprecedented strain on physical infrastructure. Simultaneously, geopolitical tensions are disrupting global supply chains and exposing new strategic vulnerabilities. Infrastructure long challenged by

physical hazards and natural disasters is now increasingly threatened by cyber risks.

Cyberattacks on infrastructure have evolved from isolated incidents into systemic, cross sector risks. Ransomware, supply chain compromises, and state sponsored campaigns are targeting the essential arteries of national life. Across the infrastructure community, there is a clear recognition that strengthening resilience is now a strategic imperative, one that transcends individual sectors and national borders.

European policymakers share this understanding and are working to translate it into meaningful behavioural change through the NIS2 Directive, governing networks and information systems, and the Critical Entities Resilience Directive (CER), which adopts an all hazards approach encompassing physical security, operational continuity, and supply chain resilience.

Together, NIS2 and CER establish a comprehensive resilience regime designed to hold organisations accountable. It is no longer sufficient to demonstrate that policies exist or that training has been completed. Regulators now expect evidence that security controls function effectively in practice.

Future challenges will remain multi dimensional, demanding that collaboration sits at the heart of every strategic, policy, procedural, and technological response.

In contributing to that collective effort, IACIPP continues to expand its activities and cultivate new, dynamic partnerships across the globe, strengthening the association's role in advancing critical infrastructure protection and resilience.

We have continued to focus on providing a platform for international partners to share information and good practices. Our web portal delivers relevant and timely information for members. That portal has become an essential component of our Association providing understanding on new legislation, communicating innovative practices and creating a reference point for

White Papers and conference presentations and materials.

The website continues to develop alongside our quarterly publication, 'Critical Infrastructure Protection and Resilience News' which hopefully is where you are reading this piece!

The magazine has been an enormous success. It features articles on a whole range of infrastructure subjects and concerns and highlights the range of new technology that is constantly emerging to assist in the protection and resilience of our Critical Entities.

Our last magazine, the Winter 2025/26 edition, contained articles on subjects such as: Lessons from Ukraine on Information Warfare, Executive Decision Failure in Critical Infrastructure, Creating Security and Resilience in Critical Infrastructure and many more. It also included opinion pieces, agency updates and Industry news.

This year will see IACIPP host the 11th 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition. The conference has grown to be the premier event covering Critical Infrastructure Protection and Resilience across Europe and will be held in Brussels in October. Previous hosts cities have included, London,

The Hague, Milan, Bucharest, Prague and Madrid and Brindisi.

This year also marks the third Critical Infrastructure Protection (CIP) Week in Europe. We launched this joint initiative in 2024 in Madrid, in partnership with our colleagues at EU CIP, a Horizon Europe project. The combination of CIPRE and EU CIP was the first of its kind—bringing together two complementary communities to deepen understanding of emerging challenges, explore the implications of new EU directives, and examine the growing complexity of the threat environment facing Europe's critical entities.

It also created a unique platform for leading stakeholders from industry, infrastructure operators, agencies, and governments to collaborate on strengthening the security and resilience of Europe's infrastructure.

This year, we have a whole raft of partners supporting us, as part of 'CIP Week in Europe' who will each be holding a Workshop during the conference, they include:

- Crisis Communications Network Europe (CCNE) - CCNE Workshop - Critical Infrastructure Protection & Resilience Europe



- Confederation of European Security Services (CoESS) - COESS Workshop - Critical Infrastructure Protection & Resilience Europe
- ECSCI cluster (European Cluster for Security Critical Infrastructures) - ECSCI Workshop - Critical Infrastructure Protection & Resilience Europe
- ISACs (Information Sharing Analysis Centres) – Auto-ISAC; Aviation ISAC; Health ISAC; Space ISAC; Telco ISAC & FS-ISAC joining forces - ISACs Workshop - Critical Infrastructure Protection & Resilience Europe - and
- Africa Young People Support Centre (AYPSC) - AYPSC Workshop - Critical Infrastructure Protection & Resilience Europe.

Our partners and supporters play a pivotal role in shaping the work of IACIPP and in adding significant value to both the association and the CIPRE community. We look

forward to continuing these strong relationships and engaging with additional organisations and stakeholders who share our commitment to collaboration and resilience.

We are also looking ahead to the conference in Brussels and to celebrating CIPRE's 11th anniversary. Over the years, we hope we have contributed in some small but meaningful way to bringing together key decision makers and influencers, creating a space where experiences can be shared, industry peers can connect, and the latest technologies and solutions can be explored to support the protection and resilience of our Critical National Infrastructure.

John Donlon QPM FSyl
Chairman IACIPP

International Association of
CIP Professionals

Global Cybersecurity Partner / Platinum Sponsor:



Gold Sponsor:



Silver Sponsor:



CIP Week Event Partners:



Executive Sponsors:



critical infrastructure PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Sheraton Hotel Brussels Airport,
Belgium

www.cipre-expo.com

Co-Hosted by:



Preliminary Conference Programme Guide

Critical Infrastructure Protection and Resilience events bring together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing the nations critical infrastructure.

Gain greater understanding on the latest challenges, changing regulations and threats against Europe's critical infrastructure and critical entities, from over 50 international expert speakers.

Join us in Brussels, Belgium for CIP Week in Europe
Register online at www.cipre-expo.com/register

Global Cybersecurity Partner/
Platinum Sponsor:



Gold Sponsor:



Silver Sponsor:



Flagship Media
Partner:





International Association of
CIP Professionals



International Association of
CIP Professionals

critical infrastructure
PROTECTION AND
RESILIENCE NEWS



Leading the debate for securing Europe's critical infrastructure



20th-22nd October 2026

Brussels, Belgium

www.cipre-expo.com

Cyber and Physical Threats to Critical Infrastructure

Cyberattacks on critical infrastructure have evolved from potential threats to a persistent reality. Power plants, chemical facilities, and nuclear sites are increasingly targeted by malicious actors. A notable example is the 2015 Ukraine power outage, which affected 225,000 customers.

More recent incidents underscore the growing vulnerability of critical infrastructure. In 2023, a significant cyberattack disrupted critical services in a European nation, highlighting the potential for widespread disruption. Additionally, physical threats, such as drone attacks and sabotage, remain a concern.

The potential consequences of these attacks are far-reaching, encompassing loss of life, economic disruption, and significant infrastructure damage. The 2015 European floods serve as a stark reminder that natural disasters can exacerbate the impact of cyber and physical attacks, necessitating robust preparedness and planning at a European scale.

Strengthening European Infrastructure Protection

To address these evolving threats, the European Union has taken significant steps to enhance the protection of critical infrastructure. The European Commission's communication on Critical Infrastructure Protection provides a framework for prevention, preparedness, and response to attacks.

The European Programme for Critical Infrastructure Protection (EPCIP) is a key initiative that mandates Operator Security Plans for all designated European critical infrastructures. This program aims to improve the security posture of these vital assets against external threats.

Furthermore, the EU is developing a comprehensive policy on critical energy infrastructure, aligning with the EPCIP to bolster the resilience of the energy sector.

Given the escalating threat landscape, it is imperative to prioritize the protection of critical infrastructure. By investing in robust cybersecurity measures, fostering international cooperation, and promoting resilience, we can mitigate risks and safeguard the essential services that underpin our societies.

Critical Infrastructure Protection and Resilience Europe brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe. The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

The integrity of critical infrastructures and their reliable operation are vital for the well-being of the citizens and the functioning of the economy.

Understanding the Impact of Recent EU Cybersecurity Directives

The European Union has taken significant steps to bolster cybersecurity and critical infrastructure resilience. The Network and Information Systems Directive 2 (NIS2), which entered into force in 2023, updates the 2016 NIS Directive. This updated legislation expands the scope of cybersecurity requirements to new sectors and entities, including key digital service providers.

Key provisions of NIS2 include:

- Enhanced security measures: Businesses designated as operators of essential services must implement robust security measures to protect their systems and data.
- Mandatory incident reporting: Entities must report serious cybersecurity incidents to national authorities.
- Increased accountability: Key digital service providers are subject to specific security and notification obligations.

In addition to NIS2, the Directive on the Resilience of Critical

Entities was adopted in 2023 to strengthen the resilience of critical entities against a wide range of threats, such as natural disasters, cyberattacks, and terrorist attacks.

Key provisions of the Resilience of Critical Entities Directive include:

- Identification of critical entities: Member States must identify entities that are critical to society and the economy.
- Risk assessments and mitigation measures: Critical entities must conduct risk assessments and implement measures to enhance their resilience.
- Cross-border cooperation: The EU will facilitate cross-border cooperation and knowledge sharing among Member States and critical entities.

By understanding and complying with these directives, organizations can better protect themselves against cyber threats and contribute to a more resilient European Union.



Critical Infrastructure Protection Week *in Europe*

20th-22nd October 2026 - Brussels, Belgium



Critical Infrastructure Protection / Physical Security

Drone's, Insider threats, Vehicle Borne IED's, Suicide Bombers and Active Shooters are just some of the myriad of known threats currently facing CNI operators. Identifying ways of detecting, defeating and mitigating against those threats and building-in resilience are crucial organisation or CNI operator.

Combining CIIP/Cyber and Physical Security into one integrated strategy is not just desirable but crucial!

Why Attend?

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is organising the 3rd 'Critical Infrastructure Protection Week' in Europe as part of an initiative focused towards enhancing collaboration and cooperation amongst the industry.

Your attendance to Critical Infrastructure Protection and Resilience Europe will ensure you are up-to-date on the latest issues, policies and challenges facing the security of Europe's critical national infrastructure (CNI), as well as the latest updates on the implementation of the NIS2 and CER Directives.

You will also gain an insight in to what the future holds for Europe's, the collaboration and support between member nations required to ensure CNI is protected from future threats and how to better plan, coordinate and manage a disaster.

- High level conference with leading industry speakers and professionals
- Learn from experiences and challenges from the experts
- Gain insight into national and European CIP developments
- Constructive debate, educational opportunities and cooperation advocacy
- Share ideas and facilitate in valuable inter-agency cooperation
- Exhibition showcasing leading technologies and products
- Networking events and opportunities

For further information and details on how to register visit www.cipre-expo.com

Join us in Brussels, Belgium, in the heart of EU policy making, for CIP Week, Critical Infrastructure Protection and Resilience Europe and join the great debate on securing Europe's critical infrastructure.

Critical Information Infrastructure Protection / Cyber Security

With the ever increasing threat from cyber attacks on critical infrastructure, the information and data stored and used by CNI systems and operators can be more crucial than the system itself. CIIP is becoming ever more important as part of the cyber security strategy of an organisation or CNI operator.

Who Should Attend

Critical Infrastructure Protection and Resilience Europe is for:

- National and local government agencies responsible for national security and emergency/contingency planning
- Police and Security Agencies; Policy, Legal and Law Enforcement
- Civil Contingencies, National Security Agencies and Ministry Infrastructure Departments
- CNI Operators (CSO, CISO, Infrastructure Managers, Facilities Managers, Security Officers, Emergency Managers)
- Energy operators, grid, T&D, power generators
- Telecommunications and Mobile Operators
- Water and Utilities Suppliers
- Emergency Services, Emergency Managers and Operators
- Local Government
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- IT, Cyber Security and Information Managers
- Port Security Managers; Airport Security Managers; Transport Security Managers
- Engineers, Architects, Constructors and Landscape Designers; Civil Engineers
- Public Administrators and Managers
- Utility Providers (Energy, Communications, Water and Wastewater)
- Urban Planners and County Commissioners
- Transportation Managers and Planners
- Facility, Data and IT Managers
- Supply Chain Logistic Managers and Operators
- Banking and Financial institutions
- Data Centres
- NATO; Military; Border Officials
- International Corporations

HOW TO REGISTER

Online at www.cipre-expo.com/register

EARLY BIRD DISCOUNT - deadline 20th September 2026

Register yourself and your colleagues as conference delegates by 20th September 2026 and save with the Early Bird Discount.

Discounts for Members of Supporting Associations

If you are a member of one of the following trade associations, supporters of the Critical Infrastructure Protection & Resilience Europe, then you can benefit from a special discount rate:

- Europe's Distribution System Operators (E.DSO)
- Auto-ISAC; Health ISAC; Aviation ISAC; Space ISAC
- European Telecommunications ISAC (ETIS-ISAC)
- The European Network of Logistics Competence Centres (OPEN ENLoCC)
- The Centre for Interdisciplinary Research on Critical Infrastructure Security and Resilience (CRISR)
- European water services association (EurEau)
- Crisis Communications Network Europe (CCNE)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- Confederation of European Security Services (CoESS)
- European Cluster for Securing Critical Infrastructures (ECSCI)

Check the Registration Fees online at
www.cipre-expo.com/conference-fees

On-Site Registration Hours

Tuesday 20th October	1.00pm to 6.30pm
Wednesday 21st October	8.30am to 5.00pm
Thursday 22nd October	8.30am to 3.30pm





Critical Infrastructure Protection Week *in Europe*

20th-22nd October 2026 - Brussels, Belgium



International Association of
CIP Professionals

Schedule of Events

Tuesday 20th October 2026

1.30pm - 3.15pm - Joint Opening Keynote

3:15pm-4:00pm - Networking Coffee Break

4.00pm-5:30pm - Session 1: From Definition to Delivery: Governance, Methodology, and Practice

5:30pm - Networking Reception (in exhibition hall)

Wednesday 21st October 2026



TRACK ONE

9:00am-10:30am - Session 2a: Emerging Threats against CI/CE

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3a: Infrastructure Interdependencies and Cascading effects

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - Session 4a: Infrastructure Resilience Under Fire: Ukraine Case Study

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5a: Skills Gaps, Fragmentation Capabilities & Public-Private and Cross-Sector Coordination

TRACK TWO

9:00am-10:30am - Session 2b: Power & Energy Sector Symposium

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3b: Cybersecurity and Cyber Resilience Sector Symposium

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - Session 4b: Transport & Logistics Sector Symposium

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5b: Maritime and Subsea Infrastructure Sector Symposium

Thursday 22nd October 2026

TRACK TWO

9:00am-10:30am - Session 6b: Risk Mitigation, Resilience, Business Continuity Strategies

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7b: AI and Cyber in CI

12:30pm-2:00pm - Delegate Networking Lunch

2pm-3:30pm - Session 8: **Panel Discussion** - Systemic Risk and Uneven Resilience: Confronting Europe

3:30pm-4:00pm - Review, Discussion and Conference Closing

al Implementation of NIS2 and CER

TRACK THREE (WORKSHOPS)

9:00am-10:30am - Crisis Communications Network Europe (CCNE) Workshop

10:30am-11:00am - Networking Coffee Break

11:00am - 12:30pm - Confederation of European Security Services (CoESS) Workshop

12:30pm-2:00pm - Delegate Networking Lunch

2:00pm-3:30pm - AYPSC Africa Workshop

3:30pm-4:00pm - Networking Coffee Break

4:00pm - 5:30pm - Information Sharing & Analysis Centres (ISACs) Workshop

TRACK THREE (WORKSHOPS)

9:00am-10:30am - European Cluster of Securing Critical Infrastructures (ECSCI) Workshop - Resilience Stress Testing

10:30am-11:00am - Networking Coffee Break

11:00am - 1:00pm - Workshop TBC

Europe's Next Critical Infrastructure Shock

e

Partner Conferences / Workshops:



Exhibition Opening Hours

Tuesday 20th October	1.00pm to 6.30pm
Wednesday 21st October	8.30am to 5.00pm
Thursday 22nd October	8.30am to 3.30pm

On-Site Registration Hours

Monday 19th October	1.00pm to 5.00pm
Tuesday 20th October	8.30am to 6.30pm
Wednesday 21st October	8.30am to 5.00pm
Thursday 22nd October	8.30am to 3.30pm

20th-22nd October 2026

Brussels, Belgium

www.cipre-expo.com

Registration and Participation Fees

GOVERNMENT, PUBLIC SECTOR AND MILITARY: The Critical Infrastructure Protection & Resilience Europe is open and ideal for members of federal government, emergency management agencies, civil contingencies, emergency response and law enforcement or inter-governmental agencies, Homeland Security & Emergency Management Agencies, Fire, Police, INTERPOL, EUROPOL and associated Agencies and members (public and official) involved in the management and protection of critical national infrastructure.

OPERATORS OF CRITICAL NATIONAL INFRASTRUCTURE: The Conference is a must attend for direct employees, CSO, CISO's, security management and security personnel of critical infrastructure owner/operators.

COMMERCIAL ORGANIZATIONS: Industry companies, other organizations and research/Universities sending staff members to Critical Infrastructure Protection & Resilience Europe are also invited to purchase a conference pass.

Register online at www.cipre-expo.com/register

GOVERNMENT, PUBLIC SECTOR AND MILITARY

Individual Full Delegate

Paid before 20th September 2026 €195
Paid on or after 20th September 2026 €295

OPERATORS OF CRITICAL NATIONAL INFRASTRUCTURE

Individual Full Delegate

Paid before 20th September 2026 €195
Paid on or after 20th September 2026 €295

COMMERCIAL ORGANIZATIONS

Individual Full Delegate

Paid before 20th September 2026 €495
Paid on or after 20th September 2026 €695

Sponsor/Exhibitor Full Delegate).

Paid before 20th September 2026 €295
Paid on or after 20th September 2026 €395

Student/University/Research Full Delegate

Student ID will be required to be shown on
collection of pass €295

Delegate Fees include: 3 day participation, conference proceedings, keynote, workshops, networking reception, coffee breaks and 2 lunches. Also includes One Year Membership of International Association of CIP Professionals (IACIPP).

Register online at www.cipre-expo.com/register

Tuesday 20th October

Conference Programme

1:30pm-3:15pm - Joint Opening Keynote

Chair: John Donlon QPM, FSyl

International adviser on security intelligence

Floriana Sipala, Director for Internal Security (Directorate D) and Counter-Terrorism Coordinator, DG Home

Oleksandr Potii, Chairman of the State Service of Special Communications and Information Protection (SSSCIP)

Ricardo De Sousa Figueiredo, Cybersecurity Expert – Resilience of Critical Sectors Unit, ENISA

Habtamu Abie, Chairman, ECSCI Cluster

3:15pm-4:00pm - Networking Coffee Break

4:00pm-5:30pm - Plenary Session 1: From Definition to Delivery: Governance, Methodology, and Practical Implementation of NIS2 and CER

This session explores how the translation of policy into practice has developed under NIS2 and CER. There still appears to be a lack of understanding around who is responsible for identifying critical infrastructures in a transnational setting, who is responsible for its security and resilience and which actors are required to report incidents, particularly under the evolving NIS-2 and the CER Directive regimes. We will examine governance models, definitions, and practical methodologies for risk assessment, compliance, and reporting.

Chair: John Donlon QPM, FSyl

When 'Critical' Depends on Where You Stand: Infrastructure Governance Across Borders - Flavio Häner, Critical Infrastructure Protection, Canton Basel-Stadt, Government

Chasing Ghosts, Missing Threats: Securing Critical Entities in the Era of Hybrid Warfare - Alessandro Lazari, Fellow and Lecturer, University of Salento - Department of Engineering for Innovation

Compliant on Paper. Ready in Practice? - Catherine Piana, Director General, Confederation of European Security Services (CoESS)

Enhancing the resilience of critical entities - the need for integrated and systemic risk management - Fred Petit, Project Officer, European Commission JRC

Critical Infrastructure Governance and Protection: Perspectives from Across the OSCE Area - Daniel Golston, Associate Programme Officer, OSCE

5:30pm-7:30pm - Networking Reception (in Exhibition Hall)

20th-22nd October 2026

Brussels, Belgium

www.cipre-expo.com

TRACK ONE

9:00am-10:30am - Session 2a: Emerging Threats against CI/CE

Critical infrastructure faces increasingly complex and evolving threats. Cyberattacks are growing more sophisticated, terrorism remains a concern, and climate change is making natural disasters more unpredictable. New dangers such as drone attacks, misuse of artificial intelligence, evolving hybrid threats and state sponsored attacks further complicate the landscape. A key challenge is how to effectively identify, monitor, and understand these diverse and emerging threats.

Chair: John Donlon QPM, FSyl

Detecting Hybrid Campaigns Against Critical Infrastructure: A Cybersecurity-Informed Framework for Early Warning - Jonas Schmänk, Policy Assistant / Doctoral Researcher, European Commission, Joint Research Centre (JRC)

Changing Threats of Terrorism Against CI - Lina Kolesnikova, Director of European & International Affairs/Fellow, ICPEM

Emerging Cyber Threats - Senior Representative, ESET

Tracking the Typhoons: China's Cyber Operations Against Critical Infrastructure - Eugenio Benincasa, Senior Cybersecurity Researcher, Center for Security Studies (CSS) at ETH Zurich

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3a: Infrastructure Interdependencies and Cascading effects

Modern critical infrastructure is deeply interconnected, making it increasingly vulnerable to cascading failures. Disruptions in one sector—such as energy, transport, or communications—can rapidly propagate across systems, amplifying impacts and complicating response efforts. Understanding these interdependencies is essential for effective protection and resilience. This session explores how to identify systemic risks, model cascading effects, and strengthen cross-sector coordination to mitigate disruptions, enhance situational awareness, and ensure continuity of essential services in an increasingly complex threat landscape.

Chair: Alessandro Lazari

Resilient Critical Infrastructure Governance in Climate-Induced Urban Crises: Lessons from Dubai's Adaptive Model - Prof. Ehab Elhegawy, Head of the Department of Security Crisis Management, Dubai Police Academy

From Compliance to Consequence: Engineering "Even If" Resilience for Europe's Energy Systems - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory

Understanding Systemic Risk in Critical Infrastructures: A Semantic Approach to Cross-Sector Resilience - Antonella Calo, Expert Consultant, European Commission - Joint Research Centre

Know Your Adversary: Sharing Threat Actor Insights to Secure Telecom Infrastructure - Andrija Višić, Senior Community & Programme Manager, ETIS – European Telecommunications ISAC

Wednesday 21st October

TRACK TWO

9:00am-10:30am - Session 2b: Power & Energy Sector Symposium

Europe's power and energy sector—spanning oil, gas, and rapidly expanding renewables—remains fundamental to all critical infrastructure. In today's security climate, it faces escalating cyber and hybrid threats targeting IT, OT, and SCADA systems, alongside intensifying climate-driven disruptions. Ensuring resilience means anticipating attacks, reducing the impact of outages, and safeguarding interconnected grids. Strengthening Europe's energy networks is now a strategic priority to maintain stability, security, and continuity across essential services and economies.

Chair: Charles Esser, EDSO

Black Start Resilience - Energy Operator*

Cyber Challenges for the Grid and Operators - Energy Operator*

Martin Hromada, Vice Dean for International Relations / Researcher, Tomas Bata University in Zlín, Czech Republic

Beyond Prevention: Engineering Cyber Resilience for Europe's Energy Infrastructure - Antoine d'Haussey, VP OT Security Practice Lead International, Fortinet

Agahro Ono, Chief Executive Officer, ASCANO Integrated Services

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 3b: Cybersecurity and Cyber Resilience Sector Symposium

Cybersecurity for critical infrastructure has shifted from prevention alone to a broader focus on resilience. While strong defenses, threat detection, and response remain essential, today's threat landscape demands the ability to withstand, adapt to, and rapidly recover from cyber incidents. This session explores the nature of increasingly sophisticated and disruptive cyber threats to proactive strategies for ensuring business continuity, disaster recovery, and operational integrity, enabling vital services to remain secure, reliable, and functional, to meet NIS2 and DORA regulations.

Chair: John Donlon QPM, FSyl

Dr Victor Vevera, General Director, National Institute for Research and Development in Informatics, ICI Bucharest

Mitigating Cybersecurity Risks in Legacy Healthcare Systems: Policy, Technology, and Response Strategies for Critical Infrastructure - Angela Wells, Professor/Technologist, City U Seattle Washington

The Human Factor: Cyber Security Culture in European Critical Infrastructure - Laith Shahin, CEO & Founder, Secolve

Critical infrastructure under pressure in an evolving threat landscape - Andrew Lee, Vice President of Government Affairs, ESET

12:30pm - Delegate Networking Lunch

Wednesday 21st October

TRACK ONE

2:00pm-3:30pm - Session 4a: Infrastructure Resilience Under Fire: Ukraine Case Study

Lessons learned from Ukraine - the most advanced real-world laboratory for modern critical infrastructure resilience under sustained attack - where the country is witnessing constant coordinated attacks. Listen to Ukraine's experts tasked with keeping the lights on and goods moving. It's the only large-scale, prolonged test of critical infrastructure under continuous cyberattacks, physical strikes (from missiles and drones) and hybrid warfare.
Chair: John Donlon QPM, FSyl

Overview of Ukraine Critical Infrastructure Protection & Resilience System: Legal Framework & Further Developments

- Vasyl Ananyev, Head of Unit, Dept of CIP, SSCIP, Ukraine

Energy Infrastructure & Energy Supply Resilience: War-time Lesson - Dr Oleksandr Sukhodolia, Head of Dept of CI, Energy & Environmental Security, National Institute for Strategic Studies & Lead Consultant, Dept of CIP, SSCIP, Ukraine

Implementation of the State Concept of Engineering Protection of CI Facilities 'Fortress Country' - Artem Bilyk, Assistant Professor, Research Institute of Military Intelligence, Ukraine
Tymur Khromaiev, Deputy Commander of Separate Special Purpose Center, Armed Forces of Ukraine

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5a: Skills Gaps, Fragmentation Capabilities & Public-Private and Cross-Sector Coordination

Critical infrastructure resilience is increasingly constrained by workforce shortages and fragmented capabilities across sectors and borders. This session explores how skills gaps in cybersecurity, OT, and crisis management limit preparedness, and siloed operations hinder effective response. It will examine the urgent need for cross-sector coordination, improved information sharing, and aligned capability development. Attendees will gain practical insights into building a more integrated, skilled, and collaborative resilience ecosystem.
Chair: John Donlon QPM, FSyl

Pressuring the chain: a live tabletop exercise for stress-testing the Gold-Silver-Bronze command - Kim Covent, Advisor, Ghent Local Police

Transforming Landscapes: How UK Counter Terrorism Policing is Supporting Aviation Security - William Hunt, National Aviation Security Lead - National Counter-terrorism Security Office, National Counter-Terrorism Security Office - UK Counter-Terrorism Policing Headquarters

Next-Generation Models for Cross-Sector Coordination: Building an Operational Ecosystem for Infrastructure Resilience - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory)

A Strategic Framework for National and Critical Infrastructure Resilience in the Hybrid Threats Era - Abraham (Avi) Bachar, CEO, IsraTeam 98 Ltd

TRACK TWO

2:00pm-3:30pm - Session 4b: Transport & Logistics Sector Symposium

The transport (road, rail, air) and logistics sector is a cornerstone of critical infrastructure, enabling the movement of people, goods, and essential services. Increasing interconnectivity, digitalisation, and reliance on complex supply chains expose it to cyber, physical and hybrid threats. This session examines strategies to enhance resilience, protect key assets, and ensure continuity, focusing on risk management, cross-border coordination, and safeguarding operations against evolving threats in a dynamic global environment.
Chair: Catherine Piana

Developing Governance to Manage Security in Infrastructure Design Projects at Airports: Heathrow Case Study - Sarah Prew, Arup UK

David Nieto, Executive Director, Aviation ISAC

Faye Francy, Executive Director, Auto-ISAC

Peter Driessens, Head of Safety, Infrabel

Philip Van den Bosch, Senior Supply Chain Strategist and Rail Freight Expert, Lineas

3:30pm-4:15pm - Networking Coffee Break

4:15pm - 5:30pm - Session 5b: Maritime and Subsea Infrastructure Sector Symposium

Maritime and subsea infrastructure now face an intensified threat landscape, from hybrid and cyber attacks on ports, vessels, and undersea cables to rising geopolitical tensions and sabotage risks. As digitalisation expands vulnerabilities, protecting this sector requires integrated resilience strategies, including integrating physical security, cybersecurity, and operational continuity, alongside stronger international collaboration to protect global trade and connectivity.

Chair: Lina Kolesnikova

Resilience of the Maritime Critical Infrastructure in Belgium

- Eric Rummens, Advisor, Service Public Federal Mobilité et Transport (DG Navigation), Belgium

SAFEDigimar: Strengthening cybersecurity to build a more resilient port ecosystem

- Maarten Boot, Policy Advisor, FEPORT - Federation of European Private Port Companies and Terminals

SIDMETICS: The Mediterranean Hub for the Protection of Submarine Critical Infrastructures - Francisco Luis De Andrés Pérez, CEO, Ciso.es

Underwater Threats - CIP Water Frontier Expansion - Simon Goldsworthy, Global Business Development Manager, Forcys

20th-22nd October 2026

Brussels, Belgium

www.cipre-expo.com

Thursday 22nd October

TRACK ONE

9:00am-10:30am - Session 6a: Technologies to Detect and Protect

The latest technologies for detecting and predicting threats to critical national infrastructure span ground, land, underwater, space-based, and cyber domains, supported by advanced sensors and access control systems. Artificial intelligence increasingly enhances these capabilities by improving speed, accuracy, and cross-domain analysis of threat signals. New, developing systems and solutions enable earlier detection, better prediction, and stronger situational awareness across interconnected infrastructure systems.

Chair: Martin Hromada

Cryptographic Keys in Access Control Systems for Critical Infrastructure - Harish Rasiah, Sales Support Manager (Speaker will be Head of Sales or Product Manager), LEGIC Identsystems
Jose Ruiz Cristina, IndraMind Security Business Development Director Indra Group, Spain, IndraMind

From Drone Detection to Defensible Decisions: Lessons from Protecting Belgium's Critical Infrastructure - Gerrit Van Kerckhoven, Key Account Manager, Skeydrone
Martin Franke, Communications Manager, Euralarm

10.30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7a: Drones and UAS

Drones present a growing threat to critical infrastructure due to their accessibility, manoeuvrability, and payload capabilities, enabling surveillance, disruption, or delivery of explosives. However, they can also support infrastructure protection through monitoring and response applications. This session examines the evolving drone threat landscape, available countermeasures, and the dual-use role of drones in both challenging and enhancing critical infrastructure security and resilience.

Chair: Catherine Piana

Clogged Skies, Clogged Feeds: Drone Sightings and the Weaponisation of Information Disorder - Natasia Kalajdziovski, Senior Fusion Threat Intelligence Analyst, SecAlliance

Drones for Resilience & Surveillance - Ievgen Romanov, CEO, SkyDock

The Convergence of Physical and Aerial Threats: Protecting Critical Infrastructure from Drone-Delivered Attacks - Hollice Stone, President, Stone Security Engineering

Adapting to Drone Threats: Scalable Non-Disruptive, Non-Kinetic Counter-UAS Strategies for Critical Infrastructure Protection - Marco Harder, Sales Director, Benelux and Scandinavia, D-Fend Solutions

TRACK TWO

9:00am-10:30am - Session 6b: Risk Mitigation, Resilience, Business Continuity Strategies

Developing effective resilience strategies across the critical infrastructure community requires disciplined information sharing, strong preparedness, and robust risk mitigation and management. This session explores how organisations can identify, assess, and prioritise risks in a structured way, while reducing vulnerabilities and strengthening overall system resilience. It also examines how to embed continuity planning for potential disruptions or disasters, ensuring coordinated responses and support long-term operational stability across interconnected infrastructure systems.

Chair: John Donlon QPM, FSyl

Bridging Public Warning Systems and Critical Get risk wrong, get the response wrong - Chris Needham-Benne, Managing Director and Visiting Professor University College London, Needams1834

Risk Mitigation, Resilience, Business Continuity Strategies - Hugo Marynissen, Managing Partner,/Co-holder Chair of Crisis Governance, PM/Risk Crisis Change, University of Antwerp

Insider Risk Management in Critical Infrastructure: A Path to Resilience and Compliance - Dennis Bijker, CEO and Isa Steijn, Senior Adviser & Thought Leadership Lead, SignPost Six

The development of an effective PNT test framework to measure resilience in critical infrastructure - Eleftherios (Akis) Drosinos, PNT Solutions Architect, Keysight

How Europe's consulting engineering community supports infrastructure reduce risk across the infrastructure lifecycle - Sue Arundal, Director General, EFCA

10:30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7b: AI and Cyber in CI

AI plays a dual role in critical infrastructure cybersecurity, acting as both a defensive tool and a potential threat. It strengthens protection by improving threat detection, automating responses, and predicting attacks through advanced data analysis and anomaly detection. However, malicious actors can also exploit AI to develop more sophisticated attacks. We investigate how effective defence requires harnessing AI's benefits while managing its risks through strong security controls and continuous adaptation.

Chair: Alessandro Lazari

AI-driven cybersecurity for critical private wireless networks - Filippo Gaggioli, Head of Security Product Introduction, Nokia Cloud and Network Services

Safety by Design: AI-Assisted Threat Detection That Protects Industrial Operations - Ali Mohammed, Senior OT/ICS Cybersecurity Engineer, Resilience

Alexandru Georgescu, ICI Bucharest, Romania

Isolated AI Systems and Secure Orchestration Strategies for Strengthening Critical Infrastructure Protection and Resilience - Roger Sanz Gonzalez, European Projects Manager. R&D, UI1 University

12:30pm - Delegate Networking Lunch

Thursday 22nd October

2:00pm-3:30pm - Plenary Session 8:

**PANEL DISCUSSION - Systemic Risk and Uneven Resilience: Confronting Europe's
Next Critical Infrastructure Shock**

In this panel discussion, we will examine Europe's current preparedness for systemic infrastructure disruption, exploring the persistent resilience gaps across Member States and critical entities, and its fragmented capabilities against the evolving hybrid threat landscape. In this engaging discussion, we will assess how current NIS2 and CER implementation is addressing these challenges, where governments and operators are succeeding and falling short, and what must change to influence future frameworks such as NIS3 and CER2, ensuring more consistent, cross-border, and operationally effective resilience across Europe.

Moderator: John Donlon QPM, FSyl,

Sebastian Serwiak, Policy Office, European Commission

Catherine Piana, Secretary General, CoESS

Vasyl Ananyev, Head of Unit, Dept of CIP, SSCIP, Ukraine

Esmeralda Kazia, Chief Technology Officer, Albanian Power Corporation

Ricardo De Sousa Figueiredo, Cybersecurity Expert – Resilience of Critical Sectors Unit, ENISA

3.30pm - Conference Close

John Donlon QPM, FSyl, Conference Chairman

Register online at www.cipre-expo.com/register

Early Bird Deadline - 20th September 2026





Crisis Communications Network Europe (CCNE) Workshop



WORKSHOP: FROM INCIDENT TO COMMUNICATION: CRISIS COMMUNICATIONS FOR CRITICAL INFRASTRUCTURE

WEDNESDAY 21ST OCTOBER - 9.00AM-10.30AM

Effective crisis communications are an essential part of organisational resilience and crisis management, as recognised by the Critical Entities Resilience (CER) Directive. In this interactive workshop, the Crisis Communications Network Europe (CCNE) will explore how communications support the response to incidents affecting critical infrastructure, from tactical communications in the field to strategic engagement with stakeholders, authorities, and the public. Working through a realistic scenario, participants will examine challenges, exchange experiences, and explore practical methodologies, best practices, and lessons

learned. The session is intended for anyone responsible for, or interested in, crisis communications and resilience, and aims to provide practical insights that can be applied across a wide range of organisations and sectors.

Speakers:

- Stijn Pieters, Managing Partner PM • Risk Crisis Change
- Robbert Meulemeester, Senior Advisor & Trainer PM • Risk Crisis Change

Register online at www.cipre-expo.com/register



Confederation of European Security Services (CoESS) Workshop

WORKSHOP: THE ROLE OF PRIVATE SECURITY IN SAFEGUARDING CRITICAL INFRASTRUCTURE IN THE CONTEXT OF EUROPE'S PREPAREDNESS UNION

WEDNESDAY 21ST OCTOBER - 11.00AM-12.30PM

Europe has entered a new era of preparedness. As the threat environment becomes more complex, the challenge is no longer simply whether Europe has the capabilities to protect its critical infrastructure, but whether those capabilities can be effectively organised and mobilised when they are needed most. This session will explore what we call the Preparedness Gap: the gap between the capabilities and experience that already exist across society and those that are effectively recognised, connected and integrated into preparedness planning before a crisis occurs.

Private security provides a compelling illustration. Every day, private security professionals protect critical infrastructure and essential services, monitor sensitive sites, assess and respond to incidents, support business continuity and contribute to situational awareness. Yet these capabilities are not always systematically embedded in emergency planning, information-sharing arrangements, joint exercises and crisis governance. How can Europe move from ad hoc cooperation during crises towards Preparedness by Design, where roles, relationships and operational interfaces are established beforehand?

Co-hosted by the Confederation of European Security Services (CoESS), the session will bring together European policymakers, corporate security leaders and private security practitioners to examine how existing capabilities can be better recognised, integrated and governed as part of Europe's preparedness architecture.

Hans Das, Deputy Director-General and Chief Operations Officer

at DG ECHO, European Commission, will open the session with a keynote, followed by Marc Léoutre, Deputy Head of Unit at DG HOME D2. The panel discussion will bring together Jean-Philippe Bérillon, Chairman of the CoESS Critical Infrastructure Protection Committee and Member of the CoESS Board of Directors; Yvan De Mesmaeker, Secretary General of the European Corporate Security Association (ECSA); and Karolien Verbeiren, Country President of Securitas Belgium NV.

Together, they will consider a central question: how do we ensure that the capabilities Europe already possesses become part of preparedness before, not during, the next crisis? The session will be moderated by Catherine Piana, Director General of CoESS."

Speakers:

- Catherine Piana, Director General, CoESS Confederation of European Security Services, Belgium
- Hans Das, Deputy Director-General and Chief Operations Officer, DG ECHO
- Marc Leoutre, Deputy Head of Unit DG HOME - Unit D2 Unit D2: Counter-Terrorism, Anti-Radicalisation, Critical Infrastructure
- Jean-Philippe Bérillon, Chair of the CoESS Critical Infrastructure Protection Committee
- Yvan De Mesmaeker, Director General of ECSA (European Corporate Security Association)
- Karolien Verbeiren, Country President of Securitas, Belgium

Register online at www.cipre-expo.com/register



African Young People Support Centre / African Smart Cities Innovation Foundation Workshop

WORKSHOP: AFRICA–EUROPE COOPERATION FOR CRITICAL INFRASTRUCTURE RESILIENCE

NIGERIA AT THE FOREFRONT: EMERGING VOICES, RISING TOGETHER YOUTH POWERING REGIONAL INFRASTRUCTURE PROTECTION

WEDNESDAY 21ST OCTOBER - 2.00PM-3.30PM

As the international communities continue to confront diverse threats to critical infrastructure—from cyber disruptions and climate shocks to energy insecurity and health crises—a more inclusive and collaborative response is urgently needed. Historically under-represented, Africa’s young people are now stepping into leadership roles, developing innovative solutions, and advocating for more secure, inclusive systems.

Nigeria, as Africa’s most populous country and economic powerhouse, is uniquely positioned to lead on young people-driven resilience efforts. This side event, held on the margins of Critical Infrastructure Protection & Resilience Europe (CIPRE), offers a platform to elevate African young people voices and foster cross-continental dialogue and cooperation with European counterparts.

Objectives

- * To highlight Nigeria’s role as a leader in young people engagement on critical infrastructure protection in Africa.
- * To facilitate dialogue between African and European people and institutional stakeholders on resilience-building.
- * To share real-life young people-led innovations and approaches from Nigeria and other African countries.
- * To lay the groundwork for a formal young people platform focused on infrastructure protection cooperation between Africa and Europe.

Target Participants

- * African and European young people and industry leaders and innovators
- * Policymakers and government officials from both continents
- * Infrastructure and cybersecurity professionals
- * Representatives of the AU, EU, UN, and development partners
- * Academic and civil society actors

AGENDA

Opening Session : Welcome address & keynote: “From Abuja to Brussels: Why Young People Must Lead the Next Era of Infrastructure Resilience”

Part 1 : “Young People at the Crossroads: Africa–Europe Partnerships for Infrastructure Resilience” Panel discussion highlighting opportunities, challenges, and success stories.

Part 2 : “Nigeria at the Forefront: Young People Powering Regional Infrastructure Protection” Dialogue on Nigeria’s national leadership, innovation, and young people participation in resilience planning.

Part 3 : “NextGen Solutions: Young People Innovations for Critical Infrastructure” Young people-led pitches and showcases of real-world projects.

Part 4 : “Co-Designing Young People-Led Africa–Europe Resilience Platforms” Interactive roundtable generating practical recommendations and frameworks.

Closing Remarks : Summarising outcomes and proposing the launch of the Young People for Infrastructure Resilience Africa–Europe Network (YIR-AEN).

Expected Outcomes

- * Strategic recommendations for enhancing young people roles in transnational infrastructure security
- * Strengthened Africa–Europe partnerships focused on inclusive resilience planning
- * Visibility for Nigerian young people leadership in global policy circles
- * Momentum for establishing a permanent young people dialogue platform

Participation in this Workshop is complimentary and open for delegates to CIP Week and CIPRE.

SPEAKERS:

- Aigbe Osagie Daniel, Systems Security Engineer, Major Solar
- How aviation, immigration, and tourism infrastructure across Africa intersect with critical infrastructure protection
- Omotola James, Travel, Tourism & Immigration Advisory Specialist
- Paul Igbinere, Executive Director, African Young People Support Centre
- Ehimwenma Idemudia, IT Specialist & Data Science & Analytics Professional, iChase Outsourcing

Register online at www.cipre-expo.com/register



Information Sharing & Analysis Centres (ISACs) Workshop



WORKSHOP: CYBER RESILIENCE WITHOUT BORDERS: LESSONS FROM THE ISAC COMMUNITY IN COLLECTIVE DEFENSE

WEDNESDAY 21ST OCTOBER - 4.00PM-5.30PM

Cyber resilience depends on trusted collaboration that transcends organizational, sector, and national boundaries. Information Sharing and Analysis Centers (ISACs) have become a cornerstone of collective defense by enabling members to exchange timely threat intelligence, operational experiences, vulnerabilities, mitigation strategies, and lessons learned within trusted communities.

This interactive session brings together leaders from multiple sector-specific ISACs—including automotive, aviation, financial services, healthcare, and space—to explore how trusted information sharing strengthens resilience across Europe's critical infrastructure. Participants will gain insight into the origins and evolution of the global ISAC model, the role of the European Council of ISACs in fostering cross-sector collaboration, and the current cyber threat landscape impacting European critical infrastructure.

The session will conclude with a discussion on the essential partnerships between ISACs and public-sector organizations, including ENISA and the European Commission, highlighting how industry and government work together to enhance situational awareness, improve coordinated response, and advance collective cyber defense across Europe.

Speakers:

- Faye Francy, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)
- David Nieto, Executive Director, Aviation ISAC
- Rebecca Huffee, Senior Consultant Secure Space Systems, CGI, UK
- Vasileios Mingos, European Operations Director Health-ISAC
- Andrija Višić, Senior Community & Programme Manager, ETIS – European Telecommunications ISAC

Register online at www.cipre-expo.com/register





European Cluster for Securing Critical Infrastructures (ECSCI) Workshop - Resilience Stress Testing

WORKSHOP: RESILIENCE STRESS TESTING AS A CRITICAL ELEMENT OF IMPLEMENTATION OF THE EUROPEAN DIRECTIVE ON CRITICAL ENTITY RESILIENCE (CER DIRECTIVE)

THURSDAY 22ND OCTOBER - 9.00AM-10.30PM

The European Directive on Critical Entity Resilience (CER Directive), has entered into force in 2023, became mandatory in the EU in 2024, and, by now, widely adopted as national law and included in national strategies for enhancing resilience of critical entities/infrastructures (CIs). Out of estimated more than 15,000 CIs concerned by CER Directive, several hundred of them are assumed to involve possible cross-border impacts. These cross-border cases will certainly increase the need for resilience benchmarking and stress testing, as metrics and processes for quantifying cross-functional and cross-border interdependencies still need to be developed and be agreed upon.

The workshop will, therefore, focus on ongoing efforts to develop the relevant, consensus-based guidelines, including those related to the common stress testing framework, agreed stress testing procedures, resilience measurement and its use in stress testing, and providing and promoting samples of good stress testing practice in the relevant stress testing application cases/scenarios.

Examples of the real-life scenarios are abundantly provided in the current geopolitical and economic risk landscape, such as extreme threats (XTs), polycrises and issues related to the critical supply chains. Networks and associations can and should play a pivotal role in both the co-development and acceptance of the above guidelines. The workshop will, therefore, explore practical approaches for co-designing, agreeing upon and aligning of the common resilience stress testing guidelines, focussing on the EU level, where the European Cluster for Securing Critical Infrastructures (ECSCI, <https://www.ecsci.eu>), which brings together 71 projects focused on critical infrastructure resilience, has already established itself as a key stakeholder actor in this context. This workshop will be part of and contribute to this broader ECSCI context.

The Workshop is organized in cooperation with IARA – International Association for Resilience Analysis.

Tentative list of topics to be considered for the short presentations & and the panel:

1. EU: Current status and scientific and technical challenges of the CER implementation
2. Implementation at the National level (Germany, France, Italy...)
3. Role of cluster, networks and associations at the EU level
4. How the EU resilience stress testing setup could look like (ENISA, NIS2, CER, DRS ...)?
5. Relevant international efforts (ISO, OECD, IARA, UK, USA, Australia, China, Canada...)
6. Discussion
 - How to ensure that all the eleven CER sectors of the CIs achieve the same maturity as the cyber/IT sector?
 - What kind of support (actions, supporting documents, events...) is needed for successful resilience stress testing?
 - What kind of interaction is needed? Interaction with the Commission? What kind interaction with regulatory and implementation authorities (e.g., the CER Competent Authorities in the EU)?
 - What can be shared as good practice internationally (US, Canada, Australia...)?
 - Relevant issues for particular stakeholders' groups? Insurance? PPP?
 - Other relevant issues?

Organizers:

- Prof. Aleksandar JOVANOVIĆ, CEO, Steinbeis European Risk & Resilience Institute (EU-VRi), Germany
- Dr. Habtamu ABIE, ECSCI Chair, Chief Research Scientist, Norwegian Computing Center (NRS), Norway
- Prof. Igor LINKOV, Founding President, International Association for Resilience Analysis (IARA), USA

Register online at www.cipre-expo.com/register



Critical Infrastructure Protection Week *in Europe*

20th-22nd October 2026 - Brussels, Belgium



Networking Reception

**Tuesday 20th October
5.30pm - 7:30pm**

We invite you to join us at the end of the day for the Networking Reception, which will see the CNI security industry management professionals and delegates gather for a more informal reception.

With the opportunity to meet colleagues and peers you can build relationships with senior government, agency and industry officials in a relaxed and friendly atmosphere.

The Networking Reception is free to attend and will take place in the Exhibition Hall at CIP Week / CIPRE.

Open to the delegates of Critical Infrastructure Protection & Resilience Europe and CIP Week.

We look forward to welcoming you.

*Built in security - increasing security without turning
our public buildings and spaces into fortresses*

Event Venue & Accommodation

Sheraton Brussels Airport Hotel

Brussels National Airport

Brussels, 1930

Belgium

www.marriott.com/en-us/hotels/brusi-sheraton-brussels-airport-hotel/overview/

For more details visit:

www.cipre-expo.com/venue



Steps away from the main gate at Brussels Airport, the Sheraton offers sound-proofed rooms with flat-screen TV. The hotel includes a gym, 24-hour room service and a lobby computer terminal. Guests can benefit from the Sheraton Club Lounge experience. The design guest rooms at Sheraton Brussels Airport Hotel & Conference Center have Sheraton Sleep Experience Bed. Each of the air-conditioned rooms

also benefit from a mini-bar. Brussels Express Train Station is located underneath the hotel and offers direct links into the center of Brussels. The Atomium is a 15-minute car journey from the hotel and the NATO Headquarters are only 5 minutes away by car. Gullivers Restaurant serves anything from a breakfast buffet to a chic à-la-carte dinner and cocktails. Guests can also enjoy a traditional Belgian beer at the bar.

**Accommodation Information and Booking link can be found at
www.cipre-expo.com/accommodation**

Direct hotel booking link: www.cipre-expo.com/hotel-booking



Critical Infrastructure Protection Week *in Europe*

20th-22nd October 2026 - Brussels, Belgium



The IACIPP is a global fraternal association of CIP professionals, dedicated to sharing ideas, information, experiences, technology and best practise, with the express purpose of making the world a safer place.

The association is open to critical infrastructure operators and government agencies, including site managers, security officers, government agency officials and policy makers. The purpose is to share ideas, information, experiences, technology and best practise.

The Association, although very young in its journey, is clear in what it is seeking to achieve. The creation of a network of like minded people who have the knowledge, experience, skill and determination to get involved in the development and sharing of good practice and innovation in order to continue to contribute to the reduction of vulnerabilities and seek to increase the resilience of Critical Infrastructure and Information.

A great new 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 currently FREE to qualifying individuals - see www.cip-association.org/join for more details.



www.cip-association.org

For further details visit www.cip-association.org or email info@cip-association.org.

The IACIPP initial 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

The Association also aims to:

- Provide proactive thought leadership in the domain of critical infrastructure security and resilience.
- Help set the agenda for discussions in infrastructure security and resilience
- Promote and encourage the sharing of information, knowledge and experience that will enhance security.
- To filter, collect, collate and co-ordinate information and data sharing.
- Identify and promote new technologies that can enhance security and resilience.
- Share information with members about the changing threat landscape
- Share information, ideas and knowledge to promote best practice
- Educate operators and provide industry standards
- Act as a Liaison between operators, government, intergovernmental bodies
- Make available surveys and research
- Provide the mechanism for liaison between operators and industry

Join today at www.cip-association.org/join

Critical Infrastructure Protection Week *in Europe*

20th-22nd October 2026 - Brussels, Belgium



International Association of
CIP Professionals

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to CIP Week and Critical Infrastructure Protection & Resilience Europe 2026.

Co-Hosted by:



Global Cybersecurity Partner / Platinum Sponsor:



Gold Sponsor:



Silver Sponsor:



CIP Week Event Partners:



Executive Sponsors:



Supporting Organisations:



Flagship Media Partner:



Media Supporters:





We look forward to welcoming you to Brussels, Belgium for the next gathering of the international critical infrastructure protection and resilience community.

critical infrastructure
PROTECTION AND RESILIENCE EUROPE

20th-22nd October 2026
Brussels, Belgium

www.cipre-expo.com



Register online at www.cipre-expo.com/register

Early Bird Deadline - 20th September 2026

Digital Sovereignty in Critical National Infrastructure – from Governance Principle to Architectural Control



What events in 2026 have shown us so far is that, for boards and operators of critical national infrastructure, digital sovereignty is no longer simply a geopolitical consideration, but a governance and resilience imperative. Energy grids, water utilities, transport systems, industrial plants, telecommunications networks and financial infrastructures underpin essential services and increasingly depend on interconnected digital and cyber-physical systems.

In this context, sovereignty is not simply about vendor nationality or where technology is manufactured. The more fundamental question is: when connectivity is disrupted, geopolitical tensions affect supply chains, regulations collide or external services become unavailable, can the organisation continue to operate securely and lawfully? If critical

operational authority depends on factors outside the operator's control, sovereignty may not be guaranteed.

Digital sovereignty is therefore not only a matter of policy. It must become technically enforceable through architecture. In practice, this means designing integrated IT/OT/CPS security architectures in which critical enforcement remains under operator and jurisdictional control, rather than



Antoine D'Haussey, Regional VP OT Practice Lead International

creating mandatory external dependencies. Cryptographic keys and their lifecycle must remain under appropriate operator control; critical security functions must continue operating securely in offline or degraded conditions; and operational data must remain subject to the operator's chosen jurisdictional and governance requirements.

Importantly, sovereignty does not mean isolation from global technology or innovation. It means retaining the ability to exercise operational authority when dependencies are disrupted. These architectural choices strengthen resilience while ensuring that responsibility remains with those ultimately accountable for safety, continuity of essential services and public trust.

Human risk: why enterprise security must go beyond cybersecurity



by Jean-Philippe Berillon, Chair of the CoESS Critical Infrastructure Protection Committee, founder of Brenus Conseil

For a long time, human risk in cybersecurity has been mainly addressed through awareness programs: learning how to recognize phishing attempts, protect passwords, and follow information security policies. This approach is too narrow today.

The human factor is now a transversal risk for the organization—at the intersection

of cybersecurity, physical security, human resources, risk management, and business operations.

A human error can lead to a cyber incident. But an employee can also become the victim of manipulation, be targeted in a social engineering attack, be recruited or exploited by a malicious actor, or—intentionally

or unintentionally—cause a leak of sensitive information.

Therefore, a governance question arises: who should truly own human risk?

Moving Beyond an IT-Centric View of Human Risk

Traditionally, cybersecurity has been attached to the IT department—or the CIO's

organization—which naturally leads to viewing cyber risk as an extension of IT risk.

This approach has a fundamental limitation: IT is responsible for designing, operating, and evolving information systems, while the CISO is responsible for managing the risk associated with their security.

The CISO must be able to define security requirements, assess risks, monitor their level of control, and, when necessary, challenge IT. When the CISO is hierarchically part of IT, this ability to challenge can be weakened by excessive proximity between the operator of the system and the manager of the associated risk.

Cybersecurity should therefore not be seen solely as a technical function. It is above all a risk management and protection function.

Human risk illustrates this particularly well. The vulnerability of an employee does not stop at the boundaries of the information system. A credential can be compromised digitally, but the person behind that credential may first have been identified, approached, manipulated or physically targeted.

This is where the convergence between cyber and corporate security becomes essential.

The Chief Security Officer at the Heart of the Framework

Corporate Security already covers a significant portion of people-related risks: insider threat, malicious intent, espionage, fraud, social engineering, executive protection, site security, physical access control, and third-



party risks. Cybersecurity now complements this protection chain.

The same individual may be the target of a social engineering operation, used to obtain credentials or access, manipulated to introduce a threat into the information system, involved in a confidential data leak, the victim of fraud or espionage, or even constitute an insider threat.

These situations cannot be effectively addressed by artificially separating cyber, physical security, and human risk.

The Chief Security Officer can therefore play a structuring role in an enterprise-wide security approach, ensuring coherence across these dimensions.

But this framework should not be limited to internal Corporate Security. Private security providers can also be an important operational component of this ecosystem.

Security officers, mobile patrols, reception teams, control-room operators and other contracted personnel are often present at

the physical interface between the organization, its employees, visitors, contractors and external stakeholders.

They can therefore contribute to the early detection of situations that may have a human-risk dimension: unusual behaviour, attempts to circumvent procedures, suspicious approaches, unauthorized access attempts, tailgating, social engineering at physical entry points, or other anomalies.

The role of private security is not to investigate cyber threats or replace the CISO. Its value lies in providing an additional operational layer of vigilance, protection and information.

CISO and Chief Security Officer: Complementary Responsibilities

This does not mean that the Chief Security Officer replaces the CISO. On the contrary, the two roles are complementary.

The CISO retains full authority and expertise over cybersecurity: cyber strategy, security architecture and requirements, vulnerability management, identity and access



security, security monitoring and incident response, data protection, threat intelligence, cyber risk management, and compliance.

The Chief Security Officer, for their part, brings a broader view of the threat landscape: physical security, insider threat, executive protection, espionage and economic intelligence, malicious intent, fraud, social engineering, site security, crisis management, and organizational resilience.

Private security providers operate primarily at the implementation and operational level. Depending on their mandate, they may provide physical protection, access control, monitoring, patrols, alarm response, security operations centre capabilities, visitor management, event security and first-line incident reporting.

Their effectiveness depends on clear governance, appropriate training and well-defined escalation procedures.

The challenge is not to merge these areas of expertise, but to place them within a common governance framework, in which

information can move across cyber, physical and human-risk domains.

From Security Provider to Security Partner

One of the most important changes concerns the relationship between the organization and its private security providers. If private security is considered solely as a manpower provider responsible for guarding premises, much of its potential contribution to human-risk management remains unused.

A more mature approach treats the security provider as an operational security partner.

This means involving private security in relevant preparedness activities, risk assessments, scenario development and exercises. It also means ensuring that security personnel understand the organization's critical assets, sensitive populations, escalation processes and the broader security context in which they operate.

For example, a security officer at a sensitive facility may be among the first people to observe an individual attempting to obtain

information from an employee, bypass an access-control procedure or gain unauthorized physical access.

That observation may appear minor when considered in isolation. Combined with information from cybersecurity, HR, fraud prevention or threat intelligence teams, however, it may become a significant indicator.

The objective is therefore to establish structured channels for reporting and escalation, rather than relying solely on informal communication.

The Security Officer as an Additional Human Sensor

Technology provides organizations with increasingly sophisticated capabilities for detecting anomalous activity. Yet the human factor remains critical.

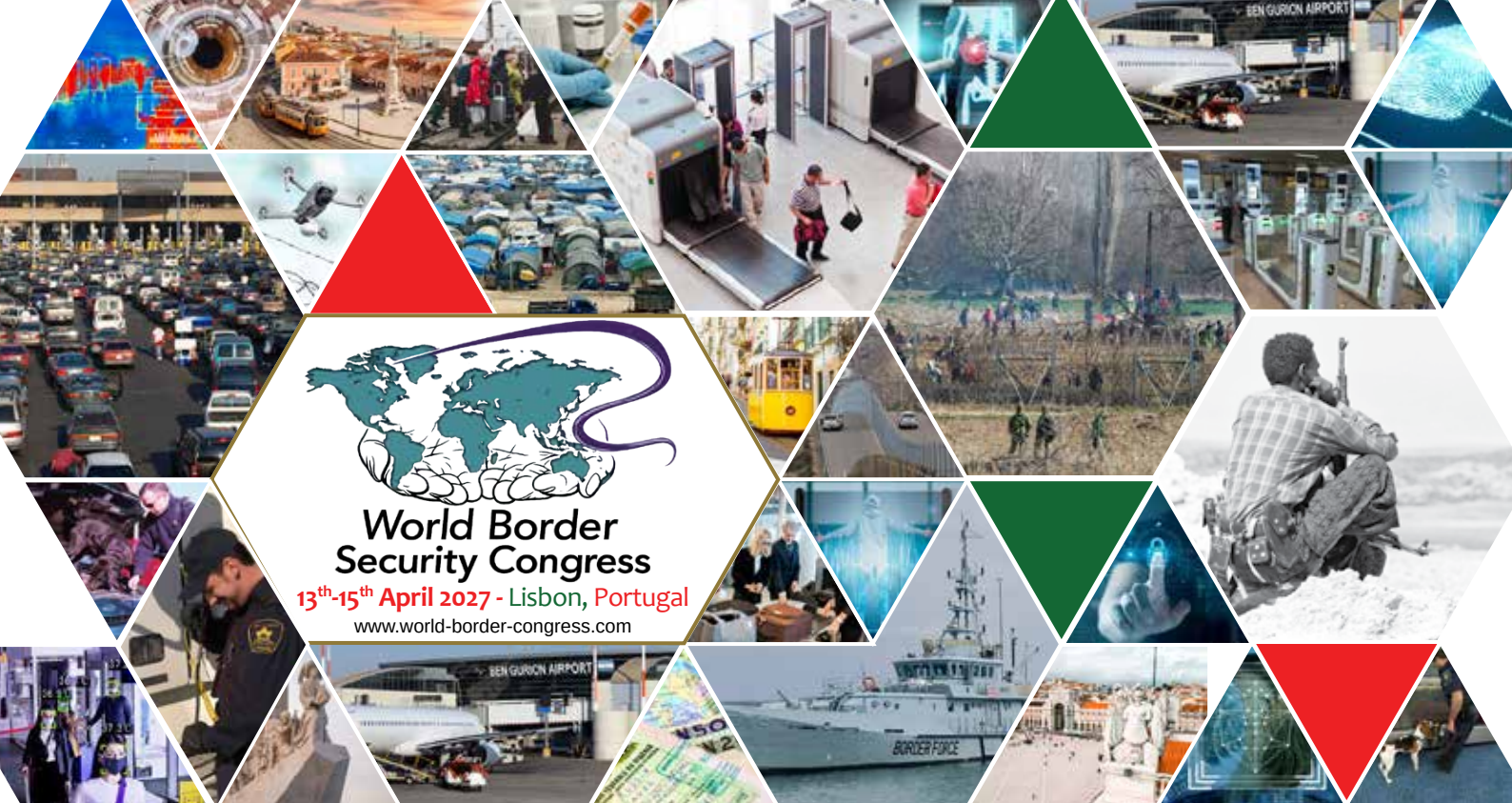
A security officer may notice behavioural changes, unusual interactions or inconsistencies that automated systems cannot easily interpret.

This makes private security personnel an additional human sensor network within the enterprise.

However, this capability must be used responsibly. Security personnel should not be expected to make psychological diagnoses, profile individuals or collect information beyond their legitimate mandate.

Their role is to observe, identify, report and escalate, according to clearly defined procedures.

The quality of the information they provide depends on training. Security officers need to understand what constitutes an



Transforming Border Management Strategies Through Co-operation and Technology

SAVE THE DATES

Portugal's border security is shaped by its geography and role within the Schengen Area, placing responsibility on protecting the EU's external frontier. Since the dissolution of the SEF, the border security function is coordinated by the Sistema de Seguranca Interna (Internal Security System) and implemented by the Polícia de Segurança Pública (PSP) and Guarda Nacional Republicana (GNR).

Administrative overload and legal migration pressure remains Portugal's main challenges, but the country relies on maritime and airport surveillance rather than land borders. Its Atlantic coastline presents monitoring challenges, particularly for irregular migration routes and drug trafficking. The country faces growing inflows of irregular migrants from Africa, Brazil, and South Asia, creating administrative strain in processing visas, asylum claims, and residency permits, leading to backlogs and delays.

Migration has become more contentious recently, with pressure to tighten rules after years of relatively open policies. At the same time, labour shortages mean Portugal still depends heavily on migrant workers.

Portugal is not unique in its border management challenges and must strengthen surveillance, streamline bureaucracy, and enhance EU cooperation while maintaining its rights-based migration approach.

The World Border Security Congress is a high level 3 day event that will discuss and debate current and future policies, implementation issues and challenges as well as new and developing technologies that contribute towards safe and secure border and migration management.

Join us in Lisbon, Portugal on 13th-15th April 2027 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

Co-hosted by:



SISTEMA DE SEGURANÇA INTERNA



To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

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

Jerome Merite
France
E: j.callumerite@gmail.com
T: +33 (0) 6 11 27 10 53

Supported by:

Media Partners:



unusual event, what information is relevant, when an observation should be escalated, and to whom it should be reported.

In this context, training should increasingly include elements of social engineering, insider threat awareness, suspicious behaviour reporting and the relationship between physical and cyber security.

An Integrated and Transversal Governance Model

In organizations where Corporate Security holds overall responsibility for enterprise security, placing the CISO under the Chief Security Officer can be a particularly coherent model.

It positions cybersecurity as a protection and risk management function rather than simply an IT component. This model positions cybersecurity as a risk protection and management function, while maintaining close collaboration with IT, HR, Risk Management, Legal/Compliance, and the Business Units—and, where relevant, trusted private security partners.

The governance model should nevertheless preserve clear boundaries. Private security providers should have access only to the information necessary to perform their responsibilities. Sensitive cyber intelligence, personal data and confidential employee information should not automatically be shared with contracted personnel.

The principle should be need-to-know, purpose limitation and controlled escalation.

Integration does not mean unrestricted information sharing. It means ensuring that

relevant information reaches the appropriate people at the appropriate time.

Shared responsibility, but clear Accountability

Saying that human risk concerns the whole organization does not mean everyone is equally responsible. We must distinguish between ownership, contribution, and accountability.

This clarification is essential: responsibility is shared, but ownership must remain identifiable.

This model positions cybersecurity as a risk protection and management function, while maintaining close collaboration with IT, HR, Risk Management, Legal/Compliance, and the Business.

Toward a true human risk management approach

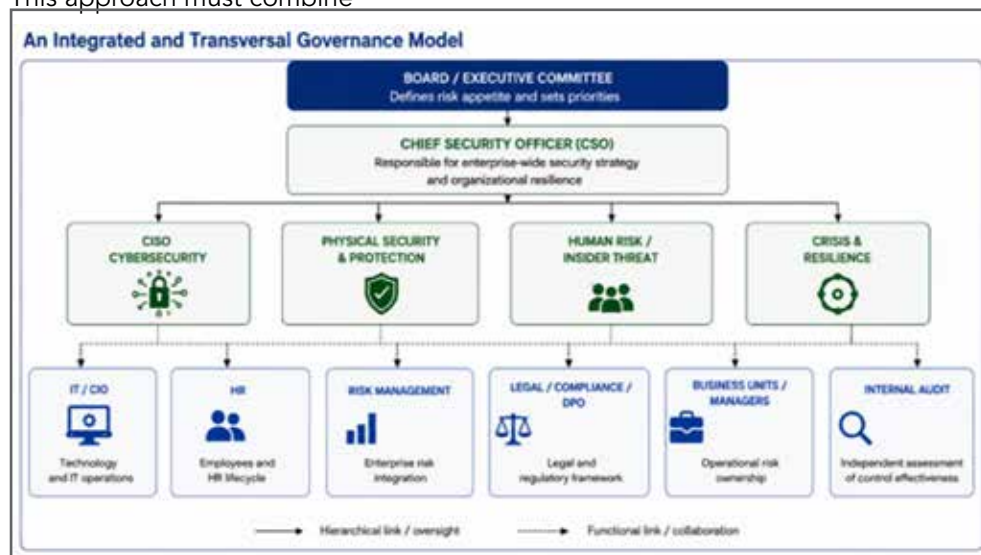
The challenge goes far beyond awareness. It is about building a genuine Human Risk Management capability to identify exposed populations, risky behaviours, threat scenarios, and potential impacts on the organization.

This approach must combine

multiple functions: cyber, security, HR, risk, private security and business context, to answer better questions:

- Which populations are most exposed?
- Which employees have access to the most sensitive assets?
- Which physical locations represent elevated human-risk exposure?
- What social engineering scenarios pose the greatest threat?
- How can we detect and address insider threats?
- How can physical security observations contribute to the broader threat picture?
- How do we manage the departure of someone with critical access or information?
- How do we combine cyber, physical, and behavioural signals while respecting privacy and legal frameworks?
- How do private security teams escalate relevant observations without creating unnecessary surveillance?
- How do we measure the real reduction of human risk?

This approach also creates an



opportunity to improve security exercises. For example, an organization could simulate a scenario in which an employee is approached physically by an external actor, subsequently targeted through social engineering, and ultimately used to obtain access to sensitive information.

Such a scenario would require cooperation between Corporate Security, cybersecurity, HR, management and private security.

The objective would not simply be to test whether the employee recognizes the phishing attempt. It would be to test whether the organization can connect the different signals, identify the threat and coordinate an appropriate response.

This is where integrated human-risk management becomes significantly more powerful than traditional awareness programs.

Building a security ecosystem

The convergence of cyber, physical and human risk also changes the way organizations should think about their security ecosystem.

Our organizations are often siloed by design, with specialized teams kept separated sometimes to segregate responsibilities, but above all to control decision-making. In a crisis, these boundaries become obstacles. Attackers, however, move at the speed of the network, respecting neither the organizational chart nor the chain of approval.

Internal security functions cannot operate in isolation. They increasingly depend on external partners: private security

companies, technology providers, specialist investigators, crisis-management firms and other security service providers.

The quality of this ecosystem depends on how well these actors are integrated into the organization's governance model.

Private security should therefore be considered not merely as an outsourced function but, where appropriate, as an extension of the organization's operational security capability.

This requires clear contractual requirements, common standards, training, performance indicators, incident-reporting mechanisms and regular exercises.

It also requires a mature relationship in which the security provider is encouraged to report weaknesses and emerging risks rather than simply demonstrate contractual compliance.

The ultimate objective is to create a shared security culture extending from the Executive Committee to the employee, and from the CISO and Chief Security Officer to the security officer at the entrance of a critical site.

Conclusion

Human risk is no longer just an IT issue. It is an enterprise risk—one that must be managed as such.

The CISO must remain independent and retain cyber expertise. IT must remain focused on operating technology. HR must own the human dimension and the employee lifecycle. Business leaders must manage operational risks.

And when Corporate Security holds overall responsibility for enterprise security, the Chief

Security Officer can legitimately become the anchor of this integrated governance model.

Within this framework, private security has an important but clearly defined role. Its strength lies in its proximity to the physical environment, its continuous operational presence, its ability to detect anomalies and its capacity to provide immediate protection and first-line reporting.

The key is to move beyond a transactional client-provider relationship toward a structured security partnership, while maintaining clear accountability, appropriate information boundaries and respect for privacy and legal requirements.

The real transformation consists in moving from a logic of "Cybersecurity Awareness" to a logic of "Enterprise Human Risk Management."

And this transformation requires the organization to recognise that the human-risk chain does not begin and end with an employee sitting behind a computer.

It extends from the digital identity to the physical person, from the workstation to the workplace, from the employee to the contractor, and from the internal security function to the private security professional on the ground.

Human risk is not an IT problem. It is an enterprise risk—and managing it effectively requires the integration of cyber, physical, human and operational security into one coherent protection framework.

A Tale of Two SOC's: Insights From Two Red Team Assessments



The Cybersecurity and Infrastructure Security Agency (CISA) conducted simultaneous red team assessments at two organizations and observed different defensive outcomes. In both environments, the red team achieved full domain compromise and accessed sensitive business systems (SBSs) and cloud resources. Organization A failed to detect or contain the activity, but Organization B rapidly identified

initial compromise attempts, isolated affected systems, and forced the red team into an assume breach model.

This advisory details the red team's activity and organizations' defensive actions, offering lessons learned and mitigations to help critical infrastructure organizations strengthen detection, response, and protections in IT, cloud, and operational technology (OT) environments.

Introduction

The Cybersecurity and Infrastructure Security Agency's (CISA's) red team simulates real-world malicious cyber operations to assess an organization's ability to detect, investigate, and respond to malicious cyber activity. Emulating cyber threat actor tradecraft, the red team attempts to gain and maintain persistent access to an organization's network and sensitive

business systems (SBSs) while avoiding detection.

CISA conducted two simultaneous red team assessments using similar tradecraft but observed different defensive responses. In one organization (Organization A), the team gained initial access to multiple workstations, gained elevated privileges over the domain, and moved laterally to SBSs and cloud resources undetected. In the second organization (Organization B), network defenders quickly detected the initial compromise and quarantined the affected systems.

Because Organization B detected the initial compromise, the red team moved to an assume breach model, where Organization B trusted agents (TAs) provided access to a host that replicated the level of access the red team would have had if defenders had not detected their activity. From there, the red team escalated privileges and moved laterally to SBSs, cloud resources, and a bastion host in the OT demilitarized zone (DMZ), where defenders again detected activity and isolated the system.

In coordination with the assessed organizations, CISA is releasing this Cybersecurity Advisory to describe the red team's activity and the organization's defensive responses and to share lessons learned that critical infrastructure organizations can use to strengthen their IT, cloud, and OT cybersecurity posture.

Overview

CISA is authorized—upon request—to provide analyses, expertise, and other technical assistance to critical infrastructure owners and operators and to provide operational and

timely technical assistance to federal and non-federal entities, with respect to cybersecurity risks. CISA conducted two concurrent red team assessments: one at a Government Services and Facilities Sector organization (Organization A), and one at a Water and Wastewater Systems Sector organization (Organization B).

During CISA's red team assessments, the red team simulates malicious cyber operations to assess an organization's threat detection and response capabilities. The red team attempts to gain and maintain persistent access to an organization's enterprise network, avoid detection, evade defenses, and access SBSs (applications, data stores, or infrastructure components where compromise would materially impact the organization's operations, finances, or customer data) selected by the organization. For the assessments described in this advisory, the team also attempted to gain access to cloud resources and to demonstrate their ability to access Organization B's OT systems without actually doing so.

Organization A

Red Team Cyber Threat Activity

Initial Access and Active Directory Discovery

During reconnaissance, CISA's red team identified a web application with default credentials for multiple built-in user accounts that allowed the team to send emails from an internal email address. The team used the internal email address to send phishing emails and gained initial access to four workstations.

From the workstations, the red

team leveraged a modified BloodHound¹ collector, customized to avoid static endpoint detection and response (EDR) signatures, to query and scrape Active Directory (AD) information. This information included AD users, computers, groups, access control lists, organizational units, and group policy objects (GPOs). The team found that one compromised workstation had the default Machine Account Quota (MAQ) of 10, allowing unprivileged users to add up to 10 computer accounts to the domain.

The red team also queried the organization's Active Directory Certificate Service (ADCS) certificate templates. Misconfigured ADCS templates are common and can allow low-privileged accounts to request a certificate on behalf of other users and computers, including highly privileged accounts. The team identified multiple templates with an ESC1 misconfiguration, which allows any user to request certificates for all users and computer accounts (see scenario ESC1 in SpecterOp's Certified Pre-Owned: Abusing Active Directory Certificate Services). The red team exploited the misconfigured MAQ to create a machine account and then exploited a misconfigured ADCS template to request a certificate for the newly created machine account. They could then obtain certificates for any user account, providing means for lateral movement.

Post Exploitation: Privilege Escalation and Lateral Movement

Sensitive Business Systems

After the red team gained elevated privileges over the domain, they



began post-exploitation activities and attempted to access SBSs. To access the SBSs, the team needed to identify their network location and security controls.

The team's plan to achieve SBS access included the following steps:

1. Use previously acquired AD data to identify users and groups related to the SBS.
2. Query system center configuration manager (SCCM) servers to enumerate user-device relationships and identify the workstations assigned to each user.
3. Move laterally from the SCCM server to the target users' workstations.
4. Find credential material on the target user's workstation to access the SBS.
5. Verify administrative access to the SBS would allow compromise of the availability, integrity, and/or confidentiality of the system and its data.

For each SBS, the red team used similar discovery and initial access techniques but unique credential retrieval methods.

For SBS 1, a database, the team located cleartext credentials on an administrative user's workstation providing access to the system. For SBS 2, also a database, the red team searched the targeted user's workstations for connections.json and product-preferences.xml files for a Structured Query Language (SQL) developer tool. The team decrypted these files to obtain the cleartext password to the database. For SBS 3, an automated processing system, the red team acquired long-lived static Amazon Web Service (AWS) identity and access management (IAM) user credentials saved in configuration files in targeted users' home directories. These credentials do not expire because the organization had not configured credential expiration or rotation.

For SBS 2 and 3, the red team expanded access beyond users' physical workstations to include their virtual desktops, which limited their access to the active, interactive sessions held by users. While virtual workstations add security controls, such as segmenting networks of sensitive systems to only allow virtual hosts,

they are generally synchronized with a root drive of the distributed file system (DFS). The red team compromised the root DFS drive, granting them access to local files of all users' virtual desktops, regardless of the existence of an active session. This allowed the team to quickly search for cloud configuration files containing credentials and database connection files for thousands of users.

The red team obtained administrative access to all targeted SBSs without defensive intervention by proxying tools through compromised workstations and using the collected credentials.

Microsoft Entra Systems

After compromising the target SBSs, the red team attempted to compromise Organization A's Microsoft cloud environment by compromising Organization A's Microsoft Entra ID (formerly Azure AD) through applications. The team targeted Entra ID applications with Application permissions, which allow applications to access data without user consent (compared to Delegated permissions, which allow applications to access data with user consent). By compromising an application that had elevated Application permissions, the red team would gain the same permissions as the application because these applications operate outside the scope of traditional conditional access policies (CAPs) that provide controls for user access and activity.

Note: Microsoft's Conditional Access for workload identities extends traditional CAPs to service principals (SPs) used by applications and governs

Application permissions by allowing organizations to broadly apply access policies to applications. Implementing Conditional Access for workload identities would have protected against red team exploiting use of Application permissions; however, the red team never observed an organization using Conditional Access for workload identities.

The team compromised applications and used their permissions by:

1. Enumerating the organization's cloud resources using the publicly available tools, including AzureHound2 and ROADrecon,3 to gather information about applications, their permissions, and their owners .
2. Identifying applications with elevated permissions to the Microsoft Graph Resource application programming interface (API), including the following:
 - a) Mail.Read – Read Outlook emails.
 - b) Mail.ReadWrite – Read and write Outlook emails.
 - c) Chat.Read.All – Access Teams messages.
 - d) Files.Read.All – Access OneDrive.
 - e) Application.ReadWrite.All – Add Client Secrets to any application or SP.
 - f) AppRoleAssignment.ReadWrite.All – Lets an SP grant itself powerful Graph application permissions such as Chat.Read.All or RoleManagement.ReadWrite.Directory.
3. Identifying the owner of an application with Mail.ReadWrite permissions.



4. Moving laterally to the owner's machine.
5. Obtaining access to the user's primary refresh token (PRT).
 - a) A PRT is a secure artifact specifically issued to Microsoft first-party token brokers to enable single sign-on (SSO) across the applications used on those devices. For more information about PRT, see Microsoft's Understanding Primary Refresh Token (PRT) in Microsoft Entra ID.
6. Using the PRT to request access and refresh tokens for the targeted application's owner.
 - a) Access tokens are short-lived tokens issued by Entra ID that grant a client permission to access specific resources or APIs on behalf of a user.
 - b) Refresh tokens are longer-lived tokens issued by Entra ID that allow a client to silently request new access tokens without requiring the user to sign in again.
7. Using the access token to add a new client secret to the target application.
 - a) A client secret is a confidential string used by the application

to authenticate itself to Entra ID during token requests.

8. Using the new client secret to request a new access token for the target application.
9. Impersonating the application by using the access token to retrieve and review target emails via the Microsoft Graph API.

This allowed the red team to review security operations center (SOC) staff emails to see if SOC staff were aware of the compromise.

Organization A's Response

The organization did not respond effectively to red team activity. The red team observed this during their engagement by accessing SOC personnel emails and moving laterally to SOC workstations where they captured screenshots, used keyloggers, and retrieved Microsoft Teams messages.

The red team observed that the SOC received medium- and low-severity EDR alerts related to the red team activity but did not respond to them. Thousands of false positive alerts corresponding to normal business operations, many with a higher severity, obscured the alerts triggered by red team activity.



Organizational silos further hindered detection and response. The organization had multiple SOC's and multiple EDR solutions. Staff did not communicate with staff from other SOC's or have visibility on their detection tools. SOC staff and system owners also did not communicate with each other.

This led to SOC staff not actioning alerts from red team activity. For example, red team members noted chat exchanges regarding an SCCM in which defenders tried and failed to identify the system owner, its function, and its typical use. The SOC team eventually flagged the alert as a false positive.

The red team believes this was because the SOC staff lacked standard operating procedures for escalating alerts and had limited personnel authority.

Organization B

Red Team Cyber Threat Activity

Initial Access

The CISA red team gained initial access to Organization B's environment through a spearphishing campaign. The team gathered email addresses from

public websites and sent phishing emails that eventually led to three users clicking on a malicious link, giving the red team access to three workstations.

Each payload execution generated a medium-severity alert: "An executable file loaded an unexpected DLL file." SOC staff triaged these alerts and manually isolated all three workstations within 10, 2, and 20 minutes. This effectively terminated the team's command and control (C2) communications with the workstations. Before staff isolated one workstation, the red team enumerated Organization B's domain's AD structure by executing various Lightweight Directory Access Protocol (LDAP) queries through the callback. The data gathered included all users, groups, computers, domains, GPO, and subsequent relationships for the entire domain.

Because the defenders removed their initial foothold, the red team switched to an assume breach model. Organization B's TAs (organization IT staff who knew of the assessment and were in contact with the red team) executed a

red-team-provided payload on a designated internal host. This host was associated with a standard user account with no administrative privileges, replicating the same level of access the red team would have maintained if Organization B's defenders had not detected them.

Domain Compromise

With persistent access to the internal network, the red team searched for ways to escalate their privileges over the domain to facilitate lateral movement and access SBSs. The red team used the assume breach account to query the MAQ attribute of Organization B's domain and discovered that all domain users were able to add accounts to the domain.

The red team created a new machine account with a hostname designed to resemble a legitimate host. The creation of the machine account provided the red team with a domain account and a password that they controlled. This allowed them to execute standalone tools from a red-team-controlled Linux workstation. The tool's traffic was proxied through the assume breach host, circumventing restrictions imposed by host-based EDR.

The red team did not identify any escalation paths from the AD data; however, enumeration of SCCM distribution points led to the discovery of an XML file with cleartext credentials for a domain service account. AD data showed that the newly acquired service account had outbound object control over almost 1,000 accounts within the domain due to its group membership. Most notably, the service account had AllExtendedRights permission over

a domain controller, which enabled the team to conduct a resource-based constrained delegation attack, granting them DCSync privileges and the ability to obtain AD account credentials. The team used these credentials throughout the remainder of their assessment to access servers and workstations. One of the first accounts the red team DCSynced was the krbtgt account, which a malicious cyber actor could use to forge Golden Tickets that allow for impersonation of any user in Organization B's domain.

Post Exploitation

Sensitive Business Systems

The TAs provided the names of two SBSs, one of which the red team successfully compromised. To do this, the team reviewed previously collected BloodHound data and identified a user account with access to an SBS web server that allowed Kerberos authentication. Because the red team had already compromised the on-premises (on-prem) AD environment, they could impersonate this user to access the server.

The team:

1. Used DCSync to acquire the user's AES256 password hash.
2. Used the password hash to request a Kerberos ticket-granting ticket (TGT) for the user.
3. Used the TGT to request a Kerberos service ticket [T1558] for the web server's service principal name (SPN).

After requesting the Kerberos service ticket, the red team imported it into a Windows virtual machine (VM) on their infrastructure. The red team configured their VM to proxy



any traffic to Organization B's network through a SOCKS proxy that tunneled traffic through a compromised host.

Operational Technology Network

The red team wanted to gain visibility of the OT network and identify OT network subnets. To do this, they first identified an IT workstation with Remote Desktop Protocol (RDP) files, including a file named ics-[redacted]-org, signifying that the user likely had remote access to the OT network. The red team identified that the workstation had remote access to a bastion host. A bastion host—sometimes referred to as a jump box or jump server—is a specialized, highly secured system (often a server or dedicated workstation) that serves as the sole access point between a network segment (such as an internal IT network) and a protected internal network (like an OT environment).

The red team gained access to this bastion host using File Transfer Protocol (FTP) credentials to log in over Secure Shell (SSH). At this point, they had visibility over the OT network.

They attempted to gain a C2 session on the server by dropping several payload files on the host and executing them. However, the callback never reached red team infrastructure because the host blocked outbound internet connections. The payload execution triggered an alert that led SOC staff to quarantine the host.

Microsoft Entra Systems

The red team attempted to access Organization B's cloud-based Entra ID infrastructure to find a way to move from on-prem AD to the cloud. Organization B had a hybrid environment, and user credentials automatically synchronized between on-prem AD and cloud Entra ID. Given this, the red team looked for the on-prem server responsible for synchronization.

Entra ID Connect (formerly Azure AD Connect) sets up an on-prem account with the prefix MSOL_ to synchronize credentials with Entra ID. The red team used the open source tool ADConnectDump4 to obtain cleartext credentials for the on-prem Microsoft Online (MSOL) account and the Entra ID account Sync_[redacted]. With cleartext



credentials for Sync_[redacted], the red team logged into the Azure portal. Sync_[redacted] was not intended for interactive logins and, in this case, did not have multifactor authentication (MFA) enabled. However, the red team used this account to obtain access tokens for use with AzureHound and ROADrecon to gather Entra ID data for Organization B's tenant.

Note: The red team obtained cleartext MSOL credentials and logged into the Azure portal because MSOL accounts used to have a large number of permissions; Microsoft has since removed these permissions. See Microsoft's Action required: MSOnline and AzureAD PowerShell retirement - 2025 info and resources and Important update: Deprecation of Azure AD PowerShell and MSOnline PowerShell modules for more information.

The interactive login from Sync_[redacted] triggered an automated alert from Microsoft, which sent the information to Organization B's SOC staff, who then blocked the suspicious activity.

The red team identified a computer account containing AZURESSO in its name, located in the on-prem AD environment. This account is part of the Seamless SSO implementation and allows users to use Kerberos tickets as the first step in authenticating to Entra ID. To abuse Seamless SSO, the red team acquired encrypted credentials of a target user via DCSync and then used the Rubeus "asktgs" module to request service tickets used for SSO. The red team imported the service tickets to their workstation and proxied their traffic through Organization B's network using a SOCKS proxy. This allowed them to browse to <https://portal.azure.com>, while using legitimate Kerberos tickets, and the traffic appeared to originate from a trusted IP address.

This approach allowed the red team to gain access to Entra ID as any user synced to AD without the user's cleartext password. However, they could only use Kerberos tickets for the first phase of the sign-in process. If a user was set up to use MFA, then Entra ID would prompt the red team for a second factor during the sign-in

process. Therefore, the red team was only able to log into any Entra ID account that did not have MFA enabled, which seemed limited to service accounts. They reviewed the previously obtained Entra ID data and looked for applications that had excessive permissions and were accessible to AD-synced service accounts.

The red team identified an application that had permission to read, write, and send emails for all users within Organization B's tenant. The application was owned by an AD-Synced account that was disabled in AD. Using a compromised host in the on-prem environment, they re-enabled this account, DCSynced its credentials, and used the AES256 hash to request Kerberos tickets. The red team used the tickets to authenticate to Entra ID and were then able to add a client secret to the application. This gave them the ability to retrieve the emails of every user within Organization B's environment from the public internet.

Organization B's Response

Organization B quickly triaged and responded to alerts after the red team gained initial access, effectively terminating the team's C2 communications with the workstations and leading the red team to move to an assume breach model. These actions demonstrated a mature, proactive security posture and helped prevent wider compromise.

When the red team gained access to a bastion host in the OT DMZ, Organization B had defensive controls that blocked outbound connections to red team infrastructure, and SOC staff quickly

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-asspociation.org/help2protect - Promo Code: 7UATQW7M

triaged and responded to an alert by isolating the host.

When the red team logged into the organization's Azure portal via a compromised account, it triggered an automated alert from Microsoft, which led the staff to block the suspicious account. In addition, Organization B had custom detections Entra ID Risky User Alerts for "Unfamiliar sign-in properties" and "Suspicious API traffic" that alerted to the AzureHound user agent and to accounts exceeding predefined request thresholds to the Microsoft Graph API.

See Table 1 for Organization B's defensive measures and associated response.

Despite these strengths, Organization B had areas for improvement. The red team was eventually able to access Entra ID through a computer account that was part of the organization's Seamless SSO implementation. The account did not have MFA and had overly permissive application permissions, indicating the need for more mature cloud security processes.

Additionally, Organization B had excessive permissions and misconfigurations in AD and service accounts, which the red team leveraged for privilege escalation. This highlights the importance of regular audits and strict enforcement of least privilege

principles. Organization B could improve credential hygiene, as the red team found credentials for OT systems stored in plaintext on jump servers. Finally, while segmentation and egress controls were effective, ongoing review and tightening of IT/OT connectivity and access architectures would reduce opportunities for lateral movement.

Lessons Learned

The red team identified lessons learned based on each organization's response. Organization A and Organization B contrasted significantly in their ability to quickly identify and respond to red team activity. However, similar gaps in both organizations contributed to the red team's compromise of their cloud systems.

Untuned Detection Tools Lead to Missed Threats

Organization A did not tune their detection tools to reduce alert noise, leading to an unmanageable level of alerts for SOC staff to review and action. The same red team activity that triggered alerts and action for Organization B led to no response for Organization A because SOC staff did not identify the activity as potentially malicious amid the overwhelming volume of alerts. Organization B had an established baseline and a fine-tuned alert system, allowing defenders to effectively filter out routine business activity and false positives. As a result, anomalies stood out, enabling the SOC staff to quickly detect and respond to red team activity.

Without well-defined baselines and alert filtering, false positives and routine alerts overwhelm

Table 1. Red Team Activity and Organization B SOC Response

Red Team Activity	Defensive Measure	SOC Response	Outcome
C2 payload executed on a workstation.	Payload execution generated a medium-severity alert.	Staff quarantined workstation; staff analyzed and reimaged before putting workstation back online.	Red team lost access to a workstation.
C2 payload executed on a second workstation.	Payload execution generated a medium-severity alert.	Staff quarantined workstation; staff analyzed and reimaged before putting workstation back online.	Red team lost access to a workstation.
C2 payload executed on a third workstation.	Payload execution generated a medium-severity alert.	Staff quarantined workstation; staff analyzed and reimaged before putting workstation back online.	Red team lost access to a workstation.
C2 payload executed on bastion host in the OT DMZ.	Payload execution generated alerts.	Staff quarantined the host.	Red team lost access to the host.
Used compromised Entra ID account to log into Azure.	Automated alert from Microsoft.	Staff blocked the account.	Red team compromised a different account and accessed Entra ID by abusing Seamless SSO.

defenders, obscuring real threats. Organizations that tune alerts to highlight anomalies and filter out normal business activity enable defenders to focus on genuine incidents and respond rapidly.

Organizational Silos and Bureaucratic Hurdles Prevent Effective Incident Response

In Organization A, lack of communication and visibility created by organizational silos (among multiple SOC teams and between SOC staff and system owners) hindered effective incident response, resulting in missed opportunities for identification of a major breach.

Bureaucratic barriers arose because SOC staff managed systems without understanding their authorities as responsibilities and authorities varied across network segments. They had no escalation procedures and so defaulted to a “wait and see” approach.

In contrast, Organization B empowered its defenders to act decisively. Staff quickly triaged alerts, investigated root causes, identified misconfigurations, and coordinated remediation with engineering.

Detection tools are only as effective as the people, processes, and procedures supporting them. SOC staff should not operate in silos and should have clear authority unhindered by bureaucracy to effectively contain and resolve incidents.

Organizations Underestimate Risks in Cloud Environments

Both organizations underestimated the risks associated with cloud environments. They granted excessive permissions to cloud



applications, allowing the red team to access cloud systems. They also lacked fully mature, defined processes for detecting and remediating compromise of cloud environments, allowing the red team to maintain access to cloud resources.

Use of Long-Lived User Identity and Access Management Credentials

Organization A used long-lived static IAM user credentials that were set to never expire. If a malicious actor obtains them, they will have all the user permissions, potentially enabling persistent, unrestricted access to the cloud environment.

Excessive Permissions

Both organizations lacked Conditional Access for workload identities. This feature extends Conditional Access beyond user accounts, covering non-human identities, such as applications. It allows organizations to broadly apply access policies to applications that control how and when the application is used to access resources. Instead, both organizations used broad

application permissions for most apps, which the team was able to exploit for access to the environment. In both organizations, the team was able to exploit excessive permissions to read emails.

Lack of Mature Remediation Processes for Tokens

Both organizations lacked processes for revoking compromised access/refresh tokens. Without a well-defined, efficient process for remediating and revoking access/refresh tokens following a cloud compromise, malicious cyber actors evicted from on-prem environments may still leverage cloud access to regain entry. Organizations should establish mature procedures to detect and remediate compromises of cloud environments to prevent malicious cyber actors from reestablishing access.

Energy Department Announces \$500 Million To Secure America's Critical Mineral and Battery Supply Chains

The U.S. Department of Energy's (DOE) Office of Critical Minerals and Energy Innovation (CMEI) announced \$500 million for seven selected projects to expand critical mineral and material processing, battery manufacturing, and recycling capacity in the United States. In accordance with President Trump's Executive Order, Unleashing American Energy, the selected projects advance the President's agenda to strengthen America's domestic critical minerals and materials supply chains, reduce reliance on foreign sources, bolster national security, and advance American energy dominance.

"For too long, America has depended on foreign actors for critical materials essential to modern life that underpin our economy, energy security, and national security," said U.S. Secretary of Energy Chris Wright. "President



Trump is reversing that dependence by securing our critical supply chains, unleashing American industry, and bringing critical materials production and processing back to the United States."

"DOE is taking decisive action to secure the critical supply chains

necessary to power our nation," said Assistant Secretary of Energy Audrey Robertson. "These projects underscore DOE's commitment to driving innovation, reducing reliance on foreign sources, and promoting American energy dominance."

This is the third round of funding from DOE's Battery Materials Processing and Battery Manufacturing and Recycling programs, which support battery materials processing, recycling, and manufacturing projects. These include demonstration projects, construction of commercial-scale facilities, and retrofitting or retooling existing facilities.

Critical minerals and materials are essential to American industry, energy production, and national security. Expanding domestic capacity will help ensure the resources America needs are processed, manufactured, and recycled in the United States.

Progress to Strengthen Energy Reliability in Puerto Rico

The U.S. Department of Energy (DOE) renewed two emergency orders to support continued improvements to Puerto Rico's electric grid as the island faces rising energy demand and the ongoing 2026 hurricane season. Building on previous actions in 2025 and 2026, the renewed emergency orders authorize the Puerto Rico Electric Power Authority (PREPA) to dispatch generation units essential for maintaining critical generation capacity, while continuing vegetation management to reduce outages, strengthen long-term grid reliability, and minimize the risk of blackouts.

"The Department of Energy will continue advancing the

modernization of Puerto Rico's electric grid to build a more affordable, reliable, and secure energy system for hardworking American families and businesses," said U.S. Secretary of Energy Chris Wright. "Renewing these orders ensures critical work moves forward, urgent reliability changes are addressed, and Puerto Rico's grid is ready to withstand rising energy demand. Thanks to President Trump, these efforts are delivering real, lasting progress for Puerto Rico."

The emergency orders help ensure the continued delivery of electricity to Puerto Ricans amid unforeseen conditions. The orders also address vegetation management issues near

power lines. Falling tree limbs or brush during Puerto Rico's frequent storms and high winds can damage transmission lines, cause widespread outages, and potentially cause wildfires.

"During the last 19 months, thanks to the partnership and support of President Trump and Secretary Wright, we have made measurable progress to strengthen Puerto Rico's electric system. The Department of Energy's Section 202(c) orders have been an essential component of that work, providing the emergency authorities needed to restore or refurbish close to 1,600 megawatts of generation capacity since they were first issued in May 2025.

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



Beyond the Perimeter: Why Critical Infrastructure Must Become Airspace-Aware



By Nele Coghe, Head of Marketing, SkeyDrone

Critical infrastructure operators have long focused on securing their facilities from threats approaching by land or through cyberspace. Fences, surveillance cameras, access control systems, cybersecurity platforms, and incident response procedures form the foundation of most security strategies. Yet a rapidly growing threat vector continues

to challenge these traditional approaches: the low-altitude airspace above critical assets.

As drones become more accessible, affordable, and sophisticated, they are opening up new possibilities, but at the same time creating risks that many critical infrastructure operators are not yet prepared to manage.

With drone-related incidents on the rise, airports, ports, energy sites, chemical facilities, financial institutions, government administration and digital infrastructure providers need to reassess how they approach security and resilience. The threat landscape no longer stops at the fence line; it now extends into the airspace above.

A Growing Threat Above Critical Assets

Recent incidents demonstrate that drone activity around sensitive sites is no longer theoretical. Unauthorised drones have been reported above nuclear facilities, chemical plants, airports, and military installations, raising concerns about security, operational continuity, and public safety. These incidents highlight a broader trend: drones are increasingly being used in ways that expose vulnerabilities in traditional protection measures.

The range of potential use cases is broad. Drones can be used for intelligence, surveillance and reconnaissance, gathering data that may later be exploited for sabotage or intrusion. They can deliver payloads into restricted areas, bypassing traditional access controls entirely. They can disrupt operations by interfering with communications or navigation systems. In more advanced scenarios, they may even be used as vectors for cyber intrusion, targeting wireless networks or connected infrastructure.

Drones Are Also Driving Operational Value

While much attention is focused on security concerns, it would be a mistake to view drones solely as a threat. In fact, many critical infrastructure operators are already benefiting from drone technology in their daily operations.

Drones have become valuable tools for asset inspection, maintenance planning, surveying, and operational monitoring. They enable organisations to inspect infrastructure that is difficult, costly, or dangerous to access manually,



such as power lines, pipelines, rail networks, industrial facilities, and large-scale energy assets. By providing rapid, detailed insights, drones help organisations improve efficiency while reducing operational disruption.

They also play an increasingly important role during emergencies and crisis situations. Real-time aerial views can support incident managers, enhance situational awareness, and accelerate decision-making during rapidly evolving events. For many organisations, drones have become an essential operational capability rather than a future innovation.

This dual reality creates a unique challenge. Organisations must simultaneously enable legitimate drone operations while protecting themselves against unauthorised or malicious drone activity. Effective security therefore depends not only on detecting drones, but also on understanding which operations are authorised and which may represent a threat.

CER Raise the Stakes

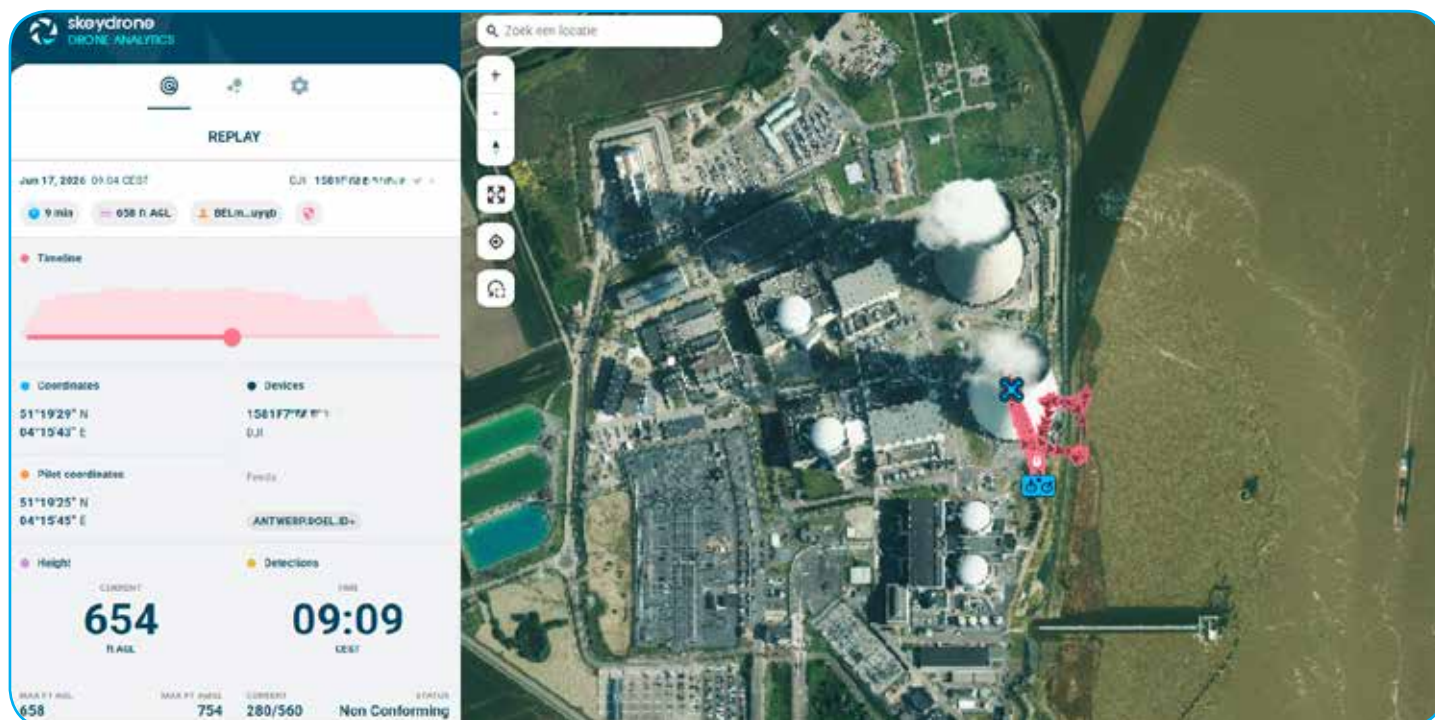
The need to address drone-related risks is being reinforced by Europe's evolving regulatory

landscape. The Critical Entities Resilience (CER) Directive is reshaping expectations around risk management, resilience, and incident preparedness for critical infrastructure operators.

The CER Directive requires critical entities to assess risks, implement resilience measures, and demonstrate their effectiveness through continuous evaluation and testing. Importantly, resilience is no longer viewed as a static capability but as an ongoing process of adaptation and improvement.

From a resilience perspective, the issue is not solely about preventing worst-case scenarios, but about ensuring continuity of operations under uncertain and dynamic conditions. A single drone incident can trigger cascading effects: halting operations, prompting evacuations, or forcing temporary shutdowns while the threat is assessed. In highly interconnected sectors such as energy, transport, and telecommunications, even short disruptions can propagate across systems, amplifying impact.

Without reliable awareness of aerial activity, response measures



cannot be effectively triggered.

The Blind Spot in Traditional Security

Most physical security systems were designed for a world where threats approached from the ground. Perimeter fences, gates, cameras, and patrols remain essential, but they were never intended to address aerial threats.

A drone can bypass a fence in seconds. It can enter restricted areas without passing a checkpoint or triggering conventional access controls. Even advanced CCTV systems often struggle to detect small drones at long range or in poor visibility conditions. Human observation offers limited protection as well, especially when dealing with fast-moving aircraft operating at varying altitudes and under challenging weather or lighting conditions.

The challenge is growing as drone technology continues to evolve. Modern drones can fly autonomously, follow pre-

programmed routes, operate beyond visual line of sight, and remain airborne for extended periods. Their increasing performance and accessibility mean that organisations can no longer rely on traditional security measures alone.

This has created a significant blind spot for many organisations: limited awareness of what is happening in the airspace immediately surrounding their facilities. Yet in today's threat environment, resilience requires visibility not only on the ground, but also in the air.

Building an Effective Drone Security Capability

Effective drone security requires much more than simply detecting a drone. Critical infrastructure operators need the ability to understand airspace activity, assess risk, and respond appropriately in real time.

The first requirement is real-time visibility of airspace activity.

Security teams need immediate awareness of where drones are located, how they are moving, and whether they are interacting with protected areas. Early detection and tracking provide valuable time to assess potential threats before they escalate.

Equally important is the ability to distinguish authorised from unauthorised activity. Many organisations already use drones for inspections, surveys, maintenance, and surveillance, while contractors and public authorities may also operate them legitimately. Effective solutions must separate these approved operations from suspicious flights, allowing security teams to focus on genuine risks.

Organisations also need contextual threat assessment. A drone's presence alone does not necessarily indicate malicious intent. Factors such as drone type, flight behaviour, duration, and proximity to sensitive assets can provide valuable insight into

the level of risk. Understanding whether a drone is simply passing through or displaying unusual behaviour enables a more informed response.

Detection and assessment must ultimately support a proportionate and coordinated response. This may include locating the drone operator, enabling intervention by security personnel or law enforcement, and supporting authorised counter-drone measures where appropriate.

Because drone incidents often involve multiple stakeholders, collaboration and coordination are essential. Security teams, operations staff, management, law enforcement, and emergency responders all benefit from a

shared operational picture that supports faster decision-making and more effective incident management.

Finally, drone security contributes to resilience and compliance. Historical drone activity data can reveal trends, vulnerabilities, and areas of heightened exposure, helping organisations strengthen resilience and support regulatory reporting.

Together, these capabilities enable a structured, risk-based approach to managing drone activity around critical infrastructure.

From Detection to Resilience

As drone activity around critical infrastructure grows, organisations must look beyond detection and

focus on resilience, operational continuity, and coordinated response.

As legitimate drone use expands, the ability to distinguish authorised from unauthorised activity, assess risk in real time, and coordinate responses will become essential. Airspace awareness is now a core part of modern security and resilience.

Just as organisations expanded from physical security to cybersecurity, they must now look upward. In the age of drones, protecting critical infrastructure requires visibility, control, and situational awareness in the airspace above.

IAEA Reviews Finland's Nuclear and Radiological Emergency Preparedness and Response

An International Atomic Energy Agency (IAEA) team of experts has concluded a ten-day mission to review Finland's preparedness and response framework for nuclear and radiological emergencies. The Emergency Preparedness Review (EPREV) Service was carried out at the request of the Government of Finland and hosted by the Radiation and Nuclear Safety Authority (STUK).

The mission reviewed Finland's arrangements and capabilities to respond to nuclear and radiological emergencies, against the IAEA safety standards.

Finland operates five nuclear power reactors at two sites: Loviisa nuclear power plant, 90 km northeast of the capital Helsinki, and Olkiluoto nuclear power plant, 270 km northwest of Helsinki. The Olkiluoto site also hosts

the Onkalo spent fuel repository, the world's first geological disposal facility for final disposal of nuclear waste.

Radiation sources are also used in Finland's medical, industrial and research applications.

The EPREV team interviewed the main governmental authorities responsible for preparedness and response to nuclear and radiological emergencies, as well as the national and regional police and rescue services, and local public authorities.

The team visited the Olkiluoto nuclear power plant and reviewed the offsite response arrangements at the Loviisa nuclear power plant. They also visited the Satasairaala hospital chemical, biological, radiological and nuclear training centre as well as food safety laboratories and the Helsinki City Rescue Department and civil

defence shelter.

Olivier Isnard, Deputy Director for Emergency Preparedness and Response at the French Authority for Nuclear Safety and Radiation Protection, led the international review team, which included experts from Argentina, Austria, Canada, France, Kingdom of the Netherlands, Slovenia and South Africa.

"Finland has invested considerable effort and resources in preparing for nuclear and radiological emergencies, and we saw this reflected in the expertise and commitment of the organizations we met," said Isnard, adding that "more systematic coordination at the national level, and across sectors and phases of an emergency, would help Finland draw even more effectively on these capabilities."

UK and Allies urge critical sectors to improve defences against Russian intelligence targeting

Organisations in critical infrastructure sectors are being supported to better understand and defend against malicious activity, as the UK and international partners today call out techniques used by Russian Intelligence Services

Alongside 18 agencies from 12 countries, the National Cyber Security Centre (NCSC) – a part of GCHQ – has published a new advisory highlighting the methods of Federal Security Service (FSB) Centre 16 cyber actors, who are exploiting vulnerable routers and opportunistically targeting networks belonging to critical national infrastructure (CNI) globally.

Sectors most at risk from this global targeting, including communications,



defence, energy, financial services, government and healthcare, are subsequently being urged to take action. This includes recommendations to use SNMPv3 and disable legacy SNMP versions, implement strong and unique passwords for network devices, and restrict access to management protocols through appropriate access controls.

Centre 16, also known as Berserk Bear, Energetic Bear, Crouching Yeti, Dragonfly, Ghost Blizzard and Static Tundra, has been seen hunting for vulnerable routers by scanning the internet for devices that still use default or weak Simple Network Management Protocol (SNMP) passwords and community strings.

Whilst the actor primarily uses SNMP scans to locate

and compromise vulnerable routers, they have also exploited well-known vulnerabilities relating to Cisco devices, Cisco's Smart Install (SMI) feature and web-portal flaws to gain control of network devices.

The UK together with EU member states has also today formally attributed the December 2025 attack on Poland's energy grid to Russia's FSB Centre 16 – an attack that if it had been successful could have caused 500,000 civilians to lose electricity.

The NCSC has co-sealed this new advisory alongside agencies from Australia, Canada, Czech Republic, Denmark, Estonia, Finland, France, Italy, New Zealand, Poland, Sweden and the United States.

ENISA scales up its role in the CVE Program

ENISA's role within the CVE™ Program continues to grow with the strategic onboarding of key entities in the global vulnerability management ecosystem and the transition of existing CNAs under the ENISA Root. Currently, there are 20 CNAs under ENISA Root, with 12 onboarded directly by ENISA and 8 transferred from MITRE Root to ENISA Root.

The Agency's contribution to the Program has expanded, attesting to its commitment to acting as a driver and facilitator of vulnerability management

at European and international level, through consistent practices, timely identification and trusted coordination among partners.

The addition of new CNAs from across multiple sectors, including CSIRTs, vendors and suppliers, international alliances, and security research organisations, further supports the objectives of the CVE Program of expanding global participation, broadening diversity of participating organisations, improving quality, and increasing operational capacity.

ENISA became a CVE Root for European entities, serving as the central point of contact within the CVE Program for EU Member States' and EU authorities alike, as well as for EU CSIRTs Network members, and cooperative partners under ENISA mandate. This role is carried out in close coordination with CISA and MITRE, as part of a shared commitment to strengthen the resilience, quality, and long-term sustainability of the global CVE Program.

Through its role as a CVE Root, ENISA recruits, onboards, trains, supports, and manages CNAs within

its scope, facilitating their transition where relevant, and ensuring the effective assignment of CVE Identifiers (CVE IDs) and publication of CVE Records. This role also helps ensure that CVE Program rules, guidelines, and processes are followed.

By expanding the number and diversity of CNAs under its Root, ENISA is helping to reinforce the CVE Program as a shared global vulnerability identification backbone relied upon by governments, vendors, researchers, defenders, and the wider cybersecurity community.

CISA, FBI and Partners Warn Organizations of Gunra Ransomware Actors Targeting Multiple Critical Infrastructure Sectors

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Department of Defense Cyber Crime Center (DC3), National Security Agency (NSA), U.S. Secret Service (USSS), and Republic of Korea's National Policy Agency (KNPA) released a joint Cybersecurity Advisory, #StopRansomware: Gunra Ransomware, a ransomware-as-a-service (RaaS) variant used by affiliates to target a range of critical infrastructure sectors and organizations worldwide—including healthcare and public health, financial services, government services and facilities, and professional and nonprofit services.

Gunra actors gain initial access by exploiting



common vulnerabilities and exposures (CVEs) *CVE-2024-55591 and CVE-2025-24472 in internet-facing devices. With access, Gunra actors use a double-extortion model that employs both data exfiltration and data encryption, and negotiate through a Tor-based portal, where they threaten to publish exfiltrated data if

the victim does not pay the ransom within five to seven days. The advisory provides tailored detection guidance, indicators of compromise (IOCs), recommended actions if potential compromise is detected, and mitigation recommendations aligned to Cross-Sector Cybersecurity Performance Goals (CPGs).

"Gunra is another variant in the ongoing trend of ransomware attacks causing disruption and harm to U.S. and international organizations. To combat cyber threat activity, CISA continues to work with our government, industry and international partners to provide timely and actionable information that reduces the prevalence of damaging ransomware incidents," said CISA Acting Executive Assistant Director for Cybersecurity, Chris Butera. "With our partners, CISA encourages organizations to urgently mitigate vulnerabilities identified in this advisory, implement recommended actions, and adopt security measures aligned to CPGs."

Cyber Storm X: 20 Years of Readiness, Resilience, and Real-World Impact

This year marks the 20th year of Cyber Storm, a full-scale national cybersecurity exercise that for two decades has brought together the people who defend the systems Americans rely on. Held every two years, Cyber Storm X arrives as threats from geo-political activity, compromised edge devices, AI risks, and more present new challenges to our nation's critical infrastructure.

As the nation's largest cybersecurity exercise, Cyber Storm plays a vital role in preparing for potential cybersecurity incidents by testing and strengthening the nation's

ability to coordinate a unified cyber response. Participants from private and public organizations work together through a simulated crisis. Together, they learn as a team and build stronger relationships that will speed response during an actual event. Importantly, organizations can also update their response plans based on lessons learned during the exercise.

Cyber Storm began with 500 participants 20 years ago as a national effort to bring government and industry together in one place when our nation needed a way to understand how a major

cyber incident could unfold across many sectors at once.

This number has grown, and this fall's Cyber Storm exercise will bring together 2,000 critical infrastructure owners and operators from around the country, spanning everything from large national companies to local utilities. Participants include legal teams, crisis communication, IT managers, and organizational leaders. For many of them, this exercise is the first time they meet those who they will need to work with during a cybersecurity crisis.

Cyber Storm features a simulated attack on the

services our nation counts on every day. These are services that keep communities moving and can't afford downtime. For example, in 2024's Cyber Storm IX, a simulated threat actor infiltrated networks modeled after those found across the Food and Agriculture sector, triggering cascading disruptions across retail, production, and distribution systems. These "interruptions" slowed the movement of food products from manufacturing plants to store shelves, caused payment processing outages at grocery retailers, and fueled public confusion as media reports highlighted delays and errors.

Africa's early warning experts and officials call for sustained momentum on life-saving disaster protection systems

Africa has made significant progress in expanding early warning systems, but with climate and disaster risks accelerating, the task now is to translate that progress into protection for every country and every community. This was a central message emerging from the Africa Early Warnings Forum, held in Addis Ababa, Ethiopia.

The number of African countries reporting multi-hazard early warning systems has risen from just 14 in 2015 to 41 in 2026, while the reported comprehensiveness of these systems has more than doubled since 2022. The region's progress reflects the leadership of African governments and regional institutions in scaling up early warning systems,



notably through the Africa Multi-Hazard Early Warning and Early Action System (AMHEWAS), led by the African Union Commission.

It was against the backdrop of growing climate risks that the UN Secretary-General launched the global Early Warnings for All initiative in 2022, with the ambition of protecting everyone, everywhere through early

warning systems by 2027. The urgency of that ambition is only increasing. In 2025 alone, extreme weather and climate-related events affected at least 13 million people and led to more than 3,000 reported fatalities across Africa. Strong El Niño conditions forecast for 2026–27 could bring further extremes, including increased rainfall in some parts of the continent and drier-than-

usual conditions in others. In this context, multi-hazard early warning systems remain one of the most proven and cost-effective means of protecting lives, livelihoods, essential services, and critical infrastructure.

This week in Addis Ababa, the Africa Early Warnings Forum brought together more than 400 technical experts from governments, regional institutions, the private sector, scientific institutions, civil society organizations, humanitarian actors and international partners to accelerate implementation, strengthen partnerships and sustain financing to expand disaster protection across Africa through multi-hazard early warning systems.

INTERPOL report finds AI linked to more than half of cybercrime in Africa

Artificial intelligence is enabling 55 per cent of reported cybercrimes across Africa making attacks faster, more scalable, and increasingly difficult for victims and platforms to detect, according to INTERPOL's African Cyberthreat Assessment Report 2026.

With more than 1.1 billion mobile subscribers recorded in 2025, Africa's digital transformation is expanding rapidly.

However, cybercrime legislation is fragmented and AI readiness in law enforcement agencies remains alarmingly low.

The 40-page report draws on survey data from 36 African member countries and highlights a defining shift: cyber-criminality has evolved from isolated incidents into an industrialized, borderless ecosystem.

East Africa emerged as a hub of mobile money fraud and infrastructure-targeted ransomware.

Business email compromise and romance scams targeting both corporate and individual victims were prolific in Central and West Africa.

Southern Africa's ultra-high

connectivity makes it a magnet for global threat actors seeking maximum disruption.

The financial toll of cybercrime in Africa is significant.

Since 2024, cybercrime-related losses have more than doubled, from USD 192 million to USD 484 million, driven primarily by AI-facilitated scams, credential harvesting, and automated social engineering campaigns.

According to the report, in 2025, online scams continued to be the most reported type of cybercrime,

with attackers leveraging mobile money platforms, social media and AI to reach their targets.

Notably, 72 per cent of surveyed countries reported the presence of scam centres, with the highest concentration in Southern and West Africa.

Digital sextortion and online harassment, often facilitated by AI-generated deepfakes and synthetic media, remained pervasive, with some 600,000 sextortion detections recorded by TrendAI, one of several partners working with INTERPOL.

New AI frontier cyber threat guidance for boards of directors

Boards of directors and senior leaders need to understand how newer frontier AI models are reshaping cyber threats. As advances in frontier AI models make it easier for cybercriminals to identify and exploit vulnerabilities, organisations face a growing threat from AI-enabled cyber attacks.

To help boards respond, we have released in partnership with the Australian Institute of



Company Directors (AICD), Frontier AI cyber threat considerations for boards of directors. The publication outlines frontier AI cyber threats

and provides practical guidance to help organisations strengthen governance, improve preparedness, and build their cyber security

posture.

It includes actions boards can take to prevent, detect, respond to, and recover from AI-related cyber security incidents in an increasingly AI-driven threat environment. By understanding these threats and strengthening oversight, organisations can better protect themselves against emerging AI-powered cyber threats.

World Bank Group Backs Water Security and Agricultural Resilience in Brazil's Paraná State

The World Bank Group will support the State of Paraná, Brazil, strengthen water security and protect farmers and rural communities from climate shocks through a new project. It is expected to generate and protect between 54,000 and 78,000 jobs across agriculture, water services, and associated economic activity in one of Brazil's most economically vital regions.

Paraná's economy depends heavily on agribusiness, which accounts for nearly a third of the state's output and the vast majority of its exports. But more frequent droughts and floods are putting this foundation at risk, threatening farms, disrupting water supplies, and eroding the livelihoods of millions of people. The proposed project aims to help reverse this trend by strengthening how water



resources are managed across the state, improving resilience to climate extremes, and securing access to water and sanitation for vulnerable communities.

The effort is supported by a US\$186 million loan from the International Bank for Reconstruction and Development (IBRD). On the agricultural side, the project will support around 9,200 farmers in protecting

their farms against drought and extreme weather across more than 130,000 hectares, reducing crop losses during dry seasons and helping farming operations remain viable and productive. For families in rural areas, improved water and sanitation services will reach approximately 60,000 people, extending access to communities that have long been underserved. In

urban areas, water safety measures will help protect more resilient water supply services for 2.2 million residents.

Beyond strengthening water governance and urban water services, the Project will invest in the restoration of riparian forests and degraded lands across 10,690 hectares of Permanent Preservation Areas (APPs) along rivers and springs, as well as in the adoption of sustainable land management practices on more than 130,000 hectares of agricultural land. By bringing nature-based solutions to the heart of watershed management, the Project will help ensure that the State's rich agricultural landscape and its water resources reinforce each other, strengthening the long-term resilience of both rural communities and urban water supply systems.

Signpost Six Publish Situation Brief – European Threat Landscape

Signpost Six have been monitoring developments and assess their implications for European organisations, summarised in their latest European Threat Landscape brief.



A series of incidents since early August 2026 indicates an increasingly active hybrid threat environment across Europe. Whilst the likelihood of conventional military action against NATO members remains low, recent reporting highlights a growing risk of disruption through sabotage, cyber activity, drone incursions, surveillance, insider-enabled access, proxy actors and other deniable means.

For organisations connected to Ukraine, NATO, defence production, energy, logistics or other critical supply chains, the more credible concern is the potential for low-level, deniable or disruptive activity designed to create operational, financial or psychological effects without crossing the threshold of open conflict.

Organisations connected to defence, energy infrastructure, logistics,

critical national infrastructure or NATO supply chains should consider the threat environment elevated and review their security posture accordingly. For affected organisations, this can translate into operational downtime, damaged infrastructure, reputational exposure, and (where personnel or access are involved) a compromised ability to trust your own security architecture from the inside out.

“Against this backdrop, a growing number of our clients are turning to structured insider risk assessments, not as a precautionary afterthought, but because insider risk is increasingly one of the most efficient routes available to a hostile actor. These assessments identify where an organisation is genuinely vulnerable and benchmark its current level of maturity against good practice.”

From Detection to Anticipation: Building Time for Critical Infrastructure Resilience

Critical infrastructure is increasingly challenged by a threat landscape in which physical, cyber, climate and operational disruptions interact. A power fluctuation, a communications anomaly or an abnormal temperature reading may appear manageable in isolation. Taken together, they may reveal an emerging disruption with implications well beyond a single asset.



Protection must therefore evolve from monitoring isolated events to building the capacity to anticipate how they may combine and escalate. Monitoring tells us what has happened; resilience depends on identifying patterns, understanding interdependencies and acting before an incident becomes a crisis. Early warning creates that time, enabling teams to protect assets, adjust operations, activate continuity plans and coordinate with public authorities and partners.

At IndraMind, we believe this shift requires an integrated approach to protection. Data from OT environments, cybersecurity tools, physical security systems, operational platforms and external context must be correlated into a single

operational picture that helps teams understand what is happening, what may happen next and which decisions require priority attention. Artificial intelligence has a clear role in that model: detecting weak signals, prioritising risks and exploring likely consequences at the speed complex situations demand, while preserving the operator's sovereign control of data, models and decision processes. It must remain trustworthy, governed and aligned with each operator's mission.

Artificial intelligence can only strengthen resilience when it is deployed responsibly. In critical infrastructure, this responsibility also includes maintaining sovereignty over the data, software, models and critical operational systems on which essential services depend. Human oversight must remain central to consequential decisions, supported by systems that are explainable, traceable and governed by clear guardrails. This creates confidence in how recommendations are produced, enables accountability, and ensures that AI supports, rather than replaces, the expertise of those responsible for protecting essential services.

New Global Survey Reveals OT Cyber Security Awareness Still Immature Despite Rising Threats, Secolve Finds

A new global survey from Secolve, Australia's leading Operational Technology (OT) cyber security company, has found that most critical infrastructure and industrial organisations remain at an early stage of OT cyber security awareness maturity, even as threats linked to geopolitical tension and supply chain compromise continue to rise.



The State of OT Cyber Security Awareness 2026 report, based on responses from professionals across manufacturing, energy, oil and gas, transport, and other OT-related sectors in Europe, North America, and Australia, found that 68.1% of organisations rate their awareness maturity as weak or developing, compared to just 28.6% who consider it defined or embedded.

"This survey confirms what we see every day working with industrial and critical infrastructure organisations - awareness has genuinely improved, but there's still a long way to go before training reflects the reality of the threats our frontline workers actually face," said Laith Shahin, CEO of Secolve. "The organisations making real progress

are the ones treating OT security awareness as an operational priority, not a compliance checkbox."

The report recommends five immediate priorities for organisations looking to strengthen their OT security posture: building role-based learning paths for operators, engineers, and contractors; combining e-learning with practical exercises such as tabletop discussions and hands-on simulations; making OT awareness training a condition of site and remote access for contractors and vendors; establishing shared governance across cyber, OT, and safety teams; and strengthening frontline reporting through plain-language, accessible escalation routes.

Cybrid Thrust Develops new Drone Threat Assessment services

The accessibility and capability of commercial drones have changed the security equation. A relatively inexpensive platform can cross physical boundaries in seconds, conduct reconnaissance, identify vulnerabilities, interfere with operations or potentially carry a payload towards sensitive assets.



For infrastructure operators, the key question is therefore no longer simply: "Do we need counter-drone technology?", but: "What exactly are we defending against?"

This is the thinking behind Cybrid Thrust's new Drone Threat Assessment service, developed for critical infrastructure operators seeking to understand their real exposure before investing in counter-UAS technologies.

Rather than beginning with a sensor or detection system, the assessment starts with the site itself. It examines critical assets, potential launch locations, approach routes, blind spots, threat-actor capabilities and realistic attack scenarios.

The result is a clearer picture of where vulnerabilities exist, how quickly a threat could reach an asset, and which mitigation measures should be prioritised.

This threat-led approach also helps organisations move beyond technology-first procurement. Radar, RF detection, electro-optical sensors and command-and-control platforms may all play an important role, but their effectiveness depends on the specific risk environment they are designed to address.

As Europe strengthens its focus on critical infrastructure resilience and counter-drone preparedness, operators increasingly need evidence-based assessments that connect threat, vulnerability and investment.

Cybrid Thrust will present this approach at Critical Infrastructure Protection & Resilience Europe (CIPRE), in Brussels from 20–22 October.

The message is simple: before deciding how to stop a drone, organisations first need to understand how one could be used against them.

Acrisure UK and ESET Announce Strategic Cyber Partnership to Strengthen Business Resilience

Acrisure UK, the retail insurance broking platform, announced an agreement with ESET, a global cybersecurity provider protecting more than 500,000 businesses worldwide.



As cyber threats continue to evolve, organisations are increasingly looking for trusted partners who can help them navigate both the technical and commercial implications of cyberattacks. The service brings together Acrisure's specialist cyber insurance capabilities and ESET's cybersecurity expertise and services, providing clients with access to a broader range of support to help strengthen resilience, manage risk and respond effectively when incidents occur.

Acrisure UK's cyber insurance specialists work with organisations across a range of sectors, providing tailored solutions designed to address the financial and operational impact of cyber incidents. Combining deep expertise with strong insurer relationships, the team helps businesses secure appropriate protection while

navigating an increasingly complex risk landscape.

Tim Wiltshire, Director at Acrisure UK, said: "Good cybersecurity and effective cyber insurance should work hand in hand. Organisations are increasingly looking at cyber risk as a business issue rather than simply an IT issue, and that requires a combination of prevention, resilience and specialist insurance support."

ESET's cloud-first ESET PROTECT platform provides next-generation threat prevention, detection and response capabilities. ESET also offers 24/7 MDR (Managed Detection and Response) services, combining AI and human expertise for advanced threat detection and proactive threat hunting without the need for in-house security specialists.

D-Fend Solutions' EnforceAir Provided World Cup Counter-Drone Security Across Array of Host Cities

D-Fend Solutions, the leader in field-proven radio frequency (RF) cyber-driven, non-kinetic, non-disruptive counter-drone takeover technology, announced that its EnforceAir platform was deployed extensively throughout North American host cities for the 2026 FIFA World Cup.



D-Fend Solutions and its public safety partners maintained a strict posture of confidentiality leading up to and during the tournament. Operations were deployed across the expansive multi-national tournament footprint, establishing a cyber counter-drone presence of unprecedented scale.

The deployment represented a major multi-site counter-drone operation, spanning key tournament locations and coordinated across a combination of international, federal, state, and local agencies operating in a complex, multi-layered security environment.

"The unprecedented scale of the 2026 World Cup required a sophisticated,

multi-layered approach to airspace safety, and the widespread deployment of EnforceAir is a profound validation of the trust elite public safety agencies place in D-Fend Solutions," said Zohar Halachmi, Chairman and CEO of D-Fend Solutions. "Protecting high-stakes events of this magnitude is exactly what our technology is built to do. By providing a non-kinetic, RF cyber-takeover capability, we enabled security professionals to safely mitigate drone risks without disrupting the matches, surrounding critical infrastructure, or vital communications, serving as a trusted foundational layer for operational safety in the security architecture for the world's biggest games."



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

