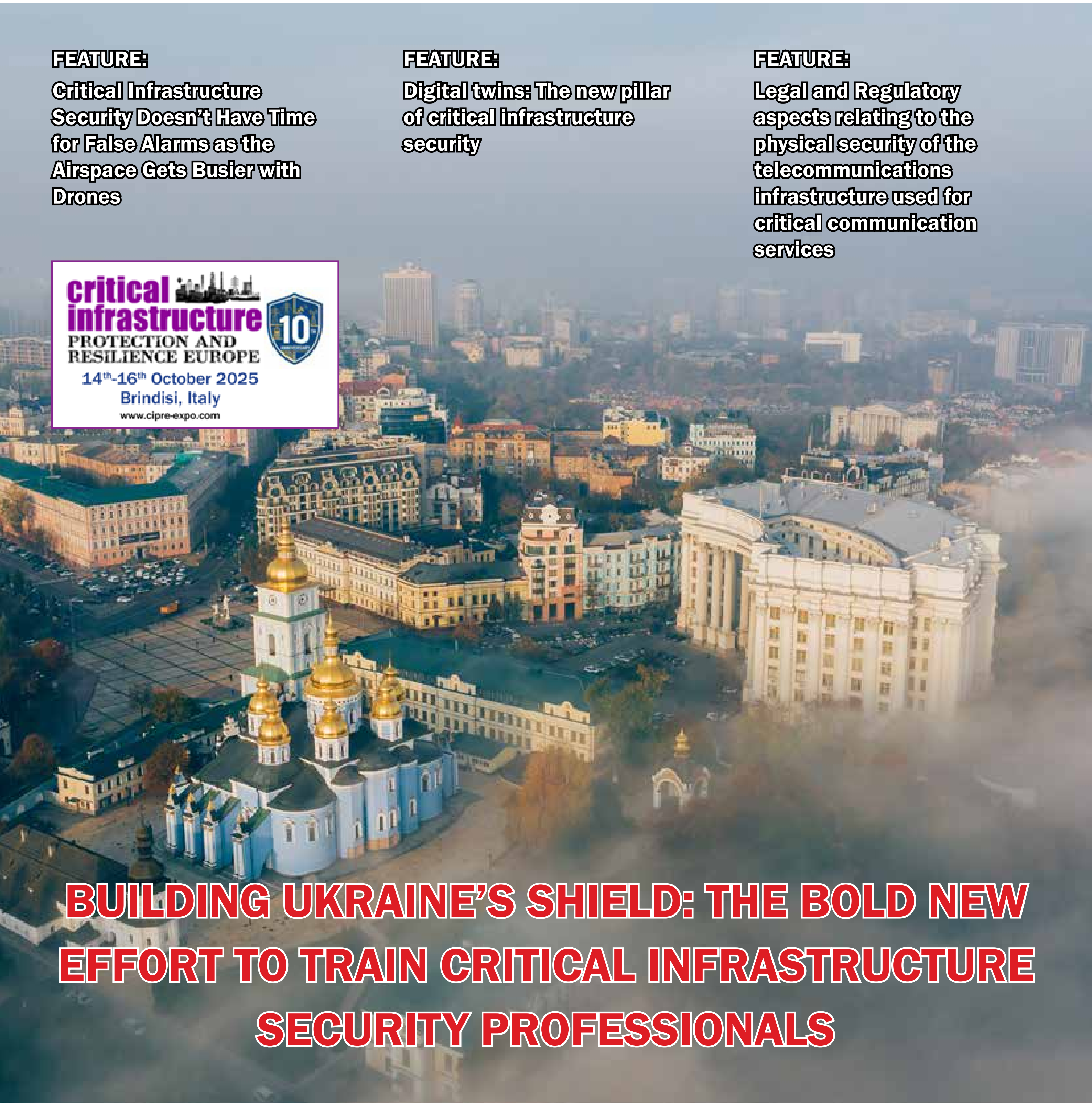
critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

SUMMER 2025
www.cip-association.org



FEATURE:

Critical Infrastructure Security Doesn't Have Time for False Alarms as the Airspace Gets Busier with Drones

FEATURE:

Digital twins: The new pillar of critical infrastructure security

FEATURE:

Legal and Regulatory aspects relating to the physical security of the telecommunications infrastructure used for critical communication services

BUILDING UKRAINE'S SHIELD: THE BOLD NEW EFFORT TO TRAIN CRITICAL INFRASTRUCTURE SECURITY PROFESSIONALS

Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

14th-16th October 2025 - Brindisi, Italy

critical infrastructure PROTECTION AND RESILIENCE EUROPE

TIEMS

With the patronage of the City of Brindisi

Co-Hosted by:

International Association of CIP Professionals

UNIVERSITÀ DEL SALENTO
DIPARTIMENTO DI INGEGNERIA DELL'INNOVAZIONE

CRISR

REGISTER ONLINE TODAY

Register at www.cipre-expo.com/register
and benefit from Early Bird Discounts

Early Bird Deadline - 14th September

Securing the Inter-Connected Society

The second 'Critical Infrastructure Protection Week' will take place in Brindisi, Italy on 14th-16th October and will see IACIPP host the 10th 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'The International Emergency Management Society (TIEMS)' conference.

The premier event for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

The recent implementation of The Critical Entities Resilience (CER) and NIS2 Directives, which lays down obligations on EU Member States to take specific measures to ensure that essential services and infrastructures, for the maintenance of vital societal functions or economic activities, are provided in an unobstructed manner in the internal market, enhancing security requirements, reporting obligations, and crisis management capabilities.

Compliance with the CER Directive and NIS2 Directive are crucial for businesses operating in the EU to safeguard their systems, mitigate threats, and ensure resilience. Penalties are enforceable on agencies and operators for non-compliance.

Join us in Brindisi, Italy for the next CIP Week in Europe and the 10th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure.

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Speaker line-up includes:

- Claudio Ciccotelli, Head of National Cybersecurity Perimeter Division Regulatory Directorate, National Cybersecurity Agency
- Harald Drager, President, The International Emergency Management Society (TIEMS)
- Cdr Col. Antonino Massara, Commander 36' Fighter Wing Commander, Ministry of Defence, Italy
- Robert Tucker, Resilient Network Manager, ESB, Ireland
- Bartel Meersman, Transport And Border Security Head Of Unit, European Commission Joint Research Centre
- Adrian Grilli, Technology Adviser, EUTC, Belgium
- Frederic Guyomard, Senior Project Manager / Cybersecurity Research Engineer, Electricite De France
- Dr Oleksandr Potii, Chairman, State Service of Special Communications and Information Protection of Ukraine (SSSCIP)
- Giampaolo Panariello, CTO Network Infrastructure, Nokia
- Daniel Golston, Associate Programme Officer, Organization for Security and Co-operation in Europe
- Alessandro Lazari, Fellow in Critical Infrastructure Protection and Resilience University of Salento, Italy & IACIPP

Full speaker line-up at **www.cipre-expo.com**

Executive Sponsors:

TCCA E.DSO EUTC open ENLIT AUTO-ISAC

Supporting Organisations:

EE-ISAC CCNE CoESS Help2Protect ISIO

Platinum Sponsor:

eset Digital Security Progress. Protected.

10 YEARS SUPPORTING THE INDUSTRY - BUILDING STRENGTH IN OUR COMMUNITY

In an age defined by complex geopolitical shifts and technological innovation, the protection of our critical infrastructure has never been more vital. From the energy grids that power our cities to the financial networks that drive our economies, these systems are the very backbone of modern society. Yet, they face a constantly evolving threat landscape, one where the lines between physical and digital attacks, and between state-sponsored and non-state actors, are increasingly blurred.

Recent years have underscored the urgency of this mission. We've seen a rise in "gray-zone warfare" and sophisticated cyber-physical attacks that seek to disrupt and destabilize. Adversaries are not only aiming to steal data but to cause kinetic effects, bringing down essential services with frightening efficiency. As we look ahead, the challenges will only grow more complex, with new vulnerabilities emerging from the proliferation of smart cities, connected devices, and the integration of artificial intelligence into core systems.

It is against this backdrop that we celebrate a truly remarkable milestone: the 10th anniversary of IACIPP and our premier industry event in Europe, Critical Infrastructure Protection & Resilience Europe, part of CIP Week in Europe in Brindisi, Italy this October, and delighted to be joined by The International Emergency Management Society (TIEMS) with their annual hybrid conference, for greater industry collaboration and sharing of ideas and experiences. For a decade, this gathering has been a crucial forum for collaboration, knowledge-sharing, and innovation. It has brought together the brightest minds from the public and private sectors to build the partnerships and develop the strategies needed to fortify our collective resilience.

As we commemorate ten years of this essential work, let this issue serve as a reminder of both the challenges ahead and the strength of our community. We have come a long way, but the journey to secure our world is ongoing. Let us continue to learn from each other, to innovate tirelessly, and to stand as a united front against those who would threaten our way of life.

Thank you for being part of this community and we hope you enjoy this edition, with some great insights and features from across different infrastructure sectors. We also look forward to welcoming you to Brindisi, Italy in October.

Thank you.

Ed.

www.cip-association.org

Editorial:
Neil Walker
E: neilw@torchmarketing.co.uk

Design, Marketing & Production:
Neil Walker
E: neilw@torchmarketing.co.uk

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

Building Ukraine's Shield: The Bold New Effort to Train Critical Infrastructure Security Professionals

By Vladlen Basystyi, Technical Advisor at CRDF Global, specializing in cybersecurity and critical infrastructure protection

In November 2021, a landmark law on Critical Infrastructure Protection (CIP) was signed by the President of Ukraine—setting in motion a national effort to secure the lifelines of the country's economy, defense, and daily life. Two years later, in September 2023, the Cabinet of Ministers approved Ukraine's National Plan for the Protection, Security, and Resilience of Critical Infrastructure, a document that not only laid out an ambitious strategy but also revealed a major vulnerability: a critical shortage of qualified professionals.

The question soon became unavoidable—how and where can Ukraine train the specialists essential to protecting its most vital systems? The National Plan mandated a full feasibility study to explore this issue and develop recommendations for building a sustainable educational and training ecosystem for CIP professionals.

This comprehensive study was the first of its kind in Ukraine and worldwide and took a global approach. It examined not only Ukraine's own experience but also incorporated lessons and best practices from the European Union, North America, and international organizations such as the United Nations, NATO, OSCE and the World Bank. The study team interviewed over 50 subject matter experts from Ukraine, the EU, and the United States, representing government agencies, industry sectors, and academic institutions.

The Feasibility Study to Affect the Development of Critical Infrastructure Security and Resilience (CISR) Education and Training System in Ukraine was carried out by Ukrainian, Italian, and American experts in critical infrastructure protection, with financial support from the U.S. Department of State. It was also supported by the Directorate of Professional Pre-Higher and Higher Education of the Ministry of Education and Science of Ukraine, the Critical Infrastructure Security Service of the National Security and Defense Council (NSDC), and the Department of Critical Infrastructure Protection of the State Service of Special Communications and Information Protection (SSSCIP).

The study's main conclusion was that the development of an education and training system for critical infrastructure protection in Ukraine is both possible and necessary. Such a system is needed to prepare leaders, managers, specialists, and trained personnel capable of carrying out a wide range of tasks in the field of CI protection — all in line with Ukrainian legislation and national security goals.

It worth to mention that the results of this Study was officially presented in Lecce, Italy, during the international workshop on "Development of University Programs on Critical Infrastructure Security and Resilience" in March 2024. The event served as a vital platform for Ukrainian participants and international experts to exchange knowledge, share best practices, and explore innovative approaches in the field of Chemical Critical Infrastructure Security and Resilience (CISR) education. The workshop highlighted the importance of academic collaboration in strengthening the resilience of critical sectors and advancing specialized university programs across borders.

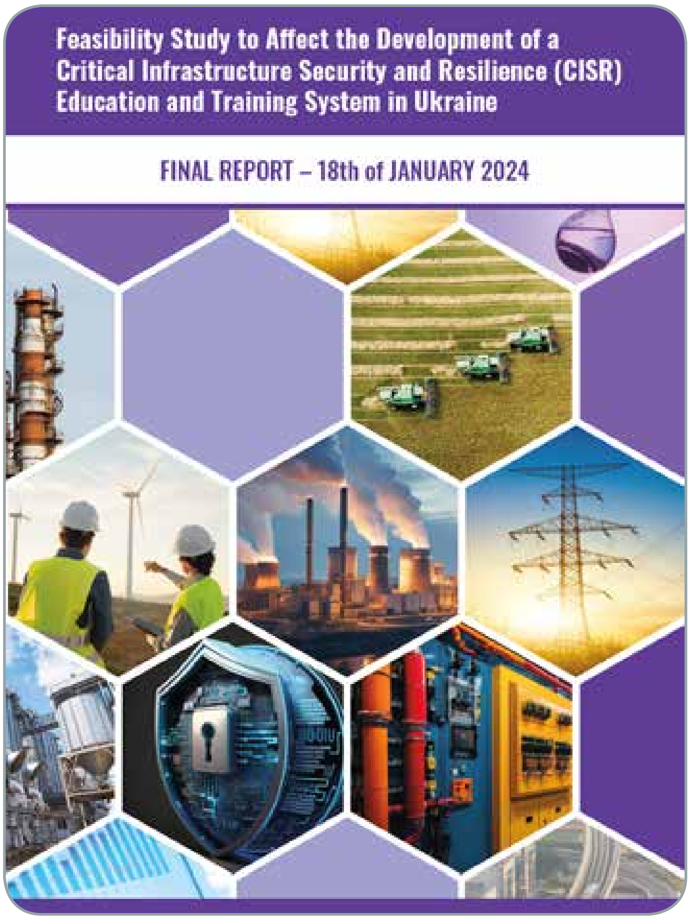
Although the study was conducted in 2024, it has already led to several significant outcomes:

1. On June 27, 2024, the Center for Critical Infrastructure Security and Resilience was established at the Department of Civil and Industrial Safety named after Hero of Ukraine O.S. Chub, within the Faculty of Environmental Safety, Engineering, and Technology at Kyiv Aviation University. This center attracted the attention of the Ministry of Infrastructure and Transportation of Ukraine, which has since accepted university students studying CIP for internships at transportation-related CI facilities in Kyiv.

2. The National Institute for Strategic Studies established two working groups focused on developing educational programs in the field of CIP. As a result, a proposal is being prepared for submission to the Ministry of Education of Ukraine to formally introduce new CIP curricula and programs in Ukrainian universities.

3. Compared to the Research on CIP education conducted in 2021, there is clear progress in the development of university-level programs both at the national level (Kyiv) and in several regions (Lviv, Kharkiv, and Cherkasy). This development is supported by the National Qualifications Agency of Ukraine and coordinated by the CIP offices of the NSDC and SSSCIP.

4. Based on the findings of the study, four new professions related to critical infrastructure protection were added to the National



Feasibility Study to Affect the Development of a Critical Infrastructure Security and Resilience (CISR) Education and Training System in Ukraine

FINAL REPORT – 18th of JANUARY 2024

CRITICAL INFRASTRUCTURE PROTECTION PROFESSIONS
RISK, THREAT, AND VULNERABILITY ANALYST FOR CRITICAL INFRASTRUCTURE
CRITICAL INFRASTRUCTUURE PROTECTION EXPERT
SPECIALIST IN CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE
HEAD OF A DEPARTMENT/UNIT FOR CRITICAL INFRASTRUCTURE PROTECTION

Occupational Classifier of Ukraine, including:

* Risk, Threat, and Vulnerability Analyst for Critical Infrastructure – identifies potential threats and vulnerabilities, assesses risks, and develops mitigation recommendations;

*Critical Infrastructure Protection Expert – provides expert assessments of protection methods and ensures resilience against threats;

*Specialist in Critical Infrastructure Protection and Resilience – directly implements protection measures and ensures operational continuity in crisis conditions;

*Head (or other manager) of a Department/Unit for Critical Infrastructure Protection – organizes, coordinates, and oversees security measures, conducts risk assessments, interacts with law enforcement and specialized agencies, and implements policies and standards to ensure CI resilience.

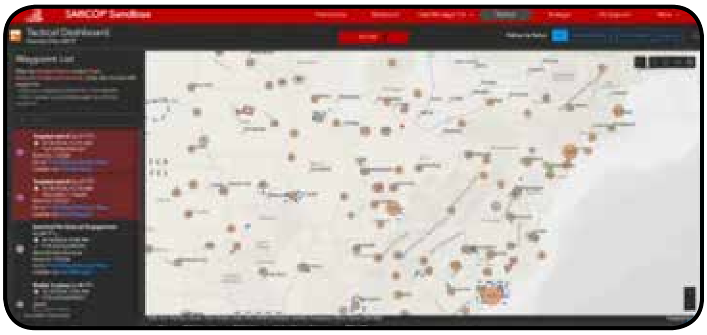
Currently, an interagency working group in Ukraine is developing professional standards for these roles. Whether this initiative will be successful will depend on the outcomes of pilot projects and the real-world performance of certified professionals at critical infrastructure enterprises. It remains to be seen whether additional, more in-depth research and business analysis of the functional responsibilities of CI professionals at enterprises across Ukraine's 24 critical infrastructure sectors (as defined by a Cabinet of Ministries of Ukraine's resolution) will be necessary. Based on such analysis, there may be a need to adjust or refine the newly introduced CIP professions, taking into account the 2008 EU Directive and the experience of the 5 CIP SISTERS: United States,Canada, the United Kingdom of the Great Britain, New Zeland and Australia.

In conclusion, the issue of training critical infrastructure protection professionals, especially for sector-specific enterprises, still requires deeper research and strategic planning. Only by thoroughly analyzing the operational needs and critical functions of CI enterprises can Ukraine accurately define the roles and responsibilities of CIP specialists and reflect them in professional standards, paving the way for the development of a qualified and mission-ready workforce.

S&T Search and Rescue Tool Plays Swift Role in Recent Flood Response

The Science and Technology Directorate's (S&T) Search and Rescue Common Operating Platform (SARCOP) was deployed immediately by response agencies battling recent floods in Texas, North Carolina, New Mexico, and Vermont. The dashboard was also used by California agencies responding to a fireworks explosion. Learn how SARCOP is saving lives, property, and precious time.

- SARCOP allows incident response teams to operate on one shared geospatial platform, ensuring they have full situational awareness about when, where, and how disaster-impacted areas are searched.
- Funded and developed by S&T in partnership with the nonprofit National Alliance for Public Safety GIS (NAPSG) Foundation, SARCOP has been indispensable in supporting local, regional, state, and federal coordination and decision-making. From 2021 to today, SARCOP has been deployed during 225 active emergency responses and 580 field exercises.
- SARCOP is available for free to agencies nationwide on Windows, Apple, and Android.



A sample screen capture shows the SARCOP dashboard. Teams in Texas are actively using SARCOP to deploy teams, allocate resources, track damages, and map out future search targets. Photo credit: NAPSG

From the early moments of the devastating July 4 floods in Kerr County, Texas, S&T's SARCOP provided integral support to the emergency responders leading search and rescue operations along the Guadalupe River. Those first on-scene quickly began logging their search targets, discoveries, and initial damage assessments—crucial incident intelligence collected and disseminated in real-time that played a dynamic role in supporting immediate recovery efforts.

"SARCOP allows field teams to access nearby resources and generate field status reports, improves transitions between shifts and team assignments, and allows for strategic decision-making during large-scale events," said S&T Program Manager Ronald Langhelm. "With such a large area to cover and with so many response agencies on the ground, SARCOP from day one immediately provided all of them with shared overall situational awareness, expedited reporting, and full visibility of operations—regardless of agency affiliation."

As the FEMA-designated primary information system for all local, regional, state, and federal urban search and rescue (US&R) teams, SARCOP continues to enable coordination across Texas as strategic field operations carry on. The platform has been instrumental during several statewide disasters in recent years, including Hurricane Ian.

"SARCOP has proven to be our go-to tool for not only effectively and quickly searching for citizens, but it's also a very effective tool for collecting time-sensitive data during a disaster," said Jeff Saunders, director of Texas A&M Task Force 1, in a letter of appreciation to NAPSG in the aftermath of the hurricane. "SARCOP was crucial to the safety of all of the responders in the area. It was the tool for dispatching, accountability, and getting everyone back at the end of the day with a full record of all that was accomplished and what still needed attention. It further has allowed our agency to collaborate with all levels of search and rescue teams from other jurisdictions, which provides for a more thorough and coordinated response."

In this month's flooding, SARCOP was deployed immediately as the two Texas Task Forces arrived on scene and has proved invaluable as assistance arrived from US&R teams in neighboring Louisiana and several other states. In each, operators were able to track search and rescue-related resources in active incident areas from coast to coast, providing finite tactical details on search metrics and field interactions, as well as big-picture metrics on past and current search patterns and worksite status.

"Coordinating disparate resources across multiple locations across the nation requires a coordinated system to provide overall mission continuity," said Langhelm. "Prior to SARCOP, US&R teams operated as siloed autonomous resources. With it, they are all connected as incident support partners."

Critical Infrastructure Security Doesn't Have Time for False Alarms as the Airspace Gets Busier with Drones

By Curtis Walters, Echodyne VP Sales, Government and Critical Infrastructure

Drones have emerged as the tool of choice for bad actors at critical infrastructure sites. The confusion and damage caused by drone activity is very real, and awareness is growing, thanks to a spate of serious recent incidents that have drawn attention to the threat. Reports in December of unknown drone activity in New Jersey sparked headlines around the world, and drone incidents also paused air traffic in two states, at an Air Force base in Ohio and an airport in New York . These, unfortunately, are not isolated incidents.

At Sweden's Stockholm Arlanda Airport , UAS sightings forced the suspension of air traffic, disrupting operations and endangering travelers. In Nashville, a man reportedly attempted to weaponize a drone with explosives to collapse the U.S. power grid. It's clear that drones are no longer a toy and are not restricted to causing annoyances such as disrupting air travel. They present a tangible risk to CI sites and reinforce the necessity for operators to be thoroughly prepared. And along with the uptick in drone sightings, a high volume of false alarms has proven a strain to security infrastructure and response teams.

The issue of false alarms is highlighted by an FBI report into drone sightings in December 2024 , concluding that many had been false alarms, with helicopters, hobbyist drones and even stars mistaken for drone threats. The FBI wrote, "Having closely examined the technical data and tips from concerned citizens, we assess that the sightings to date include a combination of lawful commercial drones, hobbyist drones, and law enforcement drones, as well as manned fixed-wing aircraft, helicopters, and stars mistakenly reported as drones. We have not identified anything anomalous and do not assess the activity to date to present a national security or public safety risk over the civilian airspace in New Jersey or other states in the northeast."

At the same time, aviation and drone flights are growing rapidly, with the FAA dealing with 45,000 flights per day, and a million drones now registered in the U.S. The skies are a busy place, and traditional '2D' security systems at critical infrastructure sites are struggling to keep up.

Recent Executive Orders, such as 'Restoring American Airspace Sovereignty' have highlighted the urgency of dealing with this issue, with the President's Executive Order noting that, "Critical infrastructure, including military bases, is subject to frequent — and often unidentified — UAS incursions. Immediate action is needed to ensure American sovereignty over its skies and that its airspace remains safe and secure."

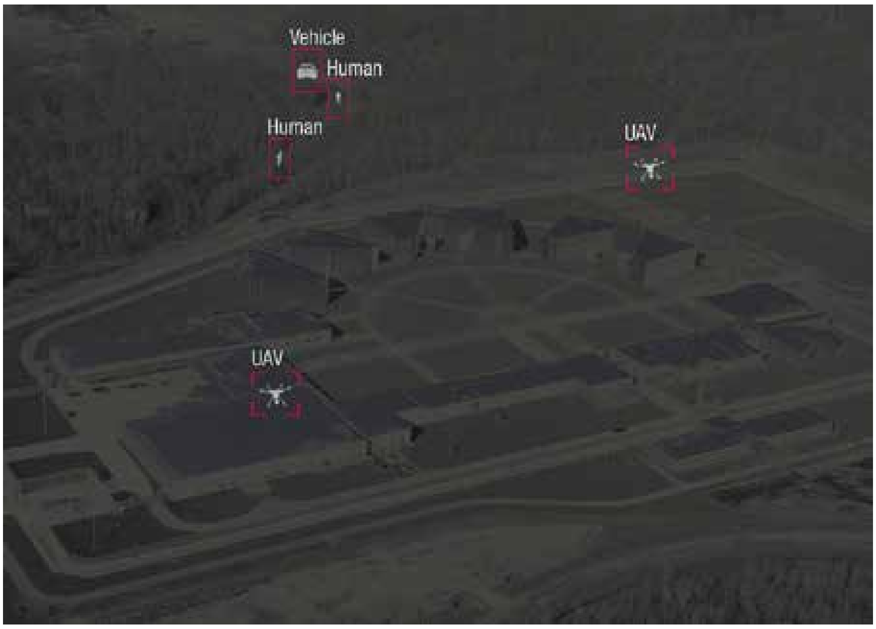
However, all too often, security teams are expected to deal with these new threats on top of their existing tasks, with teams simply asked to 'look up' rather than being augmented with specialist officers with the skills to deal with drone threats. That means already-stretched teams are stretched even further.

As demands for airspace monitoring, deconfliction, and threat management rapidly intensify, technology is becoming the essential bridge between strained security resources and evolving operational needs. Advanced sensor systems are now capable of discerning a broad range of airborne objects—not just aircraft—enabling more accurate identification and prioritization. This capability is vital in reducing false alarms and alleviating the burden on overstretched teams. Traditional perimeter intrusion detection systems (PIDS), while useful, often struggle to differentiate between drones posing real threats to critical infrastructure and benign objects like birds, debris, or weather phenomena. Emerging technologies offer a path forward, enhancing situational awareness and supporting more effective, efficient airspace security.

Cameras and radio frequency (RF) sensors have long played a valuable role in monitoring and securing critical infrastructure—from substations to dams—by providing early detection and situational awareness. However, as airborne threats grow in scale and sophistication, these traditional tools face challenges in reliability, often generating false alarms that burden security teams. Relying solely on optical or RF sensors, or ground-based guards focused on 2D perimeters, is no longer sufficient for addressing the complex dynamics of modern airspace threats. Closing this capability gap requires new technologies purpose-built for the evolving landscape.

The Good, Bad, and Ugly: The Airspace is Getting Busier

Drones are filling the skies at an unprecedented pace, driven by surging adoption in agriculture, infrastructure, and the rapid rise of commercial delivery fleets. Commercial delivery drones are expected to grow at 42.7% CAGR per year from 2025 to 2032, for example .



The FAA has registered 420,825 commercial drones and 383,007 recreational drones in the U.S., with drones used to inspect infrastructure sites sharing the skies with everything from electric vertical takeoff and landing vehicles (eVTOLs) and hobbyist UAVs. Hobbyist drone pilots may operate with good intentions, but their presence near airports, for example, can unintentionally disrupt critical airspace operations. With the FAA recording over 100 drone sightings near U.S. airports each month, the agency is focusing education efforts on recreational users to reduce these incidents and help ensure the safety and reliability of the national airspace system.

Critical infrastructure sites also face the possibility of drones being used for malicious purposes, ranging from espionage to direct attacks. To take one example, Greenpeace flew a Superman-shaped drone into a nuclear plant in 2018 to show its vulnerability. In such situations, radar sensors can play an important role in providing time-stamped and geo-located evidence for later prosecutions.

Drones can also be a powerful tool for espionage, being able to land unobserved in remote locations, even if there is human security on the ground. From that position, they can probe wireless networks for vulnerabilities. Many locations that have previously been considered 'secure', because the idea of a cheap drone with cyber capabilities was science fiction 10 years ago, are now no longer ironclad.

And it is not just remote sites that are vulnerable. Any building that houses computer systems, be that a regional bank or a datacenter hosting cloud-based resources, could potentially be vulnerable to UAV attacks. With many of the services the world relies on, from email to food delivery to internet banking, hosted in server farms, there is vulnerability to small UAVs landing on the roof to tap into networks and breach security systems, or unleashing software to steal trade secrets or simply attack and damage resources.

There are many possible motivations for attackers to target CI locations, from criminal enterprises aiming to steal intellectual property, to state-sponsored espionage and terrorism, to those who seek to cause chaos for its own sake. For such attackers, drones are particularly attractive. They are low-cost, easily and legally accessible, and easy to modify to use as weapons.

In some cases, drones are purpose-built for offensive operations. One illustrative example is the Kalashnikov KUB-UAV, a loitering munition unveiled in 2019. Roughly the size of a coffee table, the drone can fly at speeds up to 80 mph for 30 minutes while carrying a six-pound payload—typically explosives—up to 40 miles. Described by its manufacturer as offering "hidden launch, high accuracy, noiselessness, and ease of handling," it reflects the increasing sophistication of drone-based weapon systems.

In addition to individual drones, swarming tactics—in which dozens or even hundreds of smaller drones operate in coordination—represent another growing area of concern. These swarms could overwhelm traditional defenses and sensors through sheer volume and maneuverability. A RAND Corporation report identifies drone swarms as a "current and growing threat," particularly due to their potential to be used against complex and distributed infrastructure.

What Constitutes a "False Alarm" and Why

In the context of drones operating in shared airspace—whether the pilot is clueless, careless, or criminal—the term "false alarm" is often misunderstood. Many assume that if a detected drone isn't a direct threat, it must be a false alarm. But that's not the case.

A robust perimeter intrusion detection system—especially one that covers both ground and air domains—is expected to detect and identify all drones in its vicinity. That includes hobbyist drones, commercial platforms, and potential threats. The goal isn't to ignore non-threatening drones, but to accurately classify and assess them.

This is why advanced detection, tracking, and classification technology is essential. With the growing diversity of drone makes, models, sizes, and flight behaviors, the ability to distinguish between benign and potentially malicious drones has become increasingly complex—and increasingly critical. Effective classification enables informed decision-making, reduces unnecessary escalations, and ensures that security teams can focus their attention where it matters most.

Why False Alarms Create a Vulnerability for CI Security Teams

True false alarms create vulnerabilities for CI security teams, ranging from wasted man-hours to increased operational costs. The most serious of these problems is incident fatigue: if false alarms sound constantly, there is a risk that operators will begin to think, 'Nothing to worry about, it's just another false alarm.' This can lead to delayed response times and, more critically, a gradual desensitization among operators. When genuine threats do arise, the urgency to act may be diminished—resulting in missed opportunities to intervene and exposing the organization to significant financial and reputational risk.

Rising Attention from Authorities Signals a New Era of Airspace Security

As the operational implications of drone activity become clearer, federal agencies and national security leaders are responding with increased urgency. The FAA, for example, has been testing drone detection systems at airports for several years, and is now expanding these efforts to off-airport locations in New Mexico, North Dakota, and Mississippi. These trials involve hundreds of drones—both commercial and recreational—operating in real-world scenarios, highlighting a shift toward scalable, field-tested solutions for airspace awareness.

This growing investment in detection capabilities reflects mounting concern at the highest levels of government. Former FBI Director Christopher Wray, speaking before a U.S. Senate panel, called the drone threat "steadily escalating," noting it had intensified following the publicity surrounding the attempted assassination of Venezuelan President Maduro using explosive-laden drones.

Meanwhile, former CISA Assistant Director Brian Harrell offered a blunt assessment as early as 2019: "This is not an emerging threat. This was emerging five years ago. This is here. It is now… The overhead threat for attack is absolutely real today."

For operators of critical infrastructure, these signals point toward a clear trajectory: drone detection is no longer optional. In the wake of high-profile airport incidents and increasing visibility into the potential for airspace misuse, regulatory expectations are rising, and CI sites should prepare for a future where drone detection and classification are standard components of perimeter security.

Is Your Site More Susceptible to False Alarms?

While airports have received much of the public and regulatory attention around drone-related false alarms—largely due to high-profile incidents and the obvious risks associated with dense air traffic—they are far from the only critical infrastructure sites affected. In fact, what makes a site vulnerable to false alarms is not just traffic volume, it is proximity to "drone-like" airborne objects, such as birds, balloons, or weather phenomena.

Utilities, energy producers, oil and gas facilities, and nuclear plants have all reported concerns:

- **Nuclear Facilities:** The U.S. Nuclear Regulatory Commission has acknowledged the potential threats drones pose to nuclear power plants, emphasizing the need for vigilance and reporting of unauthorized drone sightings.
- **Energy Infrastructure: I**n July 2020, a modified drone was discovered near a Pennsylvania power substation , equipped in a manner suggesting an intent to disrupt operations. This incident marked the first known attempt to target U.S. energy infrastructure using a drone.
- **Oil and Gas Platforms:** Norway's Petroleum Safety Authority has urged increased vigilance after unidentified drones were observed near offshore oil and gas installations, warning of potential risks to safety and operations.

These examples demonstrate that the threat—and the potential for false alarms—extends well beyond airports, especially as the skies become increasingly crowded with commercial, recreational, and potentially hostile drones. Addressing this challenge requires precision detection technologies capable of distinguishing real threats from harmless objects across a wide range of environments and operational contexts.

Addressing the Limitations of Conventional PIDS in the Drone Era

How can critical infrastructure sites respond to the growing challenge of drones? Traditional security systems—designed for ground-level threats—are increasingly outmatched in the face of airborne risks. Most rely on thermal sensors, RF detectors, and human patrols, which are not only vulnerable to false alarms but can also miss or misclassify fast-moving, low-signature aerial objects. Cameras, for instance, often struggle to distinguish between drones and similarly sized objects like birds or debris.

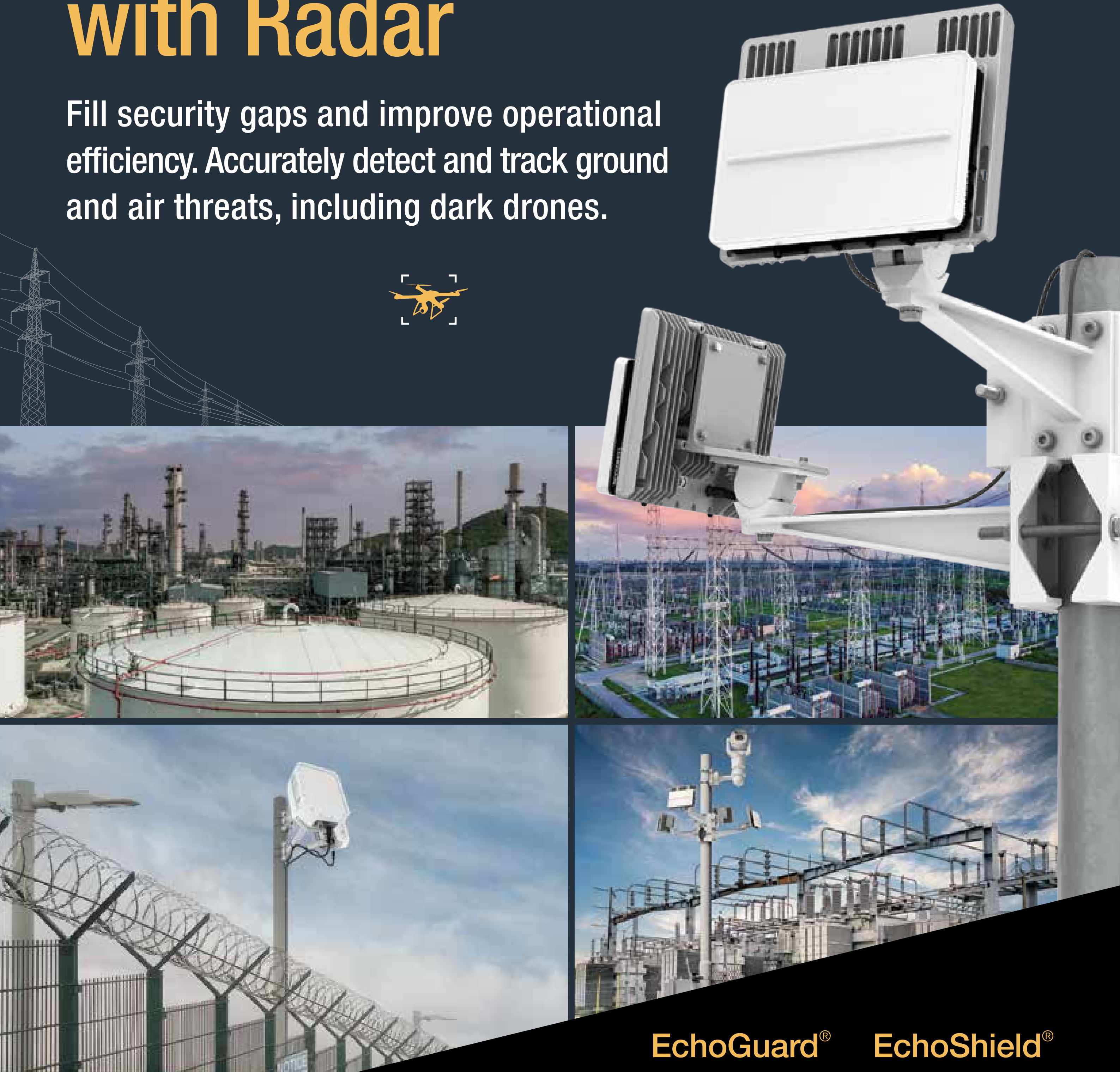
Addressing this modern threat landscape requires a layered approach, combining detection, tracking, and classification with high-performance technology layers that support future-state mitigation. In this framework, advanced drone detection radar systems play a central role—bringing the precision and persistence needed to identify, classify, and respond to airborne intrusions in real time. Unlike conventional radar designed for ground-based movement, modern airspace-focused radar systems are built for high transmit and receive density, allowing them to continuously and precisely interrogate the entire field of view—even in cluttered or obstructed environments.

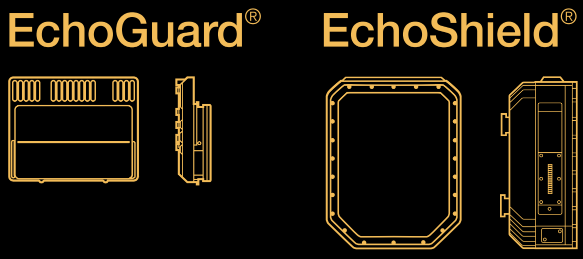
This enhanced radar capability provides far more than just detection. By analyzing size, speed, altitude, and flight behavior in real time, and when combined with optical and classification capabilities, radar helps operators distinguish between benign activity and true threats—minimizing false alarms and enhancing situational awareness. Crucially, radar performs reliably day or night, in all weather conditions, and does not depend on visible signatures or RF emissions. This makes it especially effective against so-called 'dark drones'—unmanned systems designed to evade detection by flying silently and without emitting RF signals. These drones are increasingly favored by criminal actors for their ability to bypass traditional surveillance tools such as cameras, RF sensors, and optical systems.

Modern radar systems can track multiple airborne targets at once and leverage micro-Doppler capabilities to detect subtle flight behaviors—such as drones flying in tight formation, loitering in place, or slowly approaching with potential payloads. Additionally, today's advanced drone detection radar is more compact, affordable, and easily deployable than ever before. Facilities like airports, substations, and water treatment plants can install multiple radar units to create overlapping coverage zones, even in complex layouts.

Other technologies play a valuable supporting role alongside radar, depending on the specific needs and layout of a given site. Optical sensors, such as pan-tilt-zoom (PTZ) cameras, are especially effective complements to radar, providing visual confirmation and enabling continuous monitoring once a target is detected. Additional sensors—such as thermal imaging systems and RF detection technologies for identifying drones that emit radio signals—can further strengthen the detection stack. When RF signals are catalogued and analyzed, they can also add meaningful value by helping to triangulate or trace the location of a drone's pilot, offering an additional layer of operational intelligence. Together, these tools provide layered coverage and enhance overall situational awareness.

To move beyond the limitations of conventional perimeter systems, critical infrastructure sites must adopt purpose-built technologies for today's airspace threats. Advanced radar designed




EchoGuard®
EchoShield®

specifically for drone detection is foundational to this shift, offering the precision, speed, and data richness required to manage a modern threat environment.

This level of precision becomes even more important in jurisdictions where mitigation is legal, as safely intercepting or neutralizing a drone demands real-time data on its size, velocity, flight path, and behavior. Only high-performance radar offers the responsiveness and fidelity necessary to inform proportionate, accurate, and legally defensible mitigation tactics.

Reducing False Alarms is Foundational for Modern Critical Infrastructure Protection and Resilience

For critical infrastructure security operators, the urgency to address false alarms—across personnel, systems, and overall security strategy—has never been greater. Every false positive consumes time, depletes resources, and reduces the impact of active site security efforts. It's no longer enough to ask whether your PIDS is functioning—it's time to ask whether it's keeping up with the reality of today's threats.

The threat has taken to the skies. Drones have rapidly evolved from hobbyist gadgets into instruments of espionage, disruption, and potential destruction. Site operators, policymakers, and security stakeholders must adapt to this new operational environment—one that demands new rules, new technologies, and new urgency.

A layered perimeter intrusion detection system, anchored with advanced radar that detects, tracks and classifies drones with precision delivers the situational awareness required to cut through the noise, drastically reduce false alarms, and free operators to focus on real threats. In doing so, they not only enhance site security, but also help protect the essential systems our modern world depends on. The path forward is clear: to defend what matters most, we must rise above outdated approaches—and start protecting the airspace as vigorously as we do the ground.

Tsunami alert highlights worth of global early warning system

Early warning systems kicked in overnight on 30 Jul 2025 across Pacific coastal communities after a massive earthquake in eastern Russia triggered a sea surge that reached the Japanese coastline around 1,000 kilometres (620 miles) away within about an hour, disaster relief experts said on Wednesday.

While the UN-backed International Atomic Energy Agency (IAEA) reported that there had been no damage to Japan's nuclear facilities after an 8.8 magnitude quake was recorded off Russia's Kamchatka Peninsula, coastal communities have been taking no chances and evacuating to higher ground or moving further inland.

Alerts were sent out within a few minutes of the Russia quake, the UN Office for Disaster Risk Reduction (UNDRR) confirmed. Although the authorities have now downgraded the threat across Japan as waves of 1.3 metres (4ft 2in) have been recorded, the advice is for people to stay in shelters until the danger diminishes from continuing sea surges.

"It is very complex; we are observing the tsunami data in real time, so we need people to stay at the shelter until the tsunami is completed," said tsunami engineer Professor Fumihiko Imamura from Tohoku University.

Deadly legacy

In the Asian island nation, memories are still raw from the 11 March 2011 Tohoku earthquake and tsunami which killed more than 18,000 people.

Just last year, the 7.6 magnitude Noto quake left approximately 500 dead and damaged 150,000 homes.

The disaster in 2011 also caused a major accident at the Fukushima Daiichi Nuclear Power Plant, forcing tens of thousands of people from their homes.

Today's developments come amid reports that the latest earthquake was among the 10 most powerful ever recorded, hence why the authorities are monitoring its impact so closely.

So far, alerts have been triggered off the west coast of the United States, in South America from Chile to Mexico and from Papua New Guinea to Vanuatu in the Pacific.

"A 8.8 magnitude earthquake is a very large earthquake," explained Kamal Kishore, Special Representative of the UN Secretary-General for Disaster Risk Reduction.

"As you go from magnitude eight to nine, or seven to eight, at every step the strength of the earthquake increases exponentially. So, an earthquake which is magnitude eight as opposed to seven would be 30 times bigger."

Faster than a jet liner

Speaking to UN News, Mr. Kishore highlighted the huge distances tsunamis can cover, picking up enormous energy they then dump on coastal communities.

Their progress can be as fast as a passenger jet and can be tracked by deep sea pressure change sensors, or tsunameters, that are connected to surface buoys which relay information in real time to satellites. This data is then modelled by national weather centres, influencing whether alerts are issued.

"It's a real threat because the tsunamis travel really fast from one coast to the other," continued Mr. Kishore.

"The Indian Ocean tsunami of 2004 was one of the most devastating in our memory, which travelled from all the way from the coast of Indonesia to the Sri Lankan shores within a little over an hour."

Lessons learned

In addition to the coordination role of UNDRR in the global early warning system, other UN entities also closely involved include the World Meteorological Organization (WMO) and the Intergovernmental Oceanographic Commission of the UN agency for Education, Science and Culture (UNESCO-IOC).

UK and allies expose China-based technology companies for enabling global cyber campaign against critical networks

In a new advisory published today, the National Cyber Security Centre (NCSC) – a part of GCHQ - and international partners from twelve other countries have shared technical details about how malicious cyber activities linked with these China-based commercial entities have targeted nationally significant organisations around the world.

Since at least 2021, this activity has targeted organisations in critical sectors including government, telecommunications, transportation, lodging, and military infrastructure globally, with a cluster of activity observed in the UK.

The activities described in the advisory partially overlaps with campaigns previously reported by the cyber security industry most commonly under the name Salt Typhoon.

The data stolen through this activity can ultimately provide the Chinese intelligence services the capability to identify and track targets' communications and movements worldwide.

The advisory describes how the threat actors have had considerable success taking advantage of known common vulnerabilities rather than relying on bespoke malware or zero-day vulnerabilities to carry out their activities, meaning attacks via these vectors could have been avoided with timely patching.

The Drones Revolution and Its Implications for Modern Ground Warfare with Special Focus on Critical Infrastructure Protection & Resilience

The FPV (First Person View) drone revolution is fundamentally transforming not only modern ground combat but also the landscape of homeland security and national infrastructure protection. These are not merely new weapons widely available on the battlefield—they represent a paradigm shift in how military forces, governments, and critical infrastructure operators must assess and respond to threats. Their growing use by state and non-state actors has exposed new vulnerabilities across energy grids, transportation networks, command centers, and civilian populations.

Strategic Background

In summer 2023, Ukraine launched a counteroffensive based on NATO doctrine—conventional forces, armored spearheads, and combined arms maneuvers. This approach largely failed against Russian defenses saturated with mines, electronic warfare (EW), and massive use of FPV drones. This failure highlights the doctrinal gap: Western military concepts have not adapted fast enough to the disruptive effect of low-cost, precision-guided FPV munitions, especially in how they undermine the protection of logistical hubs and civilian support zones.

The Unique Nature of FPV Weaponry

1. Human-Guided Precision

FPV drones are operated manually by pilots using real-time visual feedback, allowing for dynamic targeting even in complex, urban, or concealed environments—often including critical infrastructure sites.

2. Tactical Flexibility

They can engage moving targets, bypass fortifications, and hit soft spots such as antenna towers, fuel tanks, and backup generators with surgical accuracy.

3. Asymmetrical Advantage

A $400 drone can disrupt or destroy assets worth millions, from substations to mobile HQs. This changes the strategic cost-benefit calculus.

4. Mass Deployment

FPVs can be produced en masse, enabling saturation attacks against multiple infrastructure points or layered defense perimeters.

Operational Lessons from the Field – Updated June 2025

Ukraine-Russia War

- Russia and Ukraine both target each other's energy grids, ammunition depots, and communications nodes with FPV drones, recognizing their value in undermining operational continuity.

- Drone operators now operate as independent cells, often focusing on disruption of rear logistics and command structures rather than just frontline engagements.

Gaza Conflict (2023–2025)

- FPV drones were used to target IDF communications posts, armored vehicles, and power-distribution equipment inside urban zones.

- Israel's response included hardened perimeter protections around field HQs and power infrastructure, and the introduction of AI-assisted detection of drone threats.

Other Fronts

- In conflicts across Yemen and Sudan, drones have been used to destroy critical civilian water pumps, road chokepoints, and fuel convoys.

- Hezbollah has reportedly developed doctrine to paralyze northern Israeli road and electrical infrastructure in future conflicts using swarms of FPVs.

Implications for Critical Infrastructure Protection and Civil Defense

The proliferation of FPV drones introduces a new class of threat to essential services and infrastructure previously considered safe behind the frontlines. Their agility, affordability, and precision make them ideal tools for attacking power plants, bridges, hospitals, emergency control rooms, and national data centers.

Infrastructure protection must evolve:

- Site hardening strategies should include electronic shielding, physical barriers, and redundancy.
- Drone Defense Zones (DDZs) must be implemented around high-value assets, integrating radar, optical tracking, acoustic sensors, and kinetic or laser interceptors.
- Business continuity and resilience planning must incorporate drone attack scenarios as baseline threats.
- Emergency response protocols should include mass-casualty and mass-disruption drone events.

Recommendations for NATO, EU, and Allied Forces

1. Make the protection of critical infrastructure from drone threats a strategic-level priority.

2. Mandate the establishment of DDZs around national utilities and emergency centers.

3. Build integrated civil-military C4I systems for early detection and rapid counter-drone engagement.

4. Require national and regional resilience assessments to include swarm drone attacks.

5. Standardize training and certification of drone operators and counter-drone units.

6. Share intelligence and cross-border coordination protocols for drone threats.

Author: Brigadier General (Res.) Avi Bachar is a former Chief of Staff of the Israeli Home Front Command and former Chairman of Israel’s National Emergency Management Authority (NEMA). He currently leads IsraTeam, a consultancy specializing in emergency management, civil defense, and national resilience strategy.

NATO CCDCOE publishes new policy brief on cyber threats to maritime port infrastructure

The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has published a new policy brief, “Addressing State-Linked Cyber Threats to Critical Maritime Port Infrastructure,” which assesses the cybersecurity posture and challenges facing maritime port infrastructure and offers recommendations for strengthening NATO’s maritime cyber defence.

Maritime ports handle approximately 80% of global trade and serve as vital nodes in NATO’s defence logistics network. However, they are increasingly threatened by sophisticated cyber operations carried out by state-linked actors. The authors of the brief note that recent intelligence indicates a high frequency of cyberattacks targeting port facilities across Europe and the Mediterranean, with many of these attacks attributed to threat actors originating from Russia, Iran, and China.

The policy brief on maritime port infrastructure provides an overview of the challenges of digitalisation in the maritime sector demanding coordination between the traditional industrial control systems and contemporary digital solutions; the threat landscape from state-sponsored advanced persistent threats to financially motivated cybercriminals and the policy gaps in current cybersecurity frameworks.

The researchers point out that maritime port cybersecurity requires immediate policy intervention to establish sector-specific intelligence sharing networks, coordination mechanisms, and resilience standards.

E-GIANTS Project Concludes Study on GNSS Authentication and Security Improvements

The E-GIANTS (European GNSS Improved Authentication Solutions) project was commissioned by the European Commission and technically supervised by EUSPA. The project responds to the growing threat posed by quantum computing to traditional cryptographic methods, which could compromise the security of GNSS services in the coming decade. The study highlights that while quantum computers threaten classic asymmetric cryptography (like RSA and ECDSA), symmetric mechanisms—properly configured—remain secure, guiding the project's design choices.

The project's scope encompassed three main work objectives:

1. SBAS and OSNMA Key Management: Focused on developing a comprehensive authentication solution for Satellite-Based Augmentation Systems (SBAS) and the Galileo OSNMA (Open Service Navigation Message Authentication) service, using symmetric cryptography to ensure bandwidth efficiency and post-quantum resilience. The solution centres on a TESLA-based (Timed Efficient Stream Loss-tolerant Authentication) protocol, optimised for low authentication latency (about 1 second) and robust message recovery using Reed-Solomon encoding.

2. Additional Dissemination and Improvements of OSNMA: Proposed and validated improvements to the Galileo OSNMA protocol, including the distribution of cryptographic material via secure internet protocols (MQTTS and NTPs) for receivers with connectivity. These enhancements reduce authentication delays, improve cold-start performance, and introduce strategies for cross-constellation authentication, paving the way for integrating GPS and Galileo authentication in the future. The project also explored post-quantum resistant Merkle tree architectures for OSNMA, though further study is needed for large-scale deployment.

3. SBAS Authentication for Non-Aviation Users: Extended authentication solutions to new SBAS services (EGNOS-Next), particularly for non-aviation sectors like maritime, road, and rail. The approach adapts the TESLA-based protocol to high data rate channels (E5C/E5D), ensuring rapid, authenticated access to critical navigation and integrity messages for a broader user base.

Key outcomes of the project include:

- Post-Quantum Resilience: By relying on symmetric cryptography and hash-based structures, the solutions are designed to withstand attacks from future quantum computers, avoiding the bandwidth-heavy hybridisation of classic and post-quantum asymmetric algorithms.

- User-Centric Design: Extensive stakeholder interviews shaped requirements, emphasising minimal receiver hardware/ software impact, low authentication delays, and standardised, interoperable solutions.

- Enhanced OSNMA Protocol: The project identified improvements to the OSNMA framework, including asynchronous broadcasting of subframes across the Galileo constellation. This ensures more consistent authentication performance, even in areas with limited satellite visibility. Additionally, the proposal for cross-constellation authentication aims to extend OSNMA's capabilities to non-Galileo satellites, enhancing its versatility.

- Secure Data Distribution: A new method for distributing cryptographic material to GNSS receivers with internet connectivity was introduced, identifying MQTTS (Message Queuing Telemetry Transport over TLS) and NTPs (Network Time Protocol) as the most suitable network protocols. The implementation of non-SIS services, either independently or in conjunction with SIS, was found to improve authentication, especially in challenging environments.

- System-Level Roadmap: A detailed deployment plan was developed, outlining a roadmap for standardisation, prototyping, and phased implementation, aligning with EGNOS V3 service upgrades and future GNSS receiver capabilities. The roadmap emphasises security analysis, system design, and integration with existing GNSS infrastructure.

- Key Management Innovations: The project addressed vulnerabilities in current cryptographic practices, including the risk of quantum computing threats to classical asymmetric algorithms like ECDSA. Recommendations for resilient key management strategies were proposed to future-proof authentication systems.

By integrating these advancements, the project underscores the importance of robust authentication in maintaining the integrity of GNSS services. The findings and technical proposals from E-GIANTS will contribute to the evolution of Galileo and EGNOS's capabilities, ensuring its role as a trusted enabler for critical infrastructure across Europe and beyond.

The E-GIANTS consortium recommends further prototyping and experimentation to validate full-scale implementations, as well as continued analysis of internet-based cryptographic material distribution and time synchronization services. Standardization activities are underway to harmonize these authentication mechanisms across European and global SBAS systems.

Galileo Open Service Navigation Message Authentication adds another layer of protection against GNSS interference

GNSS interference is on the rise, with spoofing signals every day, providing unreliable or even fake positioning information.

When spoofing tricks our smartphone or vehicle navigation system into believing it is metres, if not kilometres, away from its actual location, it's a nuisance. When it targets critical applications in sectors such as transportation, finance or telecommunications, it can lead to important service disruptions with associated economic losses. In sectors such as aviation or maritime, this can lead to serious safety risks.

An added layer of protection

The Galileo Open Service Navigation Message Authentication, or OSNMA, is a new authentication mechanism that lets Galileo Open Service users verify the authenticity of their GNSS information. It will be available on 24 July.

"With OSNMA, we increase assurance that the data users receive is indeed coming from Galileo and has not been modified in any way," says EUSPA Executive Director Rodrigo da Costa.

While the OSNMA does increase the ability to detect spoofing events, it does not prevent their occurrence. Nor does it protect against jamming. "Nonetheless, by amplifying the overall robustness and resilience of the Galileo Open Service, this added layer of protection helps keep users one step ahead of hackers," adds da Costa.

Galileo is the first GNSS system to offer protection from spoofing attacks as part of its Open Service worldwide. The OSNMA declaration of service follows an extensive testing phase where GNSS manufacturers, integrators and application developers utilised the Signal in Space (SiS) to assess the service's performance across a range of scenarios and use cases.

Giving Galileo signals a unique digital signature

An integral function of the Galileo Open Service, OSNMA provides data authentication to all enabled receivers. Specifically, the OSNMA authenticates data for geolocation information from the Open Service through the Navigation Message (I/NAV) broadcast on the E1-B signal component. This is realised by transmitting authentication-specific data in the previously reserved fields of the E1 I/NAV message.

By using these previously reserved fields, OSNMA does not introduce any overlay to the system; thus, the OS navigation performance remains untouched.

When OSNMA-enabled receivers receive the signals, they can decode the cryptographic data and, thanks to a previously downloaded public key, verify the authenticity of the position and time data.

Because the OSNMA is transmitted in the Galileo Open Service signal, which is already used in most devices, receivers only need to implement the protocol and download the certified public keys from the European GNSS Service Centre (GSC) website. OSNMA relies as well on the implementation of a trusted time source to start up the protocol, accurate to at least five minutes, and a dedicated logic on the receiver side to guarantee the end-to-end authentication process. The service does not require the storage and management of secret keys on the user side, which facilitates the adoption in different communities. All details can be found in the OSNMA Receiver Guidelines.

The Galileo OSNMA delivers

OSNMA also makes Galileo signals unpredictable, thereby making them difficult to replay. This, combined with basic consistency checks in the receiver and the authentication service in general, makes spoofing an OSNMA-enabled receiver considerably more challenging.

For those segments that rely on accurate positioning information – automotive, timing and synchronisation, professional, maritime, aviation, drones – this is nothing short of a game-changer. Furthermore, and in the context of the frequent spoofing events experienced in recent years, Galileo OSNMA is now being included in the standards for civil aviation receivers, the first step for its adoption by the civil aviation community.

"Stakeholders have clearly articulated the need for more robust GNSS services," concludes da Costa. "The Galileo OSNMA delivers this robustness and, in doing so, provides enhanced security in positioning and timing solutions."

"The OSNMA Initial Service declaration has been authorised by the EU Space SAB following independent security checks and cooperation with the Programme to define risk mitigation measures. The cooperation between the SAB, the Commission and EUSPA was instrumental to getting through this very important milestone." Philippe Bertrand, EU Space Security Accreditation Chair.

"With this new capability, the EU is delivering on its commitment to provide secure, reliable space infrastructure that supports critical sectors and protects users across the globe", says Christoph Kautz, Director for Satellite Navigation and Earth Observation, at DG DEFIS, European Commission

The OSNMA will be provided by EUSPA, which serves as the Galileo service provider.

Source: European Union Agency for the Space Programme (EUSPA)

New asset inventory guidance for operational technology (OT) owners and operators

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), and partners the Cybersecurity and Infrastructure Security Agency (CISA), in partnership with the National Security Agency (NSA), Federal Bureau of Investigation (FBI), Environmental Protection Agency (EPA), Canadian Centre for Cyber Security (Cyber Centre), Germany's Federal Office for Information Security (BSI), Netherlands' National Cyber Security Centre (NCSC-NL), and New Zealand's National Cyber Security Centre (NCSC-NZ) has released new guidance in collaboration with our international partners for OT owners and operators. Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators helps critical infrastructure organisations identify which assets to secure and protect, forming a basis to organise their defences and reduce the risk of a cyber security incident.

The guidance outlines a process for OT owners and operators to create an asset inventory and taxonomy. It also outlines how OT owners and operators can maintain, improve, and use their asset inventory to protect their most vital assets.

An asset inventory is an organised, regularly updated list of an organisation's systems, hardware, and software. For OT environments, a key part of creating an asset inventory is developing a taxonomy – a system that classifies assets based on function and criticality. Using a taxonomy allows OT owners and operators to structure and prioritise OT assets, help identify risks, and manage vulnerability and incident response.

World Border Security Congress

14th-16th April 2026

Vienna, Austria

www.world-border-congress.com

Developing Border Strategies Through Co-operation and Technology

SAVE THE DATES

Co-hosted by:

Austria's border security faces a complex set of challenges, largely stemming from its geographical location and its participation in the Schengen Area. A primary concern is managing irregular migration flows, which fluctuate significantly due to geopolitical instability in various regions. This puts pressure on Austria's capacity to effectively screen and process asylum seekers.

The inherent nature of the Schengen Area, while facilitating free movement, also presents vulnerabilities. The potential for secondary migration, where individuals move from one Schengen state to another, necessitates close cooperation with neighbouring countries. However, differing national policies and capacities can complicate these efforts.

Furthermore, the rise of transnational crime, including human trafficking and smuggling, adds another layer of complexity to border security. Austrian authorities must balance the need for stringent controls with the imperative to uphold human rights and international obligations.

The evolving security landscape, with threats such as terrorism and hybrid warfare, also requires constant adaptation of border security measures. This necessitates investment in advanced surveillance technologies and enhanced intelligence sharing. The need to maintain public confidence in border security, while respecting the principles of open borders within the EU, creates a delicate balancing act for Austrian policymakers.

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 Vienna, Austria on 14th-16th April 2026 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

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

for the international border management and security industry

Supported by:

OSCE Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

African Young People Support Center

ISIO

NS&RC

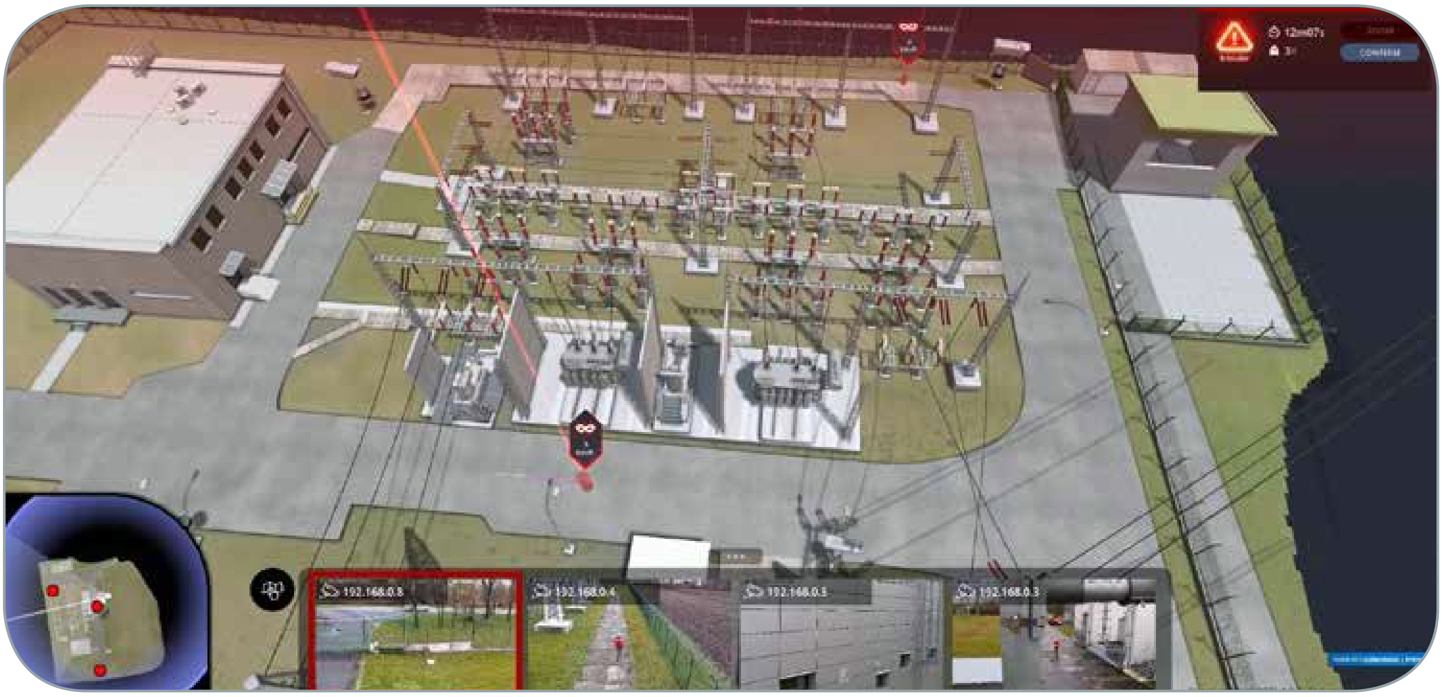
Media Partners:

World Border Security Network

BORDER SECURITY REPORT

World Security-index.com

Digital twins: The new pillar of critical infrastructure security



By Nick Karakulko, senior director of critical infrastructure protection solutions for Hexagon's Safety, Infrastructure & Geospatial division.

In an era defined by rapid technological advancement and increasingly sophisticated threats, the security of critical infrastructure has never been more important -- or more challenging.

From power grids and water treatment plants to airports, seaports, transportation networks, and communication systems, the lifelines of modern society are under constant risk from attacks, natural disasters, and system failures.

To stay ahead of these threats, the adoption of cutting-edge technologies is not a luxury but a necessity. Among these technologies, 3D digital twins have emerged as a powerful new tool for ensuring the resilience and security of critical infrastructure. And now, with the integration of LiDAR and PTZ (pan-tilt-zoom) camera systems, digital twins are redefining perimeter protection, offering unprecedented capabilities for detecting and tracking intruders in 360-degree zones.

A digital twin is a virtual replica of a physical asset, system, or environment that can be used to monitor, simulate, and optimize operations in real time. When combined with 3D modeling, LiDAR, and PTZ cameras, these digital twins provide an immersive, detailed and dynamic representation of infrastructure systems, enabling a level of precision and situational awareness that traditional security measures simply cannot achieve.

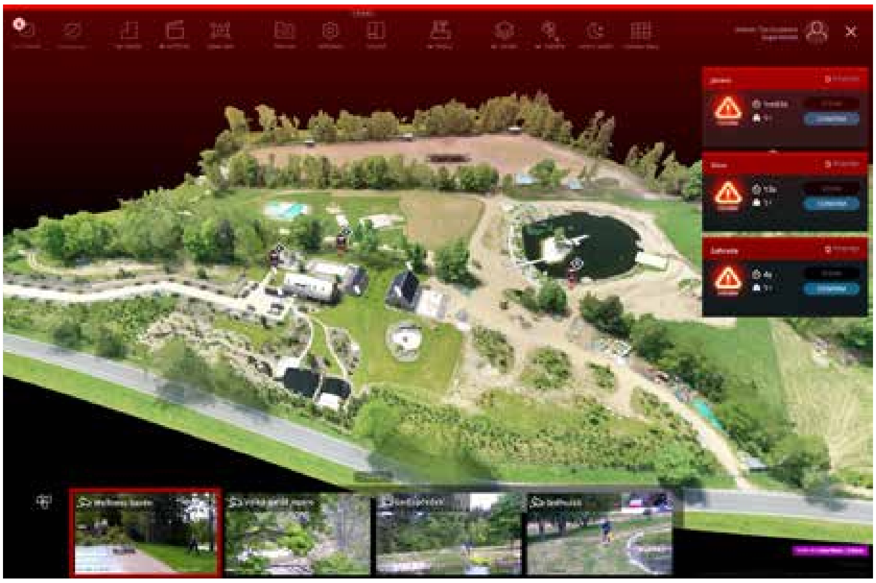
3D volumetric surveillance

Unlike traditional 2D camera setups, which are limited to flat, two-dimensional views and often struggle with blind spots, 3D volumetric systems provide a comprehensive, 360-degree understanding of the physical environment.

LiDAR, or Light Detection and Ranging, uses laser pulses to generate highly accurate 3D maps of an area, capturing details down to a few millimeters. When paired with PTZ cameras, which can dynamically zoom in on and track objects of interest, and integrated into a digital twin, these systems become even more powerful. The result is a living, breathing security model that continuously updates in real time, offering unparalleled insight into potential threats.

For example, imagine a power plant with a sprawling perimeter. A traditional 2D camera system might struggle to detect an intruder in low-light conditions or account for obstructions like trees or uneven terrain. A 3D volumetric system, by contrast, can detect and identify intruders with pinpoint accuracy regardless of environmental factors.

LiDAR provides the foundational 3D spatial data, and PTZ cameras enhance the system's ability to zoom in, track, and even classify intruders based on their size, speed, and movement patterns. This layered approach not only improves detection rates but also reduces false alarms, a common issue with traditional systems.



A large utility that supplies electricity to 2.7 million people recently piloted the latest in LiDAR-based 3D technology to secure its substations and power lines.

The project used five strategically placed LiDAR sensors to create secure zones, including perimeter fences. These zones can be switched on and off or changed at the click of a button or drag of the mouse. For example, when maintenance is being carried out, the zone in which the work is taking place can be deactivated. Meanwhile, other areas remain live to prevent workers from straying into an unauthorized or potentially hazardous area.

Situational awareness and response

Using LiDAR and digital twin technology, security teams can now visualize threats in three dimensions, giving them a deeper understanding of the spatial relationships between intruders and critical assets. This capability is particularly valuable in complex environments, such as airports or large campuses, where traditional 2D systems might struggle to provide actionable intelligence.

Digital twins also allow operators to simulate intrusion scenarios and test response strategies in a virtual environment. For instance, they can model how an intruder might navigate a facility's perimeter, identify potential blind spots, and adjust security measures accordingly. This proactive approach ensures that security teams are not just reacting to threats but actively preparing for them.

Reducing costs, improving efficiency

Traditional 2D camera systems often require extensive infrastructure, including multiple cameras to cover blind spots and additional personnel to monitor feeds.

In contrast, a single digital twin powered by LiDAR and PTZ cameras can provide comprehensive coverage with fewer resources. Additionally, the reduction in false alarms translates to significant savings in time and manpower, allowing security teams to focus on genuine threats.

As with other digital twin applications, the integration of LiDAR and PTZ systems enhances collaboration among stakeholders. The 3D volumetric data captured by these systems can be shared in real time with government agencies, private operators, emergency responders, and regulatory bodies, ensuring that all parties have a shared, accurate, and actionable understanding of the situation. This unified perspective enables faster decision-making and more effective coordination during critical incidents.

Strategic imperative

The integration of 3D digital twins with LiDAR and PTZ camera systems represents a monumental leap forward in critical infrastructure security. By combining the precision of LiDAR, the dynamic tracking capabilities of PTZ cameras, and the real-time intelligence of digital twins, organizations can achieve unparalleled levels of perimeter protection and situational awareness.

As threats to critical infrastructure continue to evolve, so must our defenses. The adoption of 3D volumetric perimeter protection is not just a technological upgrade, it is a strategic imperative. By investing in these advanced systems, we can ensure the safety and resilience of the infrastructure that underpins our society, protecting it against the challenges of today and the uncertainties of tomorrow.

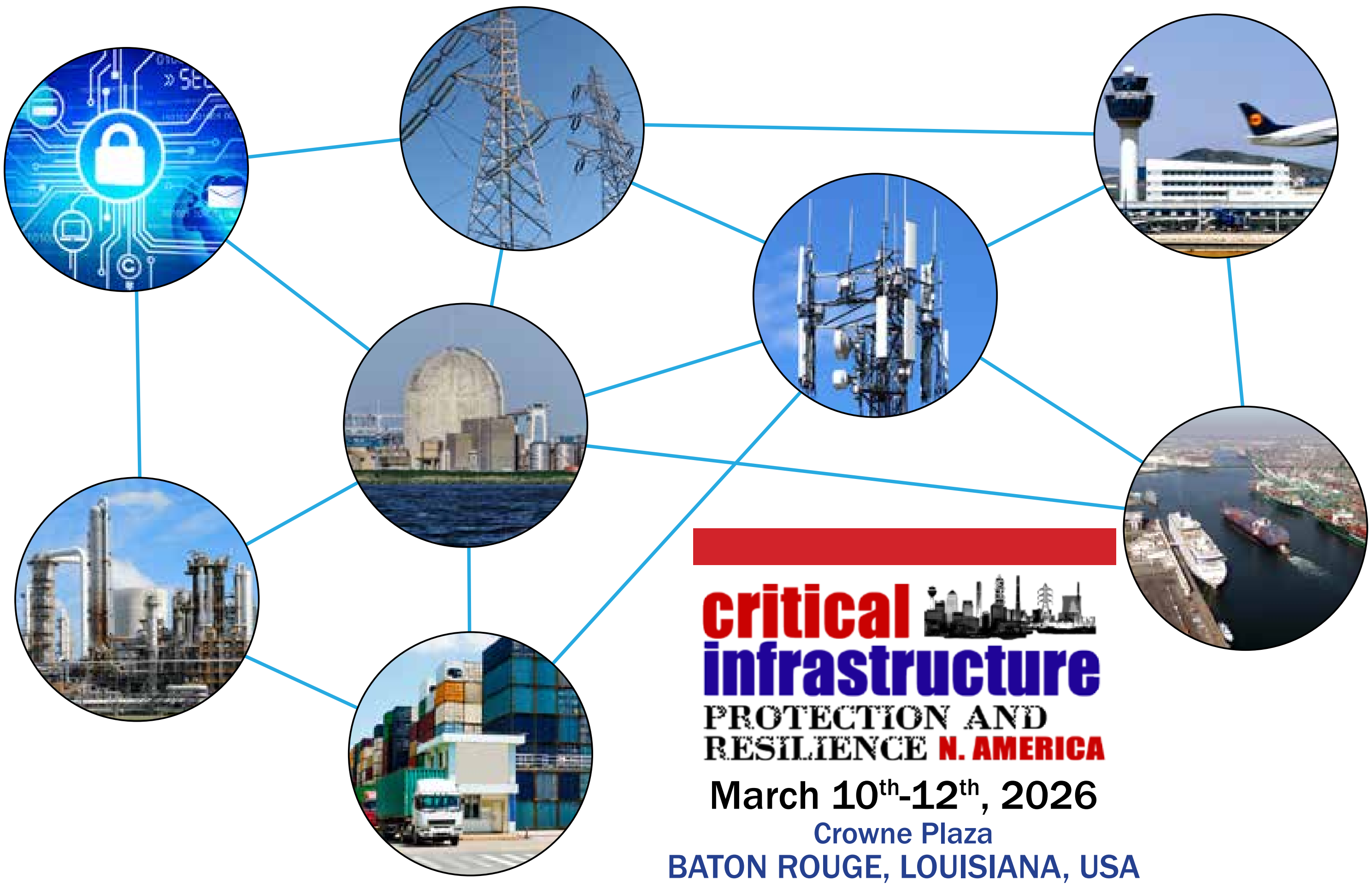
The future of security is here, and it is three-dimensional.

Reducing the Cybersecurity Risks of Portable Storage Media in OT Environments | Comment on NIST SP 1334

The National Cybersecurity Center of Excellence has developed the draft two-pager NIST Special Publication (SP) 1334, Reducing the Cybersecurity Risks of Portable Storage Media in OT Environments. The cybersecurity considerations in this two-pager are intended to help operational technology (OT) operators and manufacturers use Universal Serial Bus (USB) devices securely.

Portable storage media can be used to transfer data physically to and from OT environments. USB storage devices are convenient, but their use poses potential cybersecurity risks for organizations that utilize them in their OT environments. Organizations can reduce these risks with secure physical and logical controls on the access, storage, and usage of USB devices.

The NCCoE created the OT Security Series to assist organizations in securing their OT systems. If you have any comments on this two-pager and/or recommendations for additional topics that the OT Security Series could cover, please reach out to the NCCoE Manufacturing team at manufacturing_nccoe@nist.gov.



critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 10th-12th, 2026

Crowne Plaza

BATON ROUGE, LOUISIANA, USA

A Homeland Security Event

SAVE THE DATES

Securing the Inter-Connected Society

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

The ever changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber attacks, means the need to continually review and update policies, practices and technologies to meet these growing demands.

The 7th Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

The last few years have seen the world immersed in a period with significant challenges and a great deal of uncertainty, which has stressed how important collaboration in protection of critical infrastructure is for a country's national security.

Join us for the next gathering of operators and government establishments tasked with the regions Critical Infrastructure Protection and Resilience.

For further details visit **www.ciprna-expo.com**

To discuss sponsorship opportunities contact:

Bruce Bassin
(Americas)
E: bruceb@torchmarketing.co.uk
T: +1-702-600-4651

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

The premier discussion for securing America's critical infrastructure

Owned & Organised by:

TORCH

Supporting Organisations:

International Association of CIP Professionals

NS&RC

IACI INTERNATIONAL ASSOCIATION OF CERTIFIED ISAOs

ISIO

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Legal and Regulatory aspects relating to the physical security of the telecommunications infrastructure used for critical communication services

White paper published by TCCA's Legal and Regulatory Working Group, March 2025

Evidence from around the world indicates that threats to Mobile Network Operators (MNOs) are increasing, including to their physical infrastructure. On the other hand, critical communications are transitioning from legacy networks, primarily operated by governments, to broadband networks, in which key components such as Radio Access Networks are procured from MNOs or dedicated infrastructure providers. The combined effect of these two trends requires critical communications operators to pay special attention to the security of the physical infrastructure that is used for critical communications.

Given the importance of the topic, TCCA's Legal & Regulatory Working Group (LRWG) developed this white paper, starting with a survey of the legal and operational frameworks in the member countries of the LRWG.

As the laws and regulations amend and update dynamically, the survey outcomes that formed the basis of this paper were the position as of 31 January 2025.

The survey identified two potential approaches: impose security obligations through legislation/regulation, or rely on provisions in the contract between the critical communications operator and the MNO/infrastructure provider. The LRWG's assessment is that while each approach has advantages and disadvantages, a combination of these two, whereby legislation/regulation impose a minimum standard on which contractual terms build additional/advanced obligations, would serve the interests of the critical communication services best. As new legal/regulatory obligations on physical security would require additional investment, in what proportion that cost should be borne by the parties could ideally be set by the legislation/regulation in a proportional manner.

The European Critical Communication System (EUCCS) aims to set up a European-wide mission critical communication network that is based on national critical communications networks. It will require a common standard in physical security across all the participating critical communications networks, which can be ensured by the two-pronged approach stated above.

Though new legal/regulatory obligations on physical security would increase the costs and compliances of MNOs/infrastructure providers that provide services for critical communications, it would also have a salutary effect due to the improved standards of security in the network. It is highly likely that thebconsumers, particularly the business customers, will start demanding greater reassurances on all aspects of security in the network including of the physical infrastructure. From a wider national perspective, governments have started taking steps to ensure security of networks which will be complemented by legislative/regulatory obligations on infrastructure used for critical communications.

This paper is intended to draw the attention of the critical communications community to the importance of the issue of physical security and to generate a wide discourse which, it is hoped, will result in a global standard on a baseline on physical security of infrastructure supporting critical communications.

Background

In 2020 a bomb explosion at a central hub of the critical communications provider of a major developed country left emergency officials cut off from the outside world and public without access to emergency services. This incident demonstrates very strongly and very clearly the criticality of the security of physical infrastructure to the proper functioning of critical communications. Incidents of damage to undersea telecommunication cables connecting Nordic and Baltic states provide further evidence of the need to protect the physical infrastructure.

TCCA's LRWG has developed this white paper to highlight the importance of the security of physical infrastructure, as the LRWG is of the view that it is a topic to which more attention should be paid. This paper focuses on the physical security of telecommunications infrastructure, in order to facilitate further discussions in the critical communication community which it is hoped will result in a global standard on the baseline of physical security of infrastructure supporting critical communications. There are many other facets to the security of critical communication services including data/cybersecurity, which will be examined in other publications.

Most of the current critical communication networks using such technologies as TETRA, Tetrapol and P25, are owned and operated by the state. As such, their physical security is assured by the state to the extent deemed necessary. However, the ongoing transition from these networks to broadband networks has changed the operating model, as governmental agencies providing critical communication services will rely on MNO networks to some extent, including the Radio Access Network (RAN). In some instances, the critical communications services may procure services directly from infrastructure providers who are not MNOs, similar to the way MNOs procure services from them. The discussion of this paper is equally applicable to such infrastructure providers as it is to MNOs. Thus, the physical security of these network elements is of paramount importance. However, it is debatable whether the measures that MNOs are currently adopting in this regard are sufficiently robust and fit for purpose.

The paper titled 'Considerations for Government Authorities when they are planning to acquire Mission Critical Mobile Broadband Services'1 produced by TCCA's Critical Communications Broadband Group (CCBG) in 2015 identifies security as of vital importance to mission critical communications solutions.

Security is central to ensuring reliability, availability, stability and general performance of those solutions.

The paper details the need for physical security of all infrastructure and adds that "the level of perimeter security shall reflect the importance of the assets to the service including CCTV, intruder alarms, access locks, temperature control, fire and smoke detection."

The EC Council Cybersecurity Exchange has issued a paper titled 'The Role of Physical Security in Maintaining Network Security' in 20222 which states "Although physical security is absolutely critical to maintaining network security, it is among the most often forgotten aspects of protecting a network.

Physical security is defined as protecting physical access to your network and all network components, such as computers, servers, and routers."

The paper titled 'Mobile Telecommunications Security Landscape3' by GSMA, issued in 2022, identifies physical attack on the network as one of the operational security threats to networks.

Given the mandate of and the expertise within the LRWG, this paper focuses on legal and regulatory measures that are applicable to the physical security of telecommunication infrastructure. The LRWG notes that there are numerous technical and operational measures that are relevant but that remain outside the scope of this paper.

The LRWG also examined European Commission regulations which have provisions relevant to the physical security of telecommunication infrastructure.

The LRWG recommends that legislation on physical security of critical communication infrastructure, defining baseline requirements and rules for cost ceilings/sharing, be adopted as an EU directive. Such a multinational standard will greatly assist the decision-making process of individual countries and establish a common understanding between all relevant parties, including MNOs, Governments and users.

Moreover a European regulation would serve as an inspiration for the global community of critical communication operators.

For the full report download the TCCA White Paper - "Legal and Regulatory aspects relating to the physical security of the telecommunications infrastructure used for critical communication services"

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

In Collaboration with:

International Association of CIP Professionals

See below for 20% Off Special Offer

THREE TYPES OF INSIDERS - ONE TOOL TO DETECT THEM

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

BE PROACTIVE
AWARENESS TRAINING

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

BE READY
PROGRAM DEVELOPMENT TRAINING

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

An eLearning Platform dedicated to Security and the Insider Threat

www.help2protect.info

SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE

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

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

International Association of
CIP Professionals

10TH ANNIVERSARY

Celebrating 10 years of IACIPP

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is approaching its 10th year of operation and maybe it's because I am getting older but that time seems to have flown by. Over that decade, the protection and resilience of Critical National Infrastructure (CNI) has faced a rapidly evolving landscape of threats and risks. The increasing interconnectivity of infrastructure systems, reliance on global technologies, supply chains, adverse weather conditions and rising geopolitical tensions have made these systems more susceptible to various threats.

These infrastructures—spanning energy, water, transport, healthcare, and digital systems—are essential to national security, economic stability, and public welfare. As such, their vulnerability has become a focal point for both policymakers and those with malicious intent.

Some of the key changes during that time have included the necessary shift from a reactive to a proactive approach, the increased focus on resilience, the growing emphasis on collaboration and trusted partnerships between governments and private-sector entities and a drive for international partners to share information and good practices.

However, one of the most significant changes has been the surge in cyber threats. The impact of cyber-attacks on National Infrastructure has escalated dramatically, driven by geopolitical tensions, technological interconnectivity, and the rise of sophisticated threat actors.

The digital transformation of CNI sectors has introduced new vulnerabilities, particularly through the integration of legacy operational technology (OT) with modern IT systems. Many OT systems were never designed to be internet-connected, making them susceptible to exploitation.

2024 marked a record year for significant cyber incidents targeting UK infrastructure. Nearly two-thirds of UK water and energy providers experienced cyber-attacks. These incidents often target data, but the potential for disruption to physical infrastructure, such as power outages or water supply failures, is a growing concern.

The National Cyber Security Centre in the United Kingdom has warned of an "enduring and significant" threat from state-aligned groups, particularly those sympathetic to Russia amid its invasion of Ukraine and others such as China, Iran and North Korea.

Considering all these factors together we can clearly see that for all sectors of our CNI the stakes are high and the urgency in continually developing our protection and resilience posture is ever present.

Building resilience now requires a multi-layered approach: upgrading legacy systems, securing emerging technologies, preparing for climate impacts, and fostering local, regional and international collaboration.

It is here, within that collaboration space, that IACIPP has focused its efforts and attention. Our initial energies were concentrated around creating a network of Regional Directors both across Europe and further afield. They have provided a focal point for developing connectivity alongside our Web portal which 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.

As the web site matured it became obvious that there was a need for other forms of communication material to be made

Training & Education

The International Association of CIP Professionals (IACIPP) is committed to the training and further education of industry professionals to enhance knowledge, expertise and ultimately improve industry standards. See our recommended useful training courses: **www.cip-association.org/training-and-education.**

Countering Insider Threats

Help2Protect is an eLearning Platform dedicated to Security and the Insider Threat courses help you put in place a detection and prevention program against this widespread and yet largely underestimated issue.

Further details: www.cip-association.org/help2protect-an-elearning-program-to-counter-insider-threats

NIST Risk Management Framework

The purpose of these courses is to provide those new to risk management with an introduction to key publications associated with the NIST Risk Management Framework (RMF) methodology for managing cybersecurity and privacy risk.

Further details: www.csrc.nist.gov/Projects/risk-management/rmf-courses

Critical Infrastructure Protection Week in Europe
14th-16th October 2025 - Brindisi, Italy
International Association of CIP Professionals

critical infrastructure PROTECTION AND RESILIENCE NEWS
critical infrastructure PROTECTION AND RESILIENCE NEWS

available so we introduced a 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 CNI.

Our last magazine, the Winter 2024/25 edition, contained articles on subjects such as: Reducing Disaster Risks to Deliver a Resilient Future, the Return on Investment from EU Research, Terrorists Exploiting Global Tension, an Artificial Intelligence Perspective and many many more.

This year will see IACIPP host the 10th '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 Brindisi in Italy in October. Previous hosts cities have included, London, The Hague, Milan, Bucharest, Prague and Madrid.

This will also be the 2nd 'Critical Infrastructure Protection Week' in Europe. We introduced this joint venture in 2024 in Madrid in partnership with our colleagues from EU-CIP, a Horizon Project. The combination of CIPRE and EU-CIP was the first of its kind to seek to develop and inform thinking around the current challenges and the impact of new EU directives alongside the developing complexities of the threat environment against European critical entities.

The EU-CIP Project will come to a close at the end of September this year so unfortunately, they are unable to join us in Brindisi but a senior representative from IACIPP will be in attendance at their final meeting seeking to understand how we can assist in taking the findings from the programme forward.

We are, however, delighted to have 'The International Emergency Management Society (TIEMS)' conference with us this year as two key events within Critical Infrastructure Protection Week.

Over our 10-year tenure we have been fortunate to have established many valuable partnerships, with many organisations from across the globe. EU-CIP and TIEMS I have mentioned, and there have been many more, including significant levels of support from ICI Bucharest and the Confederation of European Security Services (CoESS).

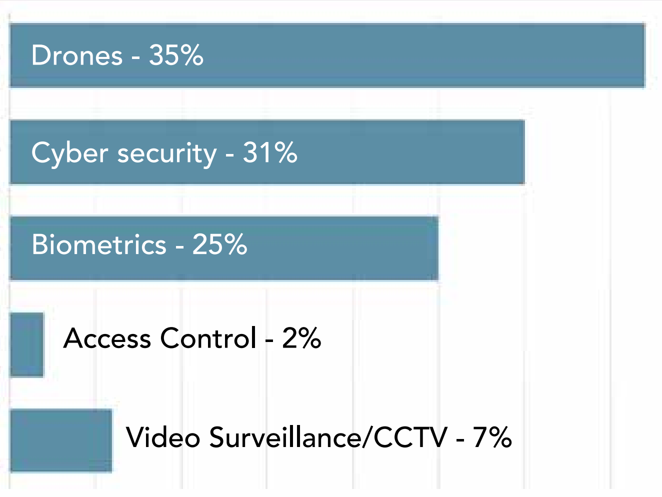
Our partners play a pivotal role in contributing to and adding significant value to both IACIPP and to the CIPRE and we look forward to continuing these relationships and reaching out to other relevant parties with whom we can collaborate.

We are looking forward to the conference in Brindisi and to celebrating CIPREs 10th anniversary. We hope that during that time we have played some small part in bringing together key decision makers and influencers to share experiences, network with industry peers and discover the latest technologies and solutions that may assist in the protection and resilience of our Critical National Infrastructure.

John Donlon QPM FSyL
Conference Chairman
Chairman, IACIPP

IACIPP Poll - Latest poll results

In which sector of the security industry do you foresee the most growth in the near future?



Aims of IACIPP

- 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 cooperation 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 visit www.cip-association.org.

critical infrastructure
PROTECTION AND
RESILIENCE EUROPE

14th-16th October 2025
Brindisi, Italy
www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

With the patronage of the City of Brindisi

Co-Hosted by:

International Association of CIP Professionals

UNIVERSITÀ DEL SALENTO
DIPARTIMENTO DI INGEGNERIA DELL'INNOVAZIONE

CRISR

Preliminary Conference Programme

Your invitation and guide to the premier event for the critical infrastructure and civil contingencies community.

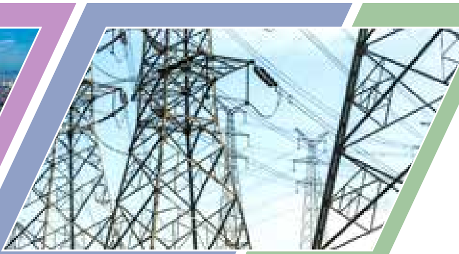
The second 'Critical Infrastructure Protection Week' will take place in Brindisi, Italy and will see IACIPP host the 10th 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'The International Emergency Management Society (TIEMS)' conference.

Join the discussions and enhance your network, help raise awareness and promote greater collaboration amongst operators, agencies and the CI security community.

Critical Infrastructure Protection Week in Europe
14th-16th October 2025 - Brindisi, Italy

critical infrastructure PROTECTION AND RESILIENCE EUROPE
14th-16th October 2025

TIEMS
13th-17th October 2025



Executive Sponsors:

AUTO-ISAC, open ENLoCC, E.DSO, EUTC, TCCA

Supporting Organisations:

CoESS, CCNE, EE-ISAC, Help2Protect, ISIO, AFRICAN SMART CITIES

Platinum Sponsor:

eset Digital Security Progress. Protected.

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

critical infrastructure
PROTECTION AND
RESILIENCE EUROPE

10th ANNIVERSARY

14th-16th October 2025
Brindisi, Italy
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.

"The EU Internal Security Strategy highlights that critical infrastructure must be better protected from criminals who take advantage of modern technologies and that the EU should continue to designate critical infrastructure and put in place plans to protect such assets, as they are essential for the functioning of society and the economy."

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.

Follow us: in

Critical Infrastructure Protection & Resilience Europe

Critical Infrastructure Protection Week *in Europe*

14th-16th October 2025 - Brindisi, Italy

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.

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.

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) has announced the launch of '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 lastest issues, policies and challenges facing the security of Europe's critical national infrastructure (CNI), as well as thelatest following the implemenation 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 Brindisi, Italy for Critical Infrastructure Protection and Resilience Europe and join the great debate on securing Europe's critical infrastructure.

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

Critical Infrastructure Protection Week *in Europe*

International Association of CIP Professionals

14th-16th October 2025 - Brindisi, Italy

critical infrastructure PROTECTION AND RESILIENCE EUROPE

Schedule of Events

Tuesday 14th October 2025

9am - 12.00pm - Site Visit - Port of Brindisi

9.30am - 12.30pm - AYPSC Workshop - Africa–Europe Cooperation for Critical Infrastructure Resilience

2.00pm - 3.30pm - Joint Opening Keynote

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

4.00pm-5:30pm - Session 1: Developing and Implementation of Risk Assessments and Emergency Management within CER and NIS2

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

Wednesday 15th October 2025

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: Drones and UAS

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

2:00pm-3:30pm - Session 4a: Collaboration, Information Sharing and Enhancing PPPs

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

4:15pm - 5:30pm - Session 5a: Cybersecurity and Cyber Resilience in CI

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: Communications Sector Symposium

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

2:00pm-3:30pm - Session 4b: Transport, Logistics & the Supply Chain Sector Symposium

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

4:15pm - 5:30pm - Session 5b: Maritime & Port Sector Symposium

Track Three (TIEMS)

9:00am-10:45am - New Challenges for Critical Infrastructure and the Role of Technologies in Emergency Management

10:45am-11:15am - Networking Coffee Break

11:15am - 1:00pm - New Challenges for Critical Infrastructure and the Role of Technologies in Emergency Management

1:00pm-2:00pm - Delegate Networking Lunch

2:00pm-3:00pm - TIEMS AGM

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

4:00pm - 5:30pm - Session 5c: ECSCI Cluster Workshop (CIPRE Programme)

Thursday 16th October 2025

Track One

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

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

11:15am - 12:30pm - Session 7a: Critical Systems and IT/OT

Track Two

9:00am-10:30am - Session 6b: Risk Management & Mitigation Strategies

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

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

Track Three (TIEMS)

9:00am-10:45am - AI and Emerging Technologies in Emergency Management

10:45am-11:15am - Networking Coffee Break

11:15am - 1:00pm - AI and Emerging Technologies in Emergency Management

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

2pm-3:30pm - Session 8: Workshop/Table Top Exercise: Developing and Implementation of Risk Assessments and Emergency Management

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

Co-located Conferences / Workshops:

STIME

African Young People Support Center

AFRICAN SMART CITIES INNOVATION FOUNDATION

Exhibition Opening Hours

Tuesday 14th October	1.00pm to 6.30pm
Wednesday 15th October	8.30am to 5.00pm
Thursday 16th October	8.30am to 3.30pm

On-Site Registration Hours

Monday 13th October	12.00pm to 5.00pm
Tuesday 14th October	8.30am to 6.30pm
Wednesday 15th October	8.30am to 5.00pm
Thursday 16th October	8.30am to 3.30pm

critical infrastructure
PROTECTION AND
RESILIENCE EUROPE

14th-16th October 2025
Brindisi, Italy
www.cipre-expo.com

HOW TO REGISTER

Online at **www.cipre-expo.com/register**

EARLY BIRD DISCOUNT - deadline 14th September 2025

Register yourself and your colleagues as conference delegates by 14th September 2025 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)
- Europe's Electricity Information Sharing and Analysis Centre (EE-ISAC)
- The International Emergency Management Society (TIEMS)
- The Critical Communications Association (TCCA)
- Crisis Communications Network Europe (CCNE)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- Confederation of European Security Services (CoESS)
- ECSCI Cluster (ECSCI)

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

On-Site Registration Hours

Tuesday 14th October	1.00pm to 6.30pm
Wednesday 15th October	8.30am to 5.00pm
Thursday 16th October	8.30am to 3.30pm

Tuesday 14th October

Conference Programme

9.00am-12.00pm - Site Visit - Port of Brindisi

9.30am-12.30pm - AYPSC Workshop - Africa–Europe Cooperation for Critical Infrastructure Resilience

2:00pm-3:30pm - Joint Opening Keynote

Chair: John Donlon QPM, FSI
International adviser on security intelligence

Dr Claudio Ciccotelli, Head of National Cybersecurity Perimeter Division, Regulatory Directorate - National Cybersecurity Agency, Italy

Olivier Onidi, Deputy Director-General, DG HOME, European Commission*

Dr Victor Vevera, General Director, ICI Bucharest, Romania

Giuseppe Marchionna, Mayor of Brindisi

Harald Drager, President, The International Emergency Management Society (TIEMS)

Prof. Antonio Ficarella, Head of the Department of Engineering for Innovation, University of Salento

Manos Athanatos, Board Member, Member of Core Management Team, ECSCI Cluster

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

4:00pm-5:30pm - Plenary Session 1: Developing and Implementation of Risk Assessments and Emergency Management within CER and NIS2

Developing and implementing Risk Assessments under CER and NIS2 necessitates identifying critical infrastructure and entities and assessing all relevant hazards and threats, including natural induced disasters like floods and earthquakes and man-made incidents. Integrated governance ensures these assessments inform robust resilience planning and emergency management frameworks. It is important to establish clear responsibilities, communication protocols, and coordinated actions across sectors to prepare for, respond to, and recover from disruptions caused by both cyber and physical events, ensuring continuity of essential services.

The Challenges of Critical Infrastructure Protection: Lessons of Ukraine - Oleksandr Sukhodolia, Head of Critical Infrastructure, Energy and Ecological Security Department, National Institute for Strategic Studies, Ukraine and Dr Oleksandr Potii, Chairman, State Service of Special Communications and Information Protection of Ukraine (SSSCIP)

Italy's Approach to National Risk Assessment and Strategy in the implementation of the CER Directive - Alessandro Lazari, Fellow and Lecturer, University of Salento - Department of Engineering for Innovation

Enhancing the Protection and Resilience of Critical Infrastructure: Perspectives from the Organization for Security and Co-operation in Europe - Daniel Golston, Associate Programme Officer, OSCE

Development Towards full Interoperability for European Civil Protection Agencies - Kyle King, Treasurer, The International Emergency Management Society (TIEMS)

Enhancement of cross-border risk assessment for critical infrastructure - Fred Petit, Project Officer, European Commission JRC

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

**invited*

Wednesday 15th October

Track One

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

The threats to critical infrastructure and entities continue to evolve. Cyberattacks are becoming more elaborate, threat of terrorism activities are on the increase, natural induced disasters worsen due to the changing weather patterns, and new threats like drone attacks and AI misuse emerge. This constant shift demands continuous updates to security measures. How can we identify, monitor and manage their potential damage?

The Convergence of latest threats to CI: Physical and Cyber threats in the Modern Era - Lina Kolesnikova, Fellow, ICPEM, Belgium

Hybrid Threats against CI/CE - Fred Petit, Project Officer, European Commission JRC

Uncovering State-Linked Espionage with Cyber AI Analyst - Nathaniel Jones, VP Threat Research, Dark Trace

Hybrid Threats to Critical Entity Resilience: Navigating Information Manipulation, Foreign Influence, and Economic Warfare in the Age of CER and NIS2 - Antonella Calo, Ph.D Candidate, University of Salento - Datalab, Italy

Robert Lipovský, Principal Threat Intelligence Researcher, ESET

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

11:15am - 12:30pm - Session 3a: Drones and UAS

Drones pose a growing threat to critical infrastructure due to their increasing accessibility, manoeuvrability, and payload capacity. They can be used for surveillance, delivering explosives, or causing disruptions. However, drones can also act as a facilitator to protect critical infrastructure. In this session we look into the threat, counter measures and impact drones can induce on CI.

JRC Drone Project - Counter Unmanned Aircraft Systems for Critical Infrastructure and Public Spaces - Bartel Meersman, Transport And Border Security Head Of Unit, European Commission Joint Research Centre, Italy

Mitigating the Rising Threat of Rogue Drones to Critical Infrastructure - Amit Haimovich, Vice President, Sales, D-Fend Solutions, Israel

Benefits of drones to protect CI/CE - Senior Representative, Preserve Project

TBC

Track Two

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

Europe's energy sector, encompassing oil, gas, and renewables, is of paramount importance. Its stability is crucial for the functioning of all other critical infrastructure/entities. The increasing frequency of cyberattacks and the impact of shifting weather patterns underscore the urgent need to protect energy assets, including IT/OT and SCADA systems. A key challenge is minimizing the impact of outages or attacks and strengthening Europe's energy grids.

Cybersecurity as a pilar for Resilience in the Energy sector - Frederic Guyomard, Senior Project Manager, Electricité De France (EDF)

Energy resilience in the Netherlands: application of the CER directive and identification of critical entities - Jaime Santiago Patterson, Scientist, TNO (Dutch Organization for Applied Scientific Research)

Robert Tucker, ESB Ireland, European Distribution System Operators (E.DSO)

TBC

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

11:15am - 12:30pm - Session 3b: Communications Sector Symposium

Communication networks are the lifeline of communities and critical infrastructure. When these networks fail, businesses are crippled, and emergency response is chaotic. With every sector now reliant on the internet, European businesses, governments, and critical infrastructure must prioritize the protection and resilience of these communications networks and assets.

Critical Operational Communications in the Utility Sector - Adrian Grilli, Technology Adviser, EUTC, Belgium

Latest Cybersecurity challenges and visions for the IRIS2 constellation - Nicolas Guillermin, Policy Officer DEFIS.C.1

Securing Private Wireless Networks in Critical Infrastructure - Filippo Gaggioli, Head of Security Product Introduction, Nokia, Italy

Evolution of First Responder & Mission Critical Communications in a CNI Context - Julian Stafford, Technical Advisor, The Critical Communications Association (TCCA)

12:30pm - Delegate Networking Lunch

Wednesday 15th October

Track One

2:00pm-3:30pm - Session 4a: Collaboration, Information Sharing and Enhancing PPPs

Building trust and dialogue by removing barriers between governments, operators, and communities is essential for effective risk, resilience, and emergency plans, enabling informed decisions for critical infrastructure and entity resilience. Stronger public-private partnerships depend on this collaborative approach. How do we enhance and promote better co-operation and secure information sharing across CI/CE in Europe.

Shaping the Future of Critical Infrastructure Security and Resilience through Public-Private Collaboration - Catherine Piana, Director General, CoESS

Strengthening Critical Infrastructure Resilience in Europe: The SUNRISE Project - Matjaz Tavcar, Project Manager, University Medical Center Ljubljana

Laura Caterick, Director, The Cross Market Operational Resilience Group (CMORG)

The Situational Awareness Challenge – Rethinking SA in Mission-Critical Environments - Chris Dreyfus-Gibson, Managing Director, DG Advisory

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

4:15pm - 5:30pm - Session 5a: Cybersecurity and Cyber Resilience in CI

Cybersecurity in CI focuses on preventing cyberattacks through robust defenses, threat detection, and incident response. Cyber resilience goes further by encompassing the ability of CI/CE to not only withstand attacks but also to continue operating and rapidly recover essential functions if an incident occurs. We need proactive measures for business continuity, disaster recovery, and maintaining operational integrity despite disruptions, ensure the security and reliability of vital services.

Alexandru Georgescu, Scientific Researcher, National Institute for Research and Development in Informatics, ICI Bucharest

Quantum Safe Networks for Critical Infrastructure Protection and Resilience - Giampaolo Panariello, CTO Network Infrastructure, Nokia

OT and Network Cybersecurity - Marek Gajarský, Senior Delivery Manager, ESET

The State of Cybersecurity in Healthcare - Nicole Wong, VP of Threat Research, Dark Trace and Nathaniel Jones, Dark Trace

Track Two

2:00pm-3:30pm - Session 4b: Transport, Logistics & the Supply Chain Sector Symposium

The Transport, Logistics, and Supply Chain sector faces critical infrastructure/entity challenges, including increased failure risks from interconnected networks, heightened cyber vulnerabilities due to IT/OT reliance, and operational disruptions from physical threats. The transport network, from rail, road, air and sea, requires better understanding of the impact of threats, whilst supply chain needs to enhance protecting sensitive data and ensuring business continuity through rapid recovery are crucial for building resilience.

Cyber Priority Report 2024/2025: Insights into Supply Chain Security - Auke Huistra, Director of Industrial and OT Cybersecurity, DNV Cyber

Practical Threat Modeling with MITRE ATT&CK Framework for Critical Environment - Ishan Upadhyaya, Senior Cyber Security Architect, Vanderlande Industries

Importance of Embedding a Holistic Approach to Security and Resilience in the Design of Airport Infrastructure - Sarah Jane Prew, Senior Security Advisor, Arup UK

Faye Francy, Executive Director, AUTO ISAC Europe

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

4:15pm - 5:30pm - Session 5b: Maritime & Port Sector Symposium

The port and maritime sector faces critical infrastructure challenges, including climate change impacts, cyberattacks, terrorist attacks and geopolitical instability, all threatening global trade, economic prosperity, national security and environmental sustainability. To protect and build resilience, the sector needs to embed climate adaptation, enhance cybersecurity measures, and foster collaboration between stakeholders. Resilient ports are crucial for economic stability and require a holistic approach.

Commander, Brindisi Port

Towards new CIP Capabilities and Resilience in Ports - Rafael Company, Director of Safety and Security, Fundacion Valenciaport

VIGIMARE Project - Johanna Karvonen, EU Project Coordinator, Laurea University of Applied Sciences, Finland

Underwater Threats - Nowhere left to hide - Simon Goldsworthy, Global Business Development Manager – Intruder Detection Systems, Wavefront Systems

Thursday 16th October

Track One

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

The latest technologies for detecting and protecting critical infrastructure and entities from physical and cyber threats, include ground, land, underwater, space-based, and cyber technologies, as well as enhanced access controls and sensors. Artificial intelligence (AI) is being utilized to improve the performance of these technologies, enabling more effective and efficient threat detection and protection.

Modern security and management solutions for critical infrastructures: Access and control technologies as the key to resilience and efficiency - Phillip Schickenberg, Director Sales, Steinbach & Vollman

Enhancing Maritime and Land-Based Security Through Advanced Software and Sensor Technologies - Slaiby Stephan, Global Sales Director, Surveillance & Mission Systems, Terma

Our world changed - Did your security? - Michael Johansen, iLOQ

TBC

10.30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7a: Critical Systems and IT/OT

Protecting critical systems, such as ICS and SCADA, within CI is vital for security and public safety. The convergence of IT and OT networks increases cyber risks, demanding robust security measures. Safeguarding these interconnected environments from cyber threats is paramount to ensure the uninterrupted operation of essential services. What are the challenges, and how do we mitigate the threats?

Implementing AI in OT environments, preparedness, and measuring maturity - Mike Echols, CEO, Max Cybersecurity, USA

Monitoring of Mission-Critical Systems in the Military Airports of the Italian Air Force: lessons learned - Commander Col. Antonino Massara, Commander 36' Fighter Wing Commander, Ministry of Defence, Italy

Eliminating OT Operations Drift with Service Management - Phil Litherland, Principal Consultant, Bridewell

Bridging Functional Safety and Cybersecurity: A Unified Approach to Protecting Critical Infrastructure - Jalal Bouhdada, Founder/CEO, Indurex

Track Two

9:00am-10:30am - Session 6b: Risk Management & Mitigation Strategies

Developing comprehensive resilience within the critical infrastructure community requires structured information sharing, a commitment to infrastructure preparedness, and robust risk management and mitigation strategies. How do we approach identifying, assessing and prioritising risks and build in resilience through reducing vulnerabilities, whilst planning for a potential disaster.

Integrative Policy Recommendations for Strengthening Infrastructure Resilience to Wildfires - Danai Kazantzidou-Firtinidou, Senior Researcher, KEMEA-Center for Security Studies, Greece

Bridging Public Warning Systems and Critical Infrastructure Security and Resilience: A Strategic Gap in Need of Integration - Antonella Calo, Ph.D Candidate, University of Salento - Datalab, Italy

Bridging AI and Systems Thinking: A Hybrid Approach to Identifying and Mitigating Human Errors in Critical Operations - Irene Bonetti, Terminal Manager, Attilio Carmagnani

Behind the Firewall: Mitigating Insider Risk in Critical Sectors - Dennis Bijker, CEO & Isa Steijn, Insider Risk Advisor, Signpost Six

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

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

Is AI a force for good or evil? AI enhances critical infrastructure cybersecurity by improving threat detection, automating responses, and predicting attacks. Machine learning algorithms can analyze vast data volumes to identify anomalies, enabling proactive defense. However, AI also presents challenges, as malicious actors can use it to create sophisticated attacks. Effective critical infrastructure protection requires leveraging AI's strengths while mitigating its potential risks through robust security measures and continuous adaptation.

Dr Victor Vevera, General Director, ICI Bucharest, Romania

Critical Infrastructure Resilience And Artificial Intelligence - Sandro Bologna, Researcher/Board Member, AIIC

AI for Secure Software Development: Integrating Security Early with DevSecOps - Mohammed Ilyas Ahmed, Security Architect, Adobe

Antonella Longo, Scientific Director of DataLab, University of Salento

12:30pm - Delegate Networking Lunch

Thursday 16th October

2:00pm-3:30pm - Plenary Session 8:
WORKSHOP - Workshop/Table Top Exercise: Developing and Implementation of Risk Assessments and Emergency Management

Join us for an engaging and interactive session on the final day of CIPRE. Titled "Developing and Implementation of Risk Assessments and Emergency Management" this session is designed to build on lessons learned from the previous sessions with greater involvement from participants through dynamic, interactive tabletop exercises and thought-provoking scenarios.

How do we actively and successfully develop and implement a Risk Assessment at national level, identify critical infrastructures and entities, and assess all relevant hazards and threats?

In this interactive and engaging workshop, we will discuss and highlight key factors in the process and how to translate them into a resilience strategy.

Moderator: Alessandro Lazari, Regional Director, IACIPP & Fellow in Critical Infrastructure Protection and Resilience University of Salento, Italy

3.30pm - Conference Close

John Donlon QPM, FSI, Conference Chairman

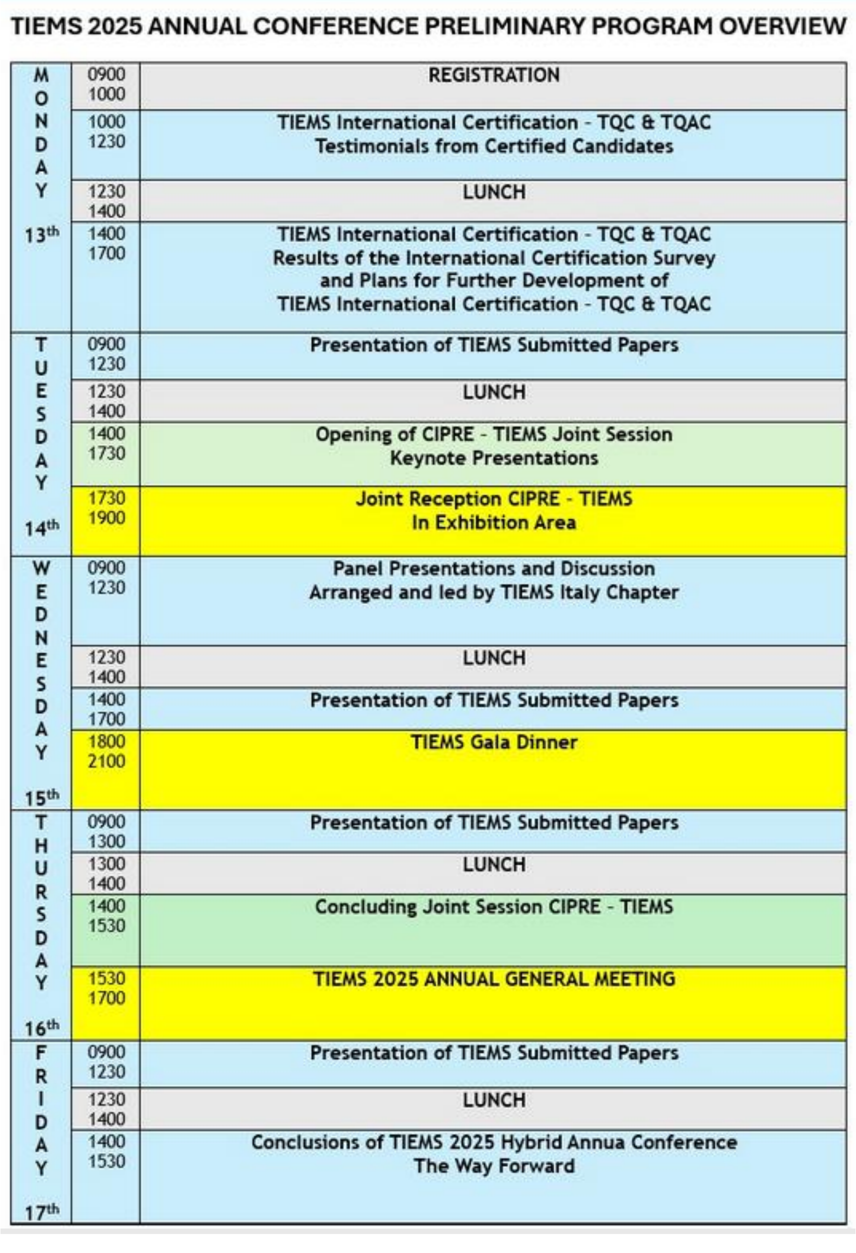
Register online at www.cipre-expo.com/register

Early Bird Deadline - 14th September 2025

13th-17th October 2025

Critical Infrastructure Protection Week in Europe

14th-16th October 2025 - Brindisi, Italy



TIEMS 2025 ANNUAL CONFERENCE PRELIMINARY PROGRAM OVERVIEW

MONDAY 13th	0900 1000	REGISTRATION
	1000 1230	TIEMS International Certification - TQC & TQAC Testimonials from Certified Candidates
	1230 1400	LUNCH
	1400 1700	TIEMS International Certification - TQC & TQAC Results of the International Certification Survey and Plans for Further Development of TIEMS International Certification - TQC & TQAC
TUESDAY 14th	0900 1230	Presentation of TIEMS Submitted Papers
	1230 1400	LUNCH
	1400 1730	Opening of CIPRE - TIEMS Joint Session Keynote Presentations
	1730 1900	Joint Reception CIPRE - TIEMS In Exhibition Area
WEDNESDAY 15th	0900 1230	Panel Presentations and Discussion Arranged and led by TIEMS Italy Chapter
	1230 1400	LUNCH
	1400 1700	Presentation of TIEMS Submitted Papers
	1800 2100	TIEMS Gala Dinner
THURSDAY 16th	0900 1300	Presentation of TIEMS Submitted Papers
	1300 1400	LUNCH
	1400 1530	Concluding Joint Session CIPRE - TIEMS
	1530 1700	TIEMS 2025 ANNUAL GENERAL MEETING
FRIDAY 17th	0900 1230	Presentation of TIEMS Submitted Papers
	1230 1400	LUNCH
	1400 1530	Conclusions of TIEMS 2025 Hybrid Annua Conference The Way Forward

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

Tuesday 14th October - 9.30am-12.30pm

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.

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

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

European Cluster for Securing Critical Infrastructures (ECSCI) Workshop

critical infrastructure
PROTECTION AND RESILIENCE EUROPE
14th-16th October 2025

EUROPEAN CLUSTER FOR SECURING CRITICAL INFRASTRUCTURES
SCIENTIFIC COLLABORATION
TECHNICAL COLLABORATION
COMMUNICATION & DISSEMINATION
STAKEHOLDERS' ALLIANCE
MARKETPLACE

Implementing the European Directive on Critical Entity Resilience (CER Directive): Status, Challenges and International Context

Wednesday 15th October - 4.00pm-5.30pm

The European Directive on Critical Entity Resilience (CER Directive, following the preceding directive on critical infrastructures (CIs), from 2008) is currently in the implementation phase.

Adopted and published in 2022, it entered into force in 2023, and, on October 18, 2024 it became applicable (mandatory) in the EU and replaced the preceding directive. The EU Member States are supposed to adopt national strategies for enhancing the resilience of critical entities and identify critical entities by 2026. The European Commission will report to the European Parliament and Council on the compliance with the Directive by 2027 and provide the review of the Directive impact by 2029.

Already the previous directive, designated over 100 CIs as the CIs with possible cross-border impact – the number estimated to exceed 15,000 CIs by 2027, involving possibly over 25,000 experts across CI operators, consultancies, governments and other stakeholders.

The above numbers, the some already experienced delays and the need to implement the Directive together with the other EU Directives (e.g., the NIS2), show the complexity and importance of the Directive and its implementation. The European Cluster for Securing Critical Infrastructures (ECSCI, https://www.ecsci.eu) set as one of its goals to contribute to the implementation of the Directive, by aligning the opinions, activities and outcomes of the EU research projects. The respective ECSCI survey results will be presented at the workshop.

This short ECSCI Workshop intends to look at the status of the Directive implementation, the challenges experienced or expected and the "international context". The cross-border impacts are an important element of the Directive and these aspects are not limited to the EU only – hence the workshop will include the views from within and outside the EU (tentatively non-EU European countries, Canada, US, Australia, ISO, …). Thanks to the hybrid format envisaged, both the participants onsite and those participating online will be able to share their views.

Organizers:

- Prof. Aleksandar JOVANOVIC (online coordinator) CEO, Steinbeis European Risk & Resilience Institute (EU-VRi), Germany

- Dr. Manos ATHANATOS (onsite coordinator) Senior Technical Project Manager, Technical University of Crete (TUC), Greece

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

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

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

Networking Reception

Tuesday 14th 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

14th-16th October 2025
Brindisi, Italy
www.cipre-expo.com

Event Hotels & Venues

Venue:
Theatre Nuovo Teatro Giuseppe Verdi
Largo Gianni D'Errico, 1,
72100 Brindisi
www.nuovoteatroverdi.com

For more details visit:
www.cipre-expo.com/venue

Teatro Nuovo Teatro Giuseppe Verdi is the main theater of the city of Brindisi, Italy. and hosts a variety of events, including operas, concerts, plays, and ballets. The theater plays a fundamental role in the cultural life of Brindisi and the surrounding region, attracting artists and spectators from all over Italy and beyond.

The Teatro Nuovo Teatro Giuseppe Verdi will act as the main building for Critical Infrastructure Protection Week in Europe, with CIPRE main conference sessions, the exhibition and networking arena/ reception.

Accommodation

Critical Infrastructure Protection & Resilience Europe event HQ hotels for the 2025 event are just a few minutes walk from the venue:

Hotel Orientale
Corso G. Garibaldi, 40 – Brindisi
+39 0831.568451
info@hotelorientale.it
www.hotelorientale.it

Boutique Hotel Executive Inn
Via Pozzo Traiano, 24 – Brindisi
+39 0831.527844
info@hotelexecutiveinn.it
www.hotelexecutiveinn.it

Promo Code 'Brindisi2025'

Accommodation Booking links at www.cipre-expo.com/accommodation
Apply Promo Code '**Brindisi2025**' for your special room discount with our partner hotels - Hotel Orientale and Boutique Hotel Executive Inn.

Brindisi, Italy

Brindisi is a port city on the Adriatic coast of Puglia, Italy, an ancient city, with deep historical roots and a strategic location. With many direct links to the Balkans, North Africa and across mainland Europe, it is the ideal location for the 2025 CIPRE and CIP Week in Europe.

Strategic Adriatic Position and Connectivity

Brindisi, located on Italy's Adriatic coast, serves as a pivotal gateway between Western Europe and the Balkans. This strategic position ensures seamless connectivity across the Adriatic and Mediterranean seas, offering direct access to key markets and regions crucial for critical infrastructure protection discussions.

Vital Sea-Facing City with Robust Port Facilities

As a vital sea-facing city, Brindisi boasts one of the most significant ports in the Adriatic, acting as a central node in maritime trade routes. The port's modern facilities and extensive connections across the region make it an essential asset for discussions on infrastructure security, particularly in the context of maritime and port security.

Proximity to Bari, Taranto, and Lecce: A Regional Powerhouse

Brindisi's strategic location is further enhanced by its proximity to the industrial powerhouses of Bari, Taranto, and Lecce. Bari, with its robust seaborne industry, plays a crucial role in the maritime economy of Southern Italy. Taranto is home to one of Europe's largest steelworks and a major oil refining industry, making it a critical player in the region's industrial landscape. Furthermore, Lecce is the landing point of the Trans Adriatic Pipeline (TAP), a key national critical infrastructure that enables Italy and Europe to diversify their gas supply chain, a crucial factor in the current geopolitical climate.

Smart City Initiatives and Technological Innovation

Brindisi is undergoing a transformative smart city project focused on crowd management, port security, public warning systems, and early warning mechanisms for natural disasters such as floods. These initiatives position Brindisi as a leader in integrating technology with urban infrastructure to enhance resilience and security. The city's experience in implementing these cutting-edge solutions provides valuable case studies for conference participants, offering practical insights into the future of urban infrastructure protection.

For more details view: www.cipre-expo.com/about-brindisi

critical infrastructure
PROTECTION AND
RESILIENCE EUROPE

14th-16th October 2025
Brindisi, Italy
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, 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 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 14th September 2025	€195
Paid on or after 14th September 2025	€295

OPERATORS OF CRITICAL NATIONAL INFRASTRUCTURE

Individual Full Delegate

Paid before 14th September 2025	€195
Paid on or after 14th September 2025	€295

COMMERCIAL ORGANIZATIONS

Individual Full Delegate

Paid before 14th September 2025	€495
Paid on or after 14th September 2025	€695

Sponsor/Exhibitor Full Delegate).

Paid before 14th September 2025	€295
Paid on or after 14th September 2025	€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, networking reception, coffee breaks and 2 lunches. Also includes One Year Membership of International Association of CIP Professionals (IACIPP). Access to TIEMS programme also included.

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

critical infrastructure

PROTECTION AND RESILIENCE EUROPE

14th-16th October 2025

Brindisi, Italy

www.cipre-expo.com

Why participate and be involved?

Critical Infrastructure Protection and Resilience Europe provides a unique opportunity to meet, discuss and communicate with some of the most influential critical infrastructure protection and security policy makers and practitioners.

Your participation will gain access to this key target audience:

- raise your company brand, profile and awareness
- showcase your products and technologies
- explore business opportunities in this dynamic market
- provide a platform to communicate key messages
- gain face-to-face meeting opportunities

Critical Infrastructure Protection and Resilience Europe gives you a great opportunity to meet key decision makers and influencers.

How to Sponsor

Gain access to a key and influential audience with your participation in the limited sponsorship opportunities available at the conference exhibition.

To discuss sponsorship opportunities and your involvement with Critical Infrastructure Protection & Resilience Europe please contact:

Paul Gloc
(UK and 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

"Although the EC Directive has helped in 'assessing the need to improve the protection of European critical infrastructures' in the transport and energy sectors, there is no indication that it has actually improved security in these sectors."

Why participate and be involved?

Critical Infrastructure Protection and Resilience Europe provides a unique opportunity to meet, discuss and communicate with some of the most influential critical infrastructure protection and security policy makers and practitioners.

Your participation will gain access to this key target audience:

- raise your company brand, profile and awareness
- showcase your products and technologies
- explore business opportunities in this dynamic market
- provide a platform to communicate key messages
- gain face-to-face meeting opportunities

Critical Infrastructure Protection and Resilience Europe gives you a great opportunity to meet key decision makers and influencers.

www.cipre-expo.com

Sponsorship Opportunities

A limited number of opportunities exist to commercial organisations to be involved with the conference and the opportunity to meet and gain maximum exposure to a key and influential audience.

Some of the sponsorship package opportunities are highlighted on the left. Packages can be designed and tailored to meet your budget requirements and objectives.

Critical Infrastructure Protection Week *in Europe*

14th-16th October 2025 - Brindisi, Italy

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.

International Association of CIP Professionals

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 AND
RESILIENCE EUROPE

10

14th-16th October 2025
Brindisi, Italy
www.cipre-expo.com

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to CIP Week and Critical Infrastructure Protection & Resilience Europe 2025.

With the patronage of the City of Brindisi

Co-Hosted by:

International Association of CIP Professionals

UNIVERSITÀ DEL SALENTO
DIPARTIMENTO DI INGEGNERIA DELL'INNOVAZIONE

CRISR

CIP Week Event Partner:

S T I M E

Platinum Sponsor:

eset®
Digital Security
Progress. Protected.

Executive Sponsors:

TCCA

E.DSO

EUTC

open ENL CC

AUTO-ISAC

Supporting Organisations:

EE-ISAC

CCNE

CoESS

African Young People Support Center

AFRICAN SMART CITIES INNOVATION FOUNDATION

Help2Protect

NS&RC

ISIO

Flagship Media Partner:

critical infrastructure
PROTECTION AND
RESILIENCE NEWS

Media Supporter:

BIOMETRIC UPDATE.COM

govCIO OUTLOOK

CIOReview EUROPE

Securing the Backbone of Society: How to Protect Critical Network Infrastructure

By Clemens Pohl, Managing Director, AP Sensing

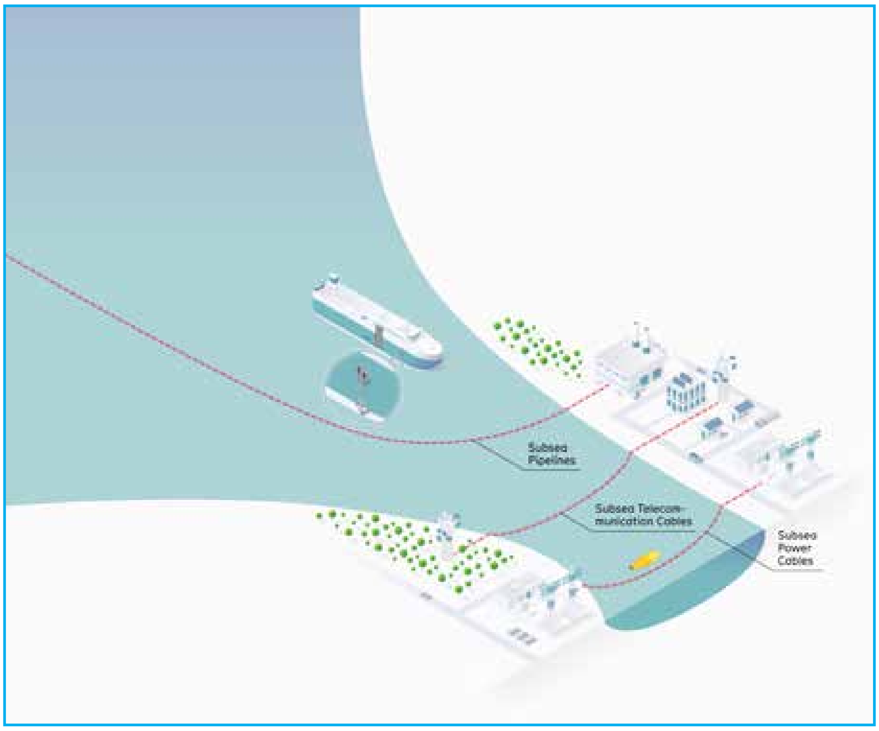
Across the globe, critical energy infrastructure is under growing pressure from both natural hazards and human-caused threats. Power grids are being pushed to their thermal and operational limits. Pipelines are exposed to third-party interference and environmental stress. Cable tunnels, transformer yards, and other confined spaces carry increasing fire risks. These assets often stretch across vast distances and pass through remote or hard-to-access areas where conventional monitoring solutions offer little real-time insight. Recent sabotage attacks on submarine cables in Europe have brought these vulnerabilities sharply into focus. To ensure safe and reliable operation, operators must detect anomalies early, localize threats precisely, and respond before failures escalate. Distributed Fiber Optic Sensing (DFOS) offers a powerful approach by transforming existing fiber optic cables into continuous, real-time sensing networks. This enables a new level of infrastructure awareness and resilience.

Distributed Fiber Optic Sensing (DFOS): How It Works

DFOS leverages the physics of light scattering within optical fibers to turn passive cable infrastructure into high-resolution, real-time sensors. DFOS is applied through three core methods: Distributed Acoustic Sensing (DAS), Distributed Temperature Sensing (DTS), and Distributed Temperature and Strain Sensing (DTSS). Each technology detects and localizes different physical phenomena along the entire length of the fiber without requiring additional in-field sensors.

At the heart of each method is a simple principle. A laser pulse is sent through a standard fiber optic cable, and the system continuously analyzes the light that is scattered back toward the source. When conditions along the fiber change, such as a shift in temperature, vibration, or strain, the properties of the backscattered light are altered. By measuring and interpreting these changes, the system can determine where along the fiber the event occurred, often with meter-level resolution. The type of scattering observed determines whether the system is sensing acoustic signals, temperature changes, or mechanical stress.

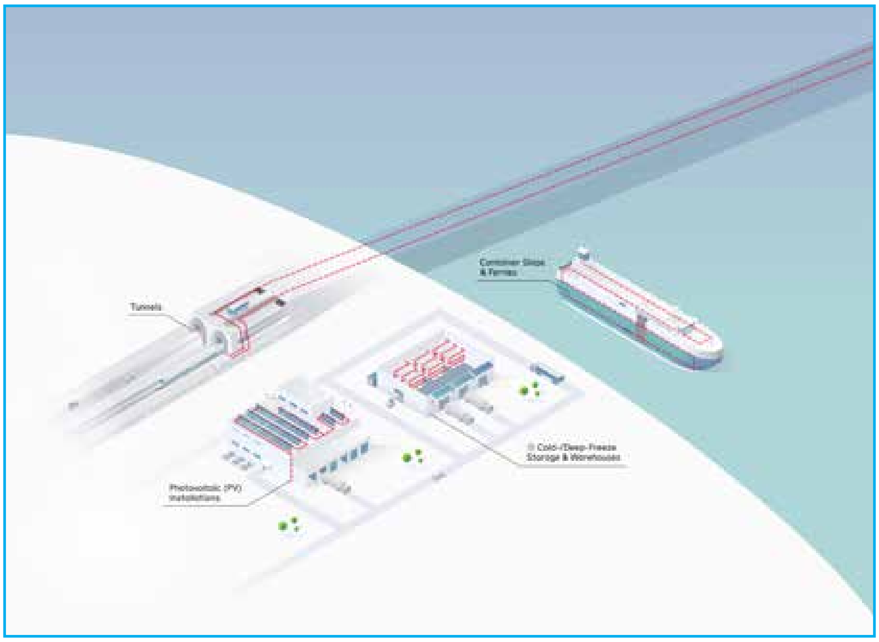
Because the fiber itself serves as the sensing element, DFOS provides continuous coverage across long distances. In contrast to conventional point sensors, which must be installed at multiple locations and only monitor discrete spots, DFOS transforms an entire length of optical fiber into a distributed array, allowing for comprehensive event detection and localization along the entire infrastructure. This makes it well suited to monitoring linear infrastructure with complex risk profiles.



Distributed Acoustic Sensing (DAS) uses coherent optical time domain reflectometry (C-OTDR) to analyze Rayleigh backscattering in fiber optics. This makes it possible to detect acoustic vibrations caused by external activity, such as footsteps, vehicles, digging, or mechanical stress, over distances of up to 100 km. DAS systems interpret these vibrations with the help of machine learning algorithms that classify and filter events in real time. This enables operators to distinguish between benign environmental influences and serious threats, such as tunneling or unauthorized access. Because DAS uses the fiber itself as the sensing element, it offers complete linear coverage and high spatial resolution.

Distributed Temperature Sensing (DTS) measures temperature changes along the fiber using Raman scattering principles. This technology enables accurate, real-time monitoring of thermal conditions across critical assets such as cable tunnels, transformer yards, or buried power lines. DTS can detect localized heating events, signal potential equipment failure, and identify fire risks. This is especially valuable in environments where uninterrupted operation and rapid response are critical, such as railways and power grids.

Distributed Temperature and Strain Sensing (DTSS), based on Brillouin optical time domain reflectometry (BOTDR), adds an additional layer of insight by measuring both thermal and mechanical strain. DTSS provides structural health monitoring over long distances, identifying issues such as ground movement, mechanical strain, or shifting in buried infrastructure. It operates reliably in environments with high electromagnetic interference, such as power substations. It


Tunnels
Container Ships & Ferries
Cold-/Deep-Freeze Storage & Warehouses
Photovoltaic (PV) Installations

also supports condition-based maintenance by identifying subtle, long-term structural changes that might otherwise go undetected.

Together, these DFOS technologies form a complementary system capable of detecting, classifying, and localizing anomalies in real time. They provide operators with a continuous understanding of what is happening along their networked infrastructure.

Real-World Applications Across Infrastructure Sectors

Power Grids

Power transmission networks face the dual challenge of rising demand and aging infrastructure. With DFOS, operators can continuously monitor underground and subsea cables, as well as bus duct systems and overhead lines. Temperature and acoustic data help detect hot spots, joint failures, or overloads before they become critical. Real-time ampacity calculations and early warning of emergency ratings allow for dynamic load management. For submarine cables, sensing technologies can also infer burial depth and detect localized disruptions caused by seabed movement or external interference.

Pipelines

DFOS technologies are increasingly used in oil and gas and water pipelines to address risks such as third-party intrusion, leaks, structural stress, or environmental damage. Acoustic sensing detects mechanical vibrations linked to unauthorized digging or tapping, while strain sensing identifies ground shifts that could compromise pipe integrity. DTS adds the ability to detect leaks based on thermal anomalies, enabling more precise incident response and better compliance with safety and environmental standards.

Railways

Rail systems are exposed to multiple operational and external risks, including track faults, equipment degradation, landslides, and vandalism. DAS enables detection of acoustic vibrations linked to wheel defects or broken rails and also serves as an early alert system for trespassing or cable theft. With the DTS technology, tunnels and stations handle fire detection. The system is fully certified to international standards and protects large scale infrastructure even in dusty and rough environments.

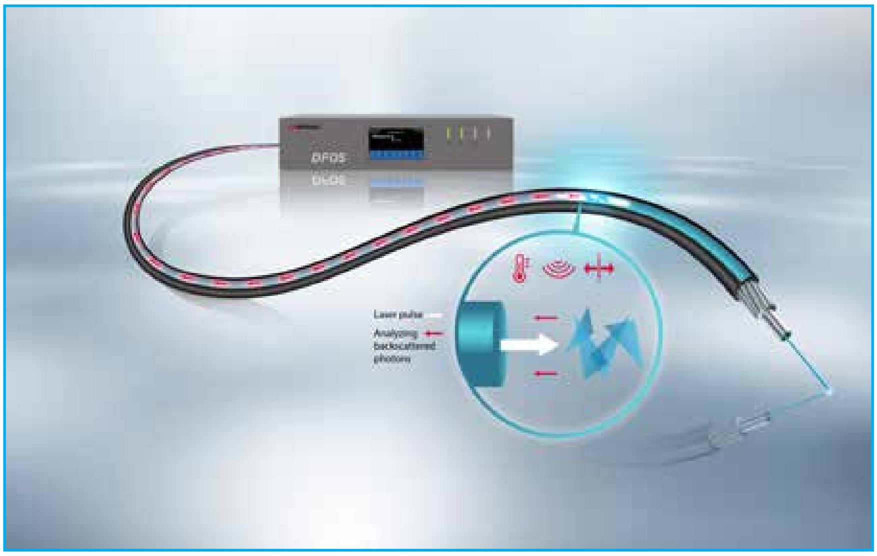
Border Protection

In perimeter security applications, DAS is used to detect and classify movement near fences or restricted zones. Fiber optic sensing identifies and distinguishes between footsteps, vehicle activity, and mechanical tampering, minimizing false alarms and enabling timely response. Since the fiber is often already installed as part of communication infrastructure, it becomes a dual-use asset for security and monitoring, especially in remote or unstaffed areas.

Real-World Insight: Leak Detection in an Ecologically Sensitive Pipeline Corridor

One example of distributed fiber optic sensing in action involves a pipeline monitoring project located in an ecologically protected coastal region in Northern Europe. The pipeline, which transports crude oil from an offshore platform to a mainland facility, runs through a designated national park known for its fragile biodiversity and tidal flats.

Given the sensitivity of the environment, local authorities required continuous monitoring with precise leak detection capabilities. A fiber optic-based Distributed Temperature Sensing (DTS) system, provided by AP Sensing, a global provider of



DFOS solutions, was selected to monitor the entire eight-kilometer stretch of pipeline. The sensor cable, designed to withstand mechanical stress and positional shifts, was installed along the full length of the buried pipeline. The route includes directional drill sections up to 1,400 meters long and reaches depths of up to 20 meters below the seabed.

Once operational, the DTS system provided continuous temperature measurements in real time. This allowed for the early detection of thermal anomalies that could indicate a leak. To improve accuracy and responsiveness, intelligent alarm algorithms were configured to identify transient thermal behaviors that might otherwise be overlooked. These analytics made it possible to detect even small leaks and precisely locate the affected section. This gave the operator the ability to respond quickly and minimize environmental impact.

By integrating real-time sensing technology in a complex and environmentally sensitive context, the project demonstrated how DTS can enhance both operational safety and environmental protection.

Key Takeaways: What DFOS Enables for Infrastructure Operators

- Continuous Monitoring
  Fiber optic cables become full-length sensors, providing instant insights along the entire asset rather than at isolated points.

- Multiple Sensing Parameters
  Temperature, strain, and acoustic events can be monitored simultaneously, offering a comprehensive view of asset health and security.

- Precise Localization
  Events such as leaks, cable faults, or unauthorized activity can be located with high spatial accuracy, enabling faster response.

- Minimal Intrusion
  DFOS systems use existing fiber infrastructure and require no power in the field, making them well suited for remote or hazardous environments.

- Cross-Sector Applications
  Applicable across energy, rail, pipeline, and perimeter protection sectors, DFOS enhances both operational performance and long-term resilience.

Building Resilience Through Insight

Distributed fiber optic sensing can serve as the nervous system of critical infrastructure, providing continuous awareness across long, complex, and vulnerable assets. By turning standard fiber optic cables into dense sensing arrays, this technology empowers operators to detect, classify, and localize threats in real time. As infrastructure systems grow more complex and interdependent, so does the need for continuous situational awareness. Distributed fiber optic sensing solutions from AP Sensing offer a practical foundation for data-driven infrastructure management, with the added benefit of long-range coverage and low maintenance. Its ability to detect changes in real time supports earlier intervention, better decision-making, and more efficient use of resources.

Clemens Pohl was instrumental in establishing the fiber optic sensing business at HP / Agilent Technologies. In 2007, he led the spin-off that formed AP Sensing and has served as CEO ever since. Today, AP Sensing is a leading global provider of Distributed Fiber Optic Sensing (DFOS) solutions, with operations on five continents and a strong presence across the energy, transportation, and industrial sectors.

Closing the Gaps in Insider Threat Mitigation: A New Resource Now Freely Available

"There are only two ways to know if you are being targeted by an Insider Threat: wait for an incident to happen – or have a mitigation programme in place." This hard-hitting statement is not just a warning — it's a call to action. And it lies at the core of Help2Protect's philosophy.

As part of its ongoing mission to support critical infrastructure (CI) operators, Help2Protect has made one of its key resources — the Program Development Module Manual — available for free. This in-depth document was previously only accessible as part of a comprehensive paid programme. Now, it can be downloaded directly via the Help2Protect platform: www.help2protect.info.

A Strategic Tool for a Systemic Challenge

The manual is more than just a guide; it is the learning companion to the "Program Development Module" of Help2Protect's e-learning platform. It offers professionals a deep dive into the foundational concepts, key milestones, and best practices essential to implementing an Insider Threat Mitigation Program.

Insider threats don't only emerge from malicious intent — they can stem from negligence, coercion, or even a lack of awareness. That's why Help2Protect's approach is holistic and organisational. It insists on the involvement of the entire C-suite, starting from the CEO's buy-in and cascading all the way through the organisation. Insider threat mitigation, when done right, becomes a cross-cutting issue — not an isolated concern for the security team.

This philosophy aligns with a broader vision: that a robust security culture is inseparable from a healthy corporate culture.

What's Inside the Platform?

The Program Development Module is built on:

- A comprehensive synthesis of existing academic and operational literature on Insider Threats;
- Real-world case studies across sectors — cyber and physical, public and private — highlighting red flags, failures, and preventive strategies;
- Self-assessment quizzes at the end of each module and a final knowledge test that leads to a certificate of completion.

It is not a theoretical toolkit. It is a pragmatic and field-driven learning pathway, designed to enable protection officers, managers and decision-makers to move from awareness to action.

Recognised by the EU and ICAO

Help2Protect originated as a spin-off of an EU-funded programme (DG HOME – ISF Fund) and has since been recognised multiple times by the European Commission as a reference initiative in its domain. Its learning resources — including the Program Development Module — are featured on the ICAO website as part of its Security Culture toolkit.

The release of this manual marks a strategic milestone: opening up access to validated, operational expertise that has already benefited numerous stakeholders across Europe.

A Call to the Community

In making this manual freely accessible, **Help2Protect** is reaffirming its commitment to the broader security community: to share knowledge, empower practitioners, and build resilience from the inside out.

Explore the manual and other tools on the platform: www.help2protect.info

International Association of
CIP Professionals

www.cip-association.org

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

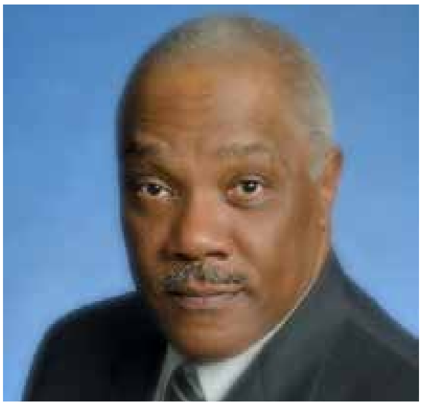
For further details and to join, visit **www.cip-association.org** and help shape the future of this increasingly critical sector of national security.

We look forward to welcoming you.

John Donlon **QPM, FSI**
Chairman
IACIPP

Zero Trust IEEE Standard: In Progress

In 2025, two members of the IEEE Zero Trust Security Working Group presented a summary of this project to the Critical Infrastructure Protection and Resilience Americas event in Houston, Texas. The project has advanced to internal work group review. The draft publication is planned for release to the public for comment in fall 2025. The following is a snapshot of the key elements of the draft standard. During the Critical Infrastructure Protection and Resilience Americas event in Baton Rouge, Louisiana, the working group team plans to present the project status.



Dr. Ron Martin, Professor of Practice, Capitol Technology University

The significance of the Zero Trust Security Standard encourages organizations to review it for potential adoption. One of the key references for Zero Trust Security is the 2022 National Institute of Standards and Technology's Special Publication 800-207. This document defines Zero Trust as a cybersecurity approach.

Recognizing the importance of this program and its potential to improve cybersecurity, the Institute of Electrical and Electronics Engineers (IEEE) launched a project to develop an IEEE and International Organization for Standardization (ISO) standard for Zero Trust.

As cyber threats continue to evolve, traditional perimeter-based security models are no longer sufficient to protect sensitive organizational resources. The Zero Trust framework provides a robust approach to cybersecurity by adopting principles such as "never trust, always verify", assume breach, and least privilege access. This standard outlines a comprehensive framework to help organizations transition to a Zero Trust Architecture (ZTA) or build systems that fully embrace Zero Trust principles.

Why This Standard Matters:

1. Enhanced Security: The framework addresses critical domains such as Identity, Devices, Networks, Applications, and Data, ensuring granular control and protection of organizational assets.
2. Risk Mitigation: By implementing Zero Trust principles, organizations can reduce vulnerabilities, mitigate risks, and safeguard against increasingly sophisticated cyber threats.
3. Compliance: The standard aligns with regulatory requirements and provides guidance for maintaining accountability and evidence of ZTA compliance.
4. Future-Ready: Zero Trust is a dynamic strategy that evolves with the threat landscape, ensuring organizations remain proactive and resilient.

Key Components to Review:

- ZT Domains: Identity, Devices, Networks, Applications, and Data.
- Cross-Cutting Domains: Governance, Visibility & Analytics, and Automation & Orchestration.
- Implementation Guidance: Practical steps for migrating to ZTA, including governance alignment, continuous monitoring, and automation.

This is not just a technical change but a strategic evolution that demands collaboration across all levels of the organization.

Institute of Electrical and Electronics Engineers. (2025). Draft standard for zero trust security (P3409™/D6). IEEE Computer Society. https://myprj-fgen.standards.ieee.org/mypr-file/par/10955/mypr

European Utilities Telecom Council (EUTC)

Ben Lane, Event Manager for Critical Infrastructure Protection & Resilience Europe, met Adrian Grilli, EUTC Technology Advisor.

Technology is rapidly changing the role of telecom in Europe's electric, gas and water utilities, energy companies and other critical infrastructure companies. They have vast experience in building and managing sophisticated telecommunications networks, but now face new challenges introducing new wireless communications systems and managing telecoms in a shared services environment.

Adrian Grilli, Technology Advisor, EUTC

Moreover, critical infrastructure has experienced spectacular changes resulting from new regulatory imperatives for sustainability. To face both challenges, EUTC has modified its legal status by becoming independent from its US parent, UTC, and has developed programs which are led and designed by Europeans, and uniquely European in focus.

Ben Lane (BL): Hello Adrian,can you tell us a little about yourself.

Adrian Grilli (AG): I'm the Technology Advisor at EUTC. I've been involved in utility telecoms for about 25 years, initially as a spectrum manager for UK transmission and distribution companies for gas and electricity. I've represented the utility sector in various international organisations and particularly spectrum. Before moving to the private sector, I worked in government, in radio regulation, standards, policy and other regulatory affairs. My background essentially is working in government and switching to the private sector.

(BL): Thank you. Could you provide a brief overview of EUTC's key aims and objectives.

(AG): We're an association of electricity and gas transmission and distribution operators, as well as generators, across Europe and now African utilities. We represent the telecom side of the energy and water sectors. If you think about a modern electricity network, you can't operate without telecoms. When you look at a control room, you will see a group of people managing a nationwide or regional network. Without telecoms they can't see what's going on and they can't control anything. So that's why telecoms are vital to any modern energy network.

(BL): Can you explain EUTC's role in the debate on radio spectrum allocation for European utilities and CI please?

(AG): Radio spectrum is important to us. Traditionally we've used copper wire for our communications and there's a lot of fibre in the network. As we've deployed more renewables, you've got a lot more devices connected to the network. Therefore, radio is critical to developing modern networks and it's good for resilience. Fibre complemented by radio is extremely resilient. Ideally, we need dedicated radio spectrum for those networks to operate reliably. The networks are nationwide, they must cover remote areas and ideally go below ground. So, you need radio spectrum, which will enable you to get good geographic coverage and penetration with as few base stations as possible, because then you can make the network highly resilient; the higher the number of base stations, the more difficult it is to make a network resilient. So, we're very keen on dedicated spectrum for utilities.

(BL): Describe how EUTC fosters awareness and maturity of cyber security and resilience of networks among utility companies in Europe.

(AG): Cybersecurity is obviously a very big field and there are lots of actors involved but it's not our central focus at EUTC. What we look at particularly, is the interaction between cybersecurity and telecoms in operational networks. Security in operational networks is different to fixed IT networks, in that if your network is under attack, you must keep operating. And even if that network is penetrated, such as a national transmission network or electric distribution, you have got to try and continue to operate as you deal with that cyber threat. You can't close the network down.

Because we've got a lot of radio communications, and often this is limited in terms of bandwidth, the security cannot consume too much bandwidth. And in operational networks, latency can be an issue. Sometimes you've got to control things quickly and that means that your security cannot take an indefinite amount of time.

Resilience is obviously crucial. Modern society depends on electricity and society falls apart without it; our food is refrigerated, our financial systems need power, our telecoms need electricity. Keeping electricity networks going is really a big challenge. Resilience means not only keeping them going, but if they do fail, getting them back into operation as quickly as possible.

(BL): I found this quote attributed to you. "The utility man has buttons, belt and braces on his trousers to ensure they don't fall down. The wise utility telecoms manager designs diversity in communication paths and ensures good power backup to guarantee their comms never fail." Can you just give us a bit more around that?

(AG): Resilience has many dimensions. Ideally, we'd want our systems to be 100% available, but nothing is 100%. We generally work to five nines, 99.999% availability, which is 20 minutes outage a year. Transmission networks often work to six nines: which is very high availability. You don't want any single point of failure. A major control room may have three fibre connections, but those fibre connections go out of the control room in three different directions, so that you avoid "JCB corrosion", as we call it, when a digger goes through all your lines.

(BL): What lessons can we learn from the April 2025 power failure

in Spain and Portugal?

(AG): The European power grid is highly resilient because of its interconnections. So, every country supports the other countries around these interconnectors, but when things go wrong, those interconnectors often must be isolated to prevent the whole grid, the whole of Europe, crashing its electricity system. What we've seen in the days of fossil fuel generation are large generators that had a lot of inertia, and they would ride through minor disturbances in the network. As we've moved to more renewables and particularly wind and solar, they're connected through inverters and reduces the inertia in the system. And of course they're intermittent, so they come on and they go off. Our network was never built for that.

Also, in the early days when we had a few big generators, they poured in energy at the top and it came out of your plug at the bottom. It was a one-way system. Now it's a two-way system, and therefore monitoring control is crucial to keep the networks running. And as we've seen with this failure in Iberia and the failure in Italy in 2003; when things go wrong, if you do lose control, they go spectacularly wrong. Our aim in the utility sector is to prevent this happening; but when they do happen, to get back to normality quickly.

(BL): How do we get a true picture of what happened? Regulators and operators are not revealing much information about the failure in Spain and Portugal.

(AG): Getting the true picture is always very complex. People are very careful about what they say because of potential legal repercussions. It is never just one cause. If it was just one item, then the network would be able to cope. And where we've seen in the past these catastrophic grid failures, it's several things happening in very close proximity to one another and the systems can't respond quickly enough.

If we look at the Iberian problem, clearly there were several things interacting together which caused the ultimate failure. What is well-known is that there was a lot of solar generation on the network. There was also wind generation, so renewables connected through inverters were a large percentage of the generation and the amount of inertia on the system was very low.

At the same time, they were also using a lot of energy to restore pump storage systems, so they were pumping water from the lower reservoirs to the higher reservoirs. That meant there wasn't a lot of hydro available to give extra inertia.

What seems to be unclear is the role of the interconnectors. Spain was interconnected with France and there seemed to be discussions about which direction the power was flowing in and the potential influence of the interconnector with Morocco. So again, we saw multiple interactions.

In the 2003 Italian grid collapse, 6 interconnectors tripped within a minute, followed by another 5 two minutes later. You're dealing with a very dynamic situation and it's very difficult to get control back again once you lose it.

(BL): What are the findings of EUTC's AI task force and what are the implications for the next five to 10 years.

(AG): AI is clearly very important to utilities. With all the monitoring and control we do, and with so much data available, it's not possible to process it and get useful information out of it without machine help, so AI is vital going forward.

What we have found is that training AI systems can be very lengthy and data integrity is vital. You also need workforce engagement. This is happening as staff see that AI systems are helping them to do their jobs better and faster, take away some of the boring stuff and make the job more interesting.

To get these systems to work, there must be close collaboration between the user utility, the software supplier, and the hardware supplier. It's not just a matter of buying something off the shelf and deploying it.

We're also aware that AI systems are renowned for "hallucinations" and making completely erroneous decisions, and that's why we are focusing on data integrity, and maintaining human oversight. You can't let these systems have control without someone there checking what they're doing. So, it's going to be a very interesting development for utilities, but we do want to introduce AI under very tight control.

(BL): The Third Generation Partnership Project (3GPP) is a global consortium of standards development organisations that develop technical specifications for mobile telecommunications. Can you tell us about 3GPP standards and what features the utility sector can expect to see?

(AG): We're engaged with 3GPP. It is a very onerous and resource intensive activity, but essential. The sort of features we are looking for in new 3GPP standards are high power user equipment because that will give us longer range and better networks. We're interested in device-to-device, particularly the potential for gatewaying into networks and meshing. We're also seeking to foster collaboration between telecom networks and power networks because we depend on each other. Another area is integration between non-terrestrial networks or satellites and terrestrial so that we have seamless roaming between various networks to enhance our telecoms resilience even more.

(BL): Okay, great. Thank you. We look forward to hearing more details on these topics when we are in Brindisi at CIPRE 2025, see more at https://www.cipre-expo.com/

(AG): Thank you and look forward to seeing you there.

TSA seeks private sector solutions to enhance airport security and passenger experience

The Transportation Security Administration (TSA) recently issued a Request for Information (RFI) for the development and deployment of turnkey solutions for use at airport security checkpoints.

The RFI supports TSA's strategic goal to identify innovative, technology-driven solutions that strengthen aviation security and enhance the overall passenger experience. Respondents are encouraged to propose turnkey models, incorporating cutting-edge screening technologies to deliver a curated, secure, customer-centric experience at security checkpoints.

"TSA is constantly looking for innovative private sector solutions to enhance security and improve the passenger experience at TSA checkpoints," said TSA Acting Administrator Ha Nguyen McNeill. "Homeland Security Secretary Noem recently announced TSA's elimination of the mandate for passengers to remove their shoes. This effort will continue to drive a golden age of travel for future innovations by allowing private sector organizations to submit ideas or solutions that will help make airport screening faster, more secure, and easier on the traveling public."

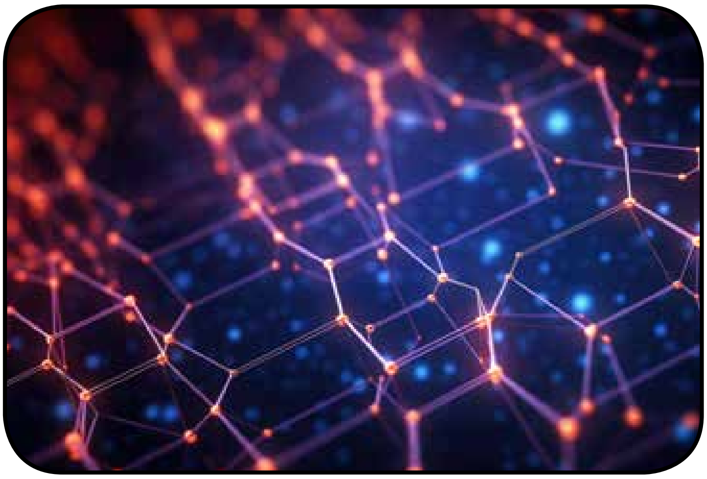
TSA is looking for solutions that will:

- Enhance aviation security effectiveness
- Reduce total operating costs, workforce requirements, and manual labor
- Improve passenger experience and throughput
- Maintain full compliance with TSA's performance standards and regulatory oversight
- Incorporate AI-driven threat detection and remote screening
- Increase adaptability during surge events or staffing constraints
- Optimize workforce capabilities through automation or robotics for passenger and baggage screening

Proposed solutions must meet TSA's high security standards while improving efficiency, reducing wait times, and promoting operational excellence. By integrating advanced technologies with thoughtful checkpoint design, TSA aims to achieve a balanced approach to ensure both safety and satisfaction for passengers nationwide. TSA requires technology adheres to open standards-based data patterns for secure, efficient, and scalable real-time data transmission to the TSA Cloud.

Securing Core Cloud Identity Infrastructure: Addressing Advanced Threats through Public-Private Collaboration

In recent years, the cloud landscape has faced increasingly sophisticated threat activity targeting identity and authentication systems. As cloud infrastructure has become more ubiquitous—underpinning key government and critical infrastructure data—sophisticated nation-state affiliated actors have exposed limitations in token authentication, key management, logging mechanisms, third-party dependencies, and governance practices. These threats reaffirm the critical role that public-private collaboration plays to safeguard cloud infrastructure and address the evolving technical and security challenges confronting our nation.



Challenges in Cloud Identity Security

Cloud providers implement measures to secure cloud identity systems with varying degrees of robustness against security threats. Review of recent cloud security incidents demonstrates threat actors are increasingly exploiting vulnerabilities, forging tokens, and using stolen credentials to compromise organizational infrastructure. To mitigate these risks, cloud service providers can further harden authentication and authorization mechanisms, prioritizing improvements in token technology, secrets management, access control, logging, and forensic capabilities. Uplifting security practices in these areas present complex challenges, including:

- Token Validation Technology: Token management is pivotal to security. Stateless tokens are particularly vulnerable, as the compromise of signing keys can lead to widespread token forgery. While stateful token validation and token binding with proof of possession offer stronger security, system complexity and integration costs hinder their adoption.

- Secrets Management Systems: Scaling centralized secrets management systems risks misconfiguration and inconsistent policies. Secure key storage, like hardware security modules, faces access restrictions and performance trade-offs. Properly managed secrets rotation and optimized frequency are vital for security and continuity.

- Logging Practices: Limited telemetry and short log retention impede detection of forged tokens, compromised keys, and unauthorized token generation. Balancing consumer visibility with manageable log volumes is challenging, while inconsistent logging standards across providers hinder threat detection and response.

Driving Public-Private Partnership to Fortify Infrastructure at Scale

To address these challenges, CISA's Joint Cyber Defense Collaborative (JCDC) is working side-by-side with cloud service providers to foster discovery and discussion of best practices for strengthening cloud identity security. Together, we are exploring innovative solutions, including approaches to better protect tokens to prevent validation errors and forgery, improved secrets management for consistent encryption and access control, and enhanced logging to better detect malicious behavior.

CISA recently hosted the JCDC Cloud Identity Security Technical Exchange, gathering approximately 50 experts across the U.S. federal government and top cloud providers to analyze core cloud identity security practices.

The goal was to promote knowledge transfer across these organizations and to discuss approaches to harden cloud identity infrastructure at scale. The exchange focused on technical insights, operational experiences, and candid perspectives grounded in real-world situations. Insights gleaned from this exchange laid the foundation on how we can work together to improve the adoption of essential cloud identity security practices and enhance the resilience of critical cloud infrastructure.

Public-private operational collaboration like this remains critical to the nation's collective defense. Through JCDC, CISA continues to deepen trust across our closest and most capable partners, sharpening our respective cyber defense capabilities while increasing our reciprocal value to each other.

Nearly Two-thirds of Cybersecurity Pros Say Job Stress Is Growing, According to New ISACA Research

Sixty-six percent of cybersecurity professionals say their role is more stressful now than it was five years ago, according to the newly released 2024 State of Cybersecurity survey report from ISACA, a global professional association advancing trust in technology.

The annual study, sponsored by Adobe, showcases the feedback of more than 1,800 cybersecurity professionals on topics related to the cybersecurity workforce and threat landscape. According to the data, the top reasons for this increased stress are:

- An increasingly complex threat landscape (81 percent)
- Low budget (45 percent)
- Worsening hiring/ retention challenges (45 percent)
- Insufficiently trained staff (45 percent)
- Lack of prioritization of cybersecurity risks (34 percent).

Increasing Cybersecurity Attacks

In line with this sentiment around challenging threats, 38 percent of organizations are experiencing increased cybersecurity attacks, compared to 31 percent a year ago. These top attack types include social engineering (19 percent), malware (13 percent), unpatched system (11 percent) and Denial of Service (11 percent).

On top of that, nearly half (47 percent) expect a cyberattack on their organization in the next year, and only 40 percent have a high degree of confidence in their team's ability to detect and respond to cyber threats.

"Social engineering attacks, such as phishing, are a growing concern for organizations as human error remains a major factor in data breaches," said Mike Mellor, VP of Cyber Operations at Adobe. "With the increasing frequency and sophistication of these attacks, it's essential for organizations to adopt secure authentication methods to strengthen their defenses. Adobe believes that fostering a deep security culture among all employees through anti-phishing training, combined with stronger controls such as zero-trust networks protected by phishing-resistant authentication are essential in safeguarding any organization."

Resource Challenges

Despite an increasingly difficult threat landscape, the survey shows cybersecurity budgets and staffing are not keeping pace. More than half (51 percent) say that cyber budgets are underfunded (up from 47 percent in 2023), and only 37 percent expect budgets will increase in the next year.

Though 57 percent of organizations say their cybersecurity teams are understaffed, hiring has slightly slowed:

- 38 percent of organizations have no open positions, compared to 35 percent last year,
- 46 percent of organizations have non-entry level cybersecurity positions open, compared to 50 percent last year.
- 18 percent have entry-level positions open, compared to 21 percent last year.

Skills and Retention Trends

Employers seeking qualified candidates for open roles are prioritizing prior hands-on experience (73 percent) and credentials held (38 percent). Respondents indicate that the main skills gaps they see in cybersecurity professionals are soft skills (51 percent)—especially communication, critical thinking and problem solving—and cloud computing (42 percent).

For the more than half of survey respondents (55 percent) that reported having difficulties retaining qualified cyber candidates, the main reasons for leaving included being recruitment by other companies (50 percent, down eight points from 2023), poor financial incentives (50 percent), limited promotion and development opportunities (46 percent), and high work stress levels (46 percent).

"Employers should home in on the occupational stress their digital defenders are facing. This is an opportunity for employers to explore ways to support staff before burnout and attrition occur," says Jon Brandt, ISACA Director, Professional Practices and Innovation. "Employees want to feel valued. As the leadership adage goes, take care of your people and they'll take care of you."

New INTERPOL report warns of sharp rise in cybercrime in Africa.

A growing share of reported crimes in Africa is cyber-related, according to INTERPOL's 2025 Africa Cyberthreat Assessment Report.

Two-thirds of the Organization's African member countries surveyed said that cyber-related crimes accounted for a medium-to-high share of all crimes, rising to 30 per cent in Western and Eastern Africa.

Online scams, particularly through phishing, were the most frequently reported cybercrimes in Africa, while ransomware, business email compromise (BEC) and digital sextortion also remain widespread.

Neal Jetton, INTERPOL Cybercrime Director, said, "This fourth edition of the INTERPOL African Cyberthreat Assessment provides a vital snapshot of the current situation, informed by operational intelligence, extensive law enforcement engagement and strategic private-sector collaboration. It paints a clear picture of a threat landscape in flux, with emerging dangers like AI-driven fraud that demand urgent attention. No single agency or country can face these challenges alone."

In the past year, suspected scam notifications rose by up to 3,000 per cent in some African countries, according to data from Kaspersky – one of several private sector partners that works with INTERPOL's cybercrime directorate.

Ransomware detections in Africa also rose in 2024, with South Africa and Egypt suffering the highest number, at 17,849 and 12,281 detections respectively according to data from Trend Micro, followed by other highly digitized economies such as Nigeria (3,459) and Kenya (3,030).

Incidents included attacks on critical infrastructure, such as a breach at Kenya's Urban Roads Authority (KURA), and on government databases, such as hacks of Nigeria's National Bureau of Statistics (NBS).

BEC-related incidents also rose significantly, with 11 African nations accounting for the majority of BEC activity originating on the continent. In West Africa, BEC fraud has driven highly organized, multi-million-dollar criminal enterprises, such as transnational syndicate Black Axe.

Sixty per cent of African member countries reported an increase in reports of digital sextortion, where threat actors use sexually explicit images to blackmail their targets. The images can be authentic – shared voluntarily or obtained through coercion or deception – or they can be generated by artificial intelligence.

Cybercrime continues to outpace the legal systems designed to stop it, according to African law enforcement. Seventy-five per cent of countries surveyed said their legal frameworks and prosecution capacity needed improvement.

20,000 malicious IPs and domains taken down in INTERPOL infostealer crackdown

More than 20,000 malicious IP addresses or domains linked to information stealers have been taken down in an INTERPOL-coordinated operation against cybercriminal infrastructure.

During Operation Secure (January – April 2025) law enforcement agencies from 26 countries worked to locate servers, map physical networks and execute targeted takedowns.

Ahead of the operation, INTERPOL cooperated with private-sector partners Group-IB, Kaspersky and Trend Micro to produce Cyber Activity Reports, sharing critical intelligence with cyber teams across Asia.

These coordinated efforts resulted in the takedown of 79 per cent of identified suspicious IP addresses.

Participating countries reported the seizure of 41 servers and over 100 GB of data, as well as the arrest of 32 suspects linked to illegal cyber activities.

Infostealer malware is a primary tool for gaining unauthorized access to organizational networks. This type of malicious software extracts sensitive data from infected devices, often referred to as bots. The stolen information typically includes browser credentials, passwords, cookies, credit card details and cryptocurrency wallet data.

eu-LISA Publishes Annual Activity Report 2024: A Year of Strategic Progress and Digital Transformation

eu-LISA released its Consolidated Annual Activity Report for 2024, highlighting key achievements and milestones in supporting EU policies through digital solutions.

The report provides a comprehensive overview of the Agency's work in delivering, maintaining and evolving the large-scale IT systems that are essential for the implementation of EU policies in the areas of border management, migration and asylum, internal security and justice.

Strengthening the Schengen Architecture

In 2024, eu-LISA continued to ensure the high availability and stable operation of all core systems under its remit, including the Schengen Information System (SIS), the Visa Information System (VIS), Eurodac, and ECRIS-RI. Notably, the Agency facilitated the connection of Frontex to SIS and enabled full access to VIS for Bulgaria and Romania – key steps in reinforcing Schengen-wide cooperation.

Progress was also made in the delivery of new systems and interoperability components. The Entry/Exit System (EES) baseline version was finalised, and successful joint rehearsals with VIS and the shared Biometric Matching Service (sBMS) were conducted. Although EES could not enter into operation in 2024 as initially planned, the Council endorsed a revised schedule for a progressive rollout starting in October 2025.

Advancing Justice and Digitalisation

As of June 2024, eu-LISA formally took over operational responsibility for e-CODEX – the EU's secure communication platform for cross-border judicial cooperation. In parallel, development advanced on key justice-related systems such as ECRIS-TCN and the Joint Investigation Teams collaboration platform.

Innovation, Cybersecurity and Sustainability

eu-LISA maintained its focus on responsible innovation, integrating cloud technologies and preparing for the use of artificial intelligence in line with EU regulations. Security and data protection remained a priority, with enhanced risk assessments and the implementation of new internal control measures.

The Agency also made significant progress in reducing its environmental footprint, achieving EMAS certification in April 2025 and continuing infrastructure upgrades at its Strasbourg site.

Organisational Transformation and Strategic Planning

In 2024, eu-LISA launched a major organisational change initiative – RAISE – aimed at improving delivery, agility and staff engagement. A strategic management action plan was introduced to strengthen in-house development capabilities, improve governance, and foster stakeholder relations.

eu-LISA reached a 97% implementation rate for outstanding audit recommendations and recorded 100% execution of its 2024 budget, reflecting strong financial discipline and effective performance monitoring.

As Chair of the Justice and Home Affairs Agencies Network (JHAAN) in 2024, the Agency led efforts to enhance inter-agency cooperation, promote digital transformation and address shared challenges in security and justice.

Executive Director ad interim, Marili Männik, stated, "2024 was a pivotal year for eu-LISA. Amid evolving priorities and complex demands, we demonstrated resilience, embraced innovation, and reinforced our role as a trusted digital partner to the EU and its Member States. I am proud of our achievements and confident that our work continues to make Europe safer, more connected and future-ready."

AI standards exchange database

A new AI Standards Exchange Database launched at the latest AI for Good Global Summit will help establish the technical foundations for artificial intelligence (AI) innovations to achieve global impact.

The database forms part of broader collaboration to ensure standards provide practical tools to shape better AI.

It will help standards bodies to coordinate their work and empower companies, policymakers and regulators with comprehensive suites of AI standards.

Translate, structure, include, connect

"Standards development organizations ultimately translate principles into practical implementation," said IEC Secretary-General and CEO Philippe Metzger. "We have a real need of translating that in the field of AI into actual governance."

Standards bodies need to collaborate in a structured way to ensure the clarity and coherence essential to global impact, he added.

Metzger emphasized the importance of inclusive standards processes, building standards capacity around the world, and strong connections among standards developers and their growing range of stakeholders.

No one left behind

ISO President Sung Hwan Cho also stressed the importance of building standards capacity everywhere.

"Inclusion and diversity are at the core of international standards' goal," said Cho. "We have to ensure no one is left behind."

He called for a human-centred AI ecosystem where standards address societal as well as technical challenges.

"AI standards should cover technology, but also how AI benefits humanity," he said.

Partnerships paramount

Together, IEC, ISO and ITU are known as the World Standards Cooperation.

"This partnership is key to comprehensive standards development for AI," said Seizo Onoe, Director of ITU's Telecommunication Standardization Bureau.

ITU maintains productive relationships and collaboration with numerous other standards bodies, he added.

"AI has created even stronger connections among standards bodies, and AI is evolving very fast," said Onoe. "We want to ensure that our standards keep pace with this evolution."

The new AI standards database supports technical cohesion and interoperable solutions – key aims of the Global Digital Compact adopted last year as part of the UN Pact for the Future.

New resources

The AI for Good summit also launched landmark resources on standards and policy considerations for multimedia authenticity from the AI and Multimedia Authenticity Standards Collaboration.

Driven by IEC, ISO, ITU and other key standards communities, the collaboration is advancing standards to detect deepfakes and verify multimedia authenticity and provenance.

EPA Announces Grant of 9 Million Dollars to Protect Drinking Water from Natural Hazards and Cybersecurity Threats

The EPA has announced that the agency is making $9 million available in grant funding for midsize and large water systems to help protect drinking water from cybersecurity threats and improve operational resilience in the face of extreme weather events. WaterISAC is sharing other funding opportunities that water and wastewater utilities can apply for to help enhance their operational resilience.

Investing in resilience and cybersecurity efforts is crucial for all water and wastewater utilities. Indeed, a report from the National Institute of Building Sciences estimated that every $1 invested in pre-disaster mitigation has led to a $6 savings. According to EPA, the Safe Drinking Water Act (SDWA) authorizes the agency to establish the Midsize and Large Drinking Water System Infrastructure Resilience and Sustainability Program.

Global operation targets NoName057(16) pro-Russian cybercrime network

A joint international operation, known as Eastwood and coordinated by Europol and Eurojust, targeted the cybercrime network NoName057(16). Law enforcement and judicial authorities from Czechia, France, Finland, Germany, Italy, Lithuania, Poland, Spain, Sweden, Switzerland, the Netherlands and the United States took simultaneous actions against offenders and infrastructure belonging to the pro-Russian cybercrime network. The investigation was also supported by ENISA, as well as Belgium, Canada, Estonia, Denmark, Latvia, Romania and Ukraine. The private parties ShadowServer and abuse.ch also assisted in the technical part of the operation.

The actions led to the disruption of an attack-infrastructure consisting of over one hundred computer systems worldwide, while a major part of the group's central server infrastructure was taken offline. Germany issued six warrants for the arrest of offenders living in the Russian Federation. Two of these persons are accused of being the main instigators responsible for the activities of "NoName057(16)". In total, national authorities have issued seven arrest warrants, which are directed, inter alia, against six Russian nationals for their involvement in the NoName057(16) criminal activities. All of the suspects are listed as internationally wanted, and in some cases, their identities are published in media. Five profiles were also published on the EU Most Wanted website.

National authorities have reached out to several hundred of individuals believed to be supporters of the cybercrime network. The messages, shared via a popular messaging application, inform the recipient of the official measures highlighting the criminal liability they bear for their actions pursuant to national legislations. Individuals acting for NoName057(16) are mainly Russian-speaking sympathisers who use automated tools to carry out distributed denial-of-service (DDoS) attacks. Operating without formal leadership or sophisticated technical skills, they are motivated by ideology and rewards.

NoName057(16) DDoS disruption attempts in favour of Russia

Offenders associated to the NoName057(16) cybercrime network targeted primarily Ukraine, but have shifted their focus to attacking countries that support Ukraine in the ongoing defence against the Russian war of aggression, many of which are members of NATO.

National authorities have reported a number of cyberattacks linked to NoName057(16) criminal activities. In 2023 and 2024, the criminal network has taken part in attacks against Swedish authorities and bank websites. Since investigations started in November 2023, Germany saw 14 separate waves of attacks targeting more than 250 companies and institutions.

In Switzerland, multiple attacks were also carried out in June 2023, during a Ukrainian video-message addressed to the Joint Parliament, and in June 2024, during the Peace Summit for Ukraine at Bürgenstock. Most recently, the Dutch authorities confirmed that an attack linked to this network had been carried out during the latest NATO summit in the Netherlands. These attacks have all been mitigated without any substantial interruptions.

Central coordination to target the pro-Russian cybercrime network

Europol facilitated the information exchange and supported the coordination of the operational activities, serving as a hub for the communication between national authorities and EU agencies. For that purpose, Europol organised over 30 online and offline meetings and two operational sprints. Europol also facilitated cooperation with private partners, who offered their assistance both ahead of and following the operation. The Agency provided extensive analytical support, as well as cryptocurrency tracing and forensic expertise over the course of the investigation. Europol coordinated the prevention campaign, released to alleged affiliates via messaging apps and social media channels.

Nokia and Leonardo partner to deliver worldwide mission-critical private wireless networks for public safety and critical infrastructures

Nokia has announced a partnership with Leonardo to deliver cutting-edge mission-critical services worldwide integrated into Nokia's Core Enterprise Solutions.

The solid collaboration strengthens Nokia's leadership in secure and scalable private wireless connectivity for essential services like public safety and industrial segments such as energy and railways that demand the highest performance, resilience, and reliability levels.

Nokia will embed Leonardo's flagship Mission Critical Services platform MC_linX a next-generation broadband mission-critical services platform, into Nokia's enterprise solutions portfolio. This technology combination will deliver worldwide a pre-integrated solution that accelerates deployment, reduces complexity, and ensures operational readiness. It also enables faster emergency response, increasing operational safety, and improving service reliability – ultimately benefiting communities and essential services worldwide.

"By combining Nokia's robust private wireless and core software capabilities with Leonardo's trusted mission-critical technologies, we are delivering a seamless solution that meets the stringent demands of industries like public safety, energy, and rail. This partnership demonstrates our commitment to empowering critical infrastructure with secure, real-time, resilient communication solutions," commented Prakash Sadagopan, Head of Enterprise Wide Area Networks at Nokia.

ESET participates in operation to disrupt the infrastructure of Danabot infostealer

ESET has participated in a major infrastructure disruption of the notorious infostealer, Danabot, by the US Department of Justice, the FBI, and US Department of Defense's Defense Criminal Investigative Service.

U.S. agencies were working closely with Germany's Bundeskriminalamt, the Netherlands' National Police, and the Australian Federal Police . ESET took part in the effort alongside Amazon, CrowdStrike, Flashpoint, Google, Intel471, PayPal, Proofpoint, Team Cymru and Zscaler. ESET Research, which has been tracking Danabot since 2018, contributed assistance that included providing technical analysis of the malware and its backend infrastructure, as well as identifying Danabot's C&C servers. During that period, ESET analyzed various Danabot campaigns all over the world, with Poland, Italy, Spain and Turkey historically being one of the most targeted countries. The joint takedown effort also led to the identification of individuals responsible for Danabot development, sales, administration, and more.

These law enforcement operations were conducted under Operation Endgame — an ongoing global initiative aimed at identifying, dismantling, and prosecuting cybercriminal networks. Coordinated by Europol and Eurojust, the operation successfully took down critical infrastructure used to deploy ransomware through malicious software.

"Since Danabot has been largely disrupted, we are using this opportunity to share our insights into the workings of this malware-as-a-service operation, covering the features used in the latest versions of the malware, the authors' business model, and an overview of the toolset offered to affiliates. Apart from exfiltrating sensitive data, we have observed that Danabot is also used to deliver further malware, which can include ransomware, to an already compromised system," says ESET researcher Tomáš Procházka, who investigated Danabot.

Aéroport Toulouse-Blagnac and Airbus Protect sign a strategic cybersecurity contract

Aéroport Toulouse-Blagnac (ATB) and Airbus Protect have signed a multi-year cybersecurity contract, marking the beginning of a strategic partnership aimed at enhancing the security of the airport's digital infrastructure.

By leveraging Airbus Protect's expertise, the partnership will ensure the continuous monitoring and protection of the airport's information systems and critical assets.

Under the agreement, Airbus Protect will deliver advanced cybersecurity solutions, including real-time monitoring, threat detection, and response capabilities. This initiative aligns with the shared goal of strengthening the resilience of the aviation ecosystem and fostering a secure environment for all stakeholders.

In 2024, the Toulouse-Blagnac airport welcomed around 8 million passengers travelling to more than 80 destinations. More than 65,000 flights were operated to and from this airport, by 26 airlines.

"Cybersecurity is a top priority. We are confident that Airbus Protect's expertise will play a pivotal role in protecting our systems and maintaining the high standards of security our passengers and partners expect."said Philippe Crébassa, President of the Toulouse-Blagnac Airport.

"We are pleased to partner with Toulouse Airport to address their cybersecurity needs. This collaboration reflects our mutual commitment to securing the future of air travel and ensuring the trust and safety of passengers, operators and the aviation ecosystem at large." commented Thierry Racaud, CEO of Airbus Protect.

Major European Financial Institution Selects Corero Network Security in Multi-Year Deal to Safeguard Critical Infrastructure

Corero Network Security, a recognized leader in DDoS protection and champion of adaptive, real-time service availability, announced it has secured a multi-year agreement with a leading European financial institution to enhance the resilience and availability of critical digital services.

The win underscores Corero's growing role in the global financial services sector and highlights the strategic value of its alliance with Akamai Technologies, which enables integrated protection strategies for enterprise environments.

Under the terms of the agreement, Corero will replace an incumbent on-premises DDoS protection solution following performance challenges and limited support experienced by the customer. Corero's ease of use, real-time mitigation capabilities and leading security operations center services were key factors in the decision. The agreement spans an initial three-year term and an optional two-year extension for a single country with the opportunity for further growth.

The customer already relies on Akamai's cloud-based DDoS protection. By adding the on-premises component, sold as Akamai Prolexic On-Prem powered by Corero, they gain a unified defense model that delivers high availability, operational visibility and proactive mitigation against evolving cyber threats. Procuring the full solution through Akamai also streamlined the purchasing and deployment process.

RTX BBN Technologies to advance high-fidelity exploit chain testing and evaluation

RTX's BBN Technologies was awarded a contract from DARPA to support its Intelligent Generation of Tools for Security, or INGOTS, program.

INGOTS aims to strengthen cybersecurity by developing advanced methods to identify and mitigate complex exploit chains, preventing their use in real-world attacks.

Exploit chains pose a growing threat, amplified by the increasing complexity and sophistication of cyberattacks. The U.S. Cybersecurity and Infrastructure Security Agency's Known Exploited Vulnerabilities catalog has surpassed 1,300 entries, with steady growth reflecting the increasing number of threats targeting essential services and networks. Despite this rising threat, current assessment methods rely heavily on manual analysis, requiring significant expertise and time. INGOTS seeks to address this challenge by automating the creation, modification, modeling and analysis of exploit chains to enable faster and more effective security interventions.

"Effectively countering exploit chains requires more than just identifying individual vulnerabilities. It demands a system that can replicate real-world attack scenarios and anticipate potential risks before they are exploited," said Jack Dietz, BBN principal investigator.

To support this effort, BBN will apply its expertise in testbed architecture to develop the System Test of Android at Large-scale Accelerating Generation and Modeling for INGOTS Test and Evaluation, or STALAGMITE. This system will serve as a comprehensive platform for testing and evaluating exploit analysis tools, offering key capabilities such as:

- Accurate real-world simulations: High-fidelity testing in combined virtual and physical environments ensures realistic assessments of Android vulnerabilities in a secure and controlled setting.
- Proactive threat responses: Seamless integration of INGOTS components enables security teams to anticipate and mitigate potential attacks, enhancing preparedness against emerging threats.
- Efficient security research: A robust environment for reproducible, automated testing advances research in software vulnerabilities and countermeasures, improving operating system and application security.

Eviden to Deploy a 5G Mobile Private Network at Port of Ploce

Eviden, the Atos Group product brand leading in advanced computing, cybersecurity products, mission-critical systems and vision AI, has announced that it has been awarded a strategic contract to deploy a 5G Mobile Private Network featuring key components of its Lifelink solution at the Port of Ploče in Croatia.

This initiative marks a major step in the port's digital transformation journey through the ambitious Smart Port project, aimed at modernizing logistics, improving operational efficiency, and enhancing security using cutting-edge 5G technology.

The Port of Ploce serves as a critical logistics hub in Central and Southeastern Europe, and the deployment of a dedicated 5G network will enable seamless, real-time connectivity across port operations.

The Lifelink 5G Mobile Private Network key components deployed by Eviden's critical communications experts, support:

- Real-time location system (RTLS)
- Advanced cargo monitoring
- Incident prevention and manaagement
- Drone surveillance

"Through this agreement, we will significantly enhance and digitalize processes within the port area. This will ultimately enable better traffic management, increase efficiency in the transport of goods and passengers, improve safety in cargo transport and port operations, and reduce pollution," said Tomislav Batur, Director of the Port of Ploce Authority.

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 Week *in Europe*

14th-16th October 2025 - Brindisi, Italy

International Association of CIP Professionals

critical infrastructure PROTECTION AND RESILIENCE EUROPE

T I E M S

With the patronage of the City of Brindisi

Co-Hosted by:

International Association of CIP Professionals

UNIVERSITÀ DEL SALENTO
DIPARTIMENTO DI INGEGNERIA DELL'INNOVAZIONE

CRISR

REGISTER ONLINE TODAY

Register at www.cipre-expo.com/register
and benefit from Early Bird Discounts

Early Bird Deadline - 14th September

Securing the Inter-Connected Society

The second 'Critical Infrastructure Protection Week' will take place in Brindisi, Italy on 14th-16th October and will see IACIPP host the 10th 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'The International Emergency Management Society (TIEMS)' conference.

The premier event for the critical infrastructure protection and resilience community, Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

The recent implementation of The Critical Entities Resilience (CER) and NIS2 Directives, which lays down obligations on EU Member States to take specific measures to ensure that essential services and infrastructures, for the maintenance of vital societal functions or economic activities, are provided in an unobstructed manner in the internal market, enhancing security requirements, reporting obligations, and crisis management capabilities.

Compliance with the CER Directive and NIS2 Directive are crucial for businesses operating in the EU to safeguard their systems, mitigate threats, and ensure resilience. Penalties are enforceable on agencies and operators for non-compliance.

Join us in Brindisi, Italy for the next CIP Week in Europe and the 10th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure.

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Speaker line-up includes:

- Claudio Ciccotelli, Head of National Cybersecurity Perimeter Division Regulatory Directorate, National Cybersecurity Agency
- Harald Drager, President, The International Emergency Management Society (TIEMS)
- Cdr Col. Antonino Massara, Commander 36' Fighter Wing Commander, Ministry of Defence, Italy
- Robert Tucker, Resilient Network Manager, ESB, Ireland
- Bartel Meersman, Transport And Border Security Head Of Unit, European Commission Joint Research Centre
- Adrian Grilli, Technology Adviser, EUTC, Belgium
- Frederic Guyomard, Senior Project Manager / Cybersecurity Research Engineer, Electricite De France
- Dr Oleksandr Potii, Chairman, State Service of Special Communications and Information Protection of Ukraine (SSSCIP)
- Giampaolo Panariello, CTO Network Infrastructure, Nokia
- Daniel Golston, Associate Programme Officer, Organization for Security and Co-operation in Europe
- Alessandro Lazari, Fellow in Critical Infrastructure Protection and Resilience University of Salento, Italy & IACIPP

Full speaker line-up at **www.cipre-expo.com**

Executive Sponsors:

TCCA E.DSO EUTC AUTO-ISAC

Supporting Organisations:

EE-ISAC CCNE CoESS Help2Protect ISIO

Platinum Sponsor

eset Digital Security Progress. Protected.