critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

SPRING 2025
www.cip-association.org

FEATURE:
The US Defense Industrial Base Risks & Opportunities

FEATURE:
Unlocking the Potential of Public-Private Partnerships for Enhanced Security

FEATURE:
Rapid Reconnaissance Surveillance for Energy Infrastructure: A new era of energy site security

SYNERGIES BETWEEN DIRECTIVES THE CRITICAL ENTITIES RESILIENCE DIRECTIVE (CER), GDPR, NIS2 AND DORA.

Critical Infrastructure Protection Week *in Europe*

14th–16th October 2025 – Brindisi, Italy

International Association of CIP Professionals

critical infrastructure PROTECTION AND RESILIENCE EUROPE

STIME

INVITATION TO ATTEND

Securing the Inter-Connected Society

With the patronage of the City of Brindisi

The International Association for CIP Professionals is delighted to be hosting the 2025 CIP Week in Europe with the patronage of the City of Brindisi.

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

Co-Hosted by:

International Association of CIP Professionals

UNIVERSITÀ DEL SALENTO
DIPARTIMENTO DI INGEGNERIA DELL'INNOVAZIONE

CRISR

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

To discuss sponsorship opportunities:

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

PREDICTING WHEN THE (UN)PREDICTABLE IN UNCERTAIN TIMES

It's been another interesting and challenging period since our last publication. We have seen Heathrow Airport suffer a huge power outage, causing mass travel disruptions for tens of thousands of people for a few days, as well as an international power outage between Spain and Portugal, putting millions in the dark for a period of time. You can read more thoughts about this later in the publication.

Much of this was already known as a possible threat to continuous power supply, but we still seem unprepared for when it actually happens. Spain saw some public disorder requiring the intervention of law enforcements services as thieves took advantage of now lights or security systems and ransacked shops.

A huge disruption and impact on the economy and people's lives in both cases. So how was this missed by the brightest of minds?

President Trump's policies are also creating uncertainty, with the Federal Emergency Management Agency (FEMA) is undergoing significant changes with a combination of restructuring, shifting responsibilities to state and local governments, and altering funding priorities. This has led to debates about the agency's future role and its ability to effectively respond to increasing disaster threats.

There is also a desire to significantly alter the Cybersecurity & Infrastructure Security Agency's (CISA) operational priorities and funding, which has generated considerable debate about the agency's role in safeguarding national cybersecurity. What short term (and long term) impact could this have on infrastructure security and stability?

We watch this space as answers to these challenges unfold, but it certainly adds to the challenges of predicting when the predictable will happen to secure our critical infrastructures. It certainly emphasises the need to continue the discussions and sharig of information and ideas.

Enjoy this edition of CIPR News, our way to help share information, experiences and stories.

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.

Synergies between Directives the Critical Entities Resilience Directive (CER), GDPR, NIS2 and DORA.

By Michael Kolatchev, Principal for Rossnova Solutions (Belgium) & Lina Kolesnikova, Senior Consultant for Rossnova Solutions (Belgium)

Major incidents – floods, forest fires and terrorist attacks – do not respect national borders, and cooperation within the EU is a prerequisite for effective risk, security and crisis management.

Before 2008, the situation regarding critical infrastructure protection (CIP) at the national level varied greatly: for example, eleven countries did not even have a national definition of critical infrastructure. While some Member States were only beginning to recognise the need for action, others had national CIP programmes that were more advanced than the proposed European initiatives. There were also differences in leadership: in some countries critical infrastructure protection was overseen by the defence ministries, in others by the interior ministries or by civil protection departments, etc.

Regulations and Directives

The European Union is based on the rule of law. Every action taken by the EU is based on the treaties - the binding agreements between EU member states, which set out the objectives of the EU, the rules for EU institutions,

the way decisions are taken, and the relations between the EU and its members. The Treaties are the starting point for EU law and are known in the EU as primary law. The body of law that follows from the principles and objectives of the Treaties is known as secondary law and it includes regulations, directives, decisions, recommendations, and opinions.

Regulations are binding legislative acts. They must be applied in its entirety across the EU. In turn, Directives require EU countries to achieve certain results, and, sometimes, introduce certain frameworks, but leave members free to choose how precisely to do that. EU countries must take measures to incorporate (transpose) directives into national law in order to achieve the objectives set out in the directive. National authorities must notify these measures to the European Commission.

Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

The terrorist attacks in Madrid (2004) and in London (2005) drew attention to the risk of terrorist attacks on European critical infrastructure. To counter potential vulnerabilities, the European Council asked the European Commission to prepare a common strategy and action plan to improve the protection of the European Critical Infrastructure (ECI). As a result of this request, the Commission proposed the establishment of the European Critical Infrastructure Protection Programme (EPCIP, which consisted of three main parts:

- the Directive on the identification and marking of ECI,
- the financial programme, and
- the Information Alert Network (CIWIN).

While the Directive formed the core of the programme, the other two components represented key measures designed to facilitate the implementation of the Directive.

First of all, the Directive introduced the concept of European Critical Infrastructure and was based on an 'all-hazards approach', with terrorism being given priority. The scope of EPCIP was limited to the energy and transport sectors, as these two sectors had horizontal implications and were also the most advanced in terms of developing sectoral criteria.

If we consider the conceptual basis for understanding the EU crisis management cycle for critical infrastructures protection in 2008, then EPCIP fell under the stages of prevention and preparedness.

The primary responsibility for protecting critical infrastructure at member state lied with the Member States, their national authorities and the owners/ operators of such infrastructure. This was also recognised by the Directive. The principle of subsidiarity and the fact that CIP is closely interlinked with national defence issues was one of the explanation for the partial reluctance of Member States to share information and kept national primacy in this area. (MK&LK: Subsidiarity is a principle that allows individual members of a larger organisation to make decisions on issues that concern them, rather than leaving these decisions to the group as a whole).

Reasons to change the approach to CIP

The following years after Directive 2008 were marked by significant events and challenges for EU. Among the most important were terrorist attacks, pandemic of covid 19, floods and acts of sabotage on CI.

The COVID 19 pandemic has revealed a more insidious risk picture, with increased spillover risks (those that usually trigger different types of crises), greater interconnectedness of sectors and the need for more coordinated response mechanisms in the EU.

For example, the pandemic has demonstrated how disrupted supply chains can negatively impact societies and economies across sectors and borders.

New and developing trends, which, first, thought to be primarily positive, further challenged the existing situation with CIP. Among such trends were across the board digitalization, the emergence of smart city systems, and the growing interdependence of critical infrastructure.

CIs in Europe often use old software and hardware. This situation creates a problem of "bad legacy" when these old technologies with their large technical debt get integrated into new "smart" system, a system of systems.

If there were not enough risks… Organized Crime

Often, considerations of the risk of criminal activity to critical national infrastructure (CNI), assume that threats come only from outside the CNI. That assumption cannot hold anymore. In recent years, we have seen the rise of organized crime networks that see CNI as a means to use and abuse convenient, publicly accessible legitimate infrastructures for their own gain.

In the past, criminal enterprises built their own infrastructures to be independent of the legitimate world. Today, providing adequate services is very expensive and time-consuming, and the infrastructure needed may be too large to hide. Consequently, criminals are no longer interested in building their own critical infrastructure. Instead, these legitimate critical (and non-critical) infrastructures that provide modern services, regardless of domain, will increasingly be used by criminals, leading to a need for criminals to participate in such infrastructure, have influence, create a specialized layer, and even a controlling position.

All these developments became a driver for major overhaul in CIP approach

CIP is becoming an area where protection and control over processes and data are key factors. In the context of evolving risks and emerging systems of systems, it is becoming increasingly difficult to trust (and to verify and control) existing security measures and governance. They (both measures and governance) require dialogue, consultation, participation, education and awareness; there is no substitute for good management. All parties involved must become comparable, compatible and speak the same language.

That is the context where new Directives fit, set to define common approach to common problems, and to align Members around objectives, frameworks and methods of achieving them.

Modern landscape is more and more thought of as a complex system, whose components are themselves complex systems. As with any complex system, it is rather impossible to get it in full detail at once. Hence, the step by step, piece by piece, process of singling out one view, on one or few components of a complex system. Legislation follows the same pattern, putting one piece at a time, with us all hoping these pieces will come to work together.

Currently, the following Directives are the primary ones related to Critical Infrastructure Protection:

- Directive 2022/2557 (CER, Critical Entities Resilience Directive)
- Directive 2022/2555 (on measures for a high common level of cybersecurity across the Union)
- DORA (Digital Operational Resilience Act)
- GDPR (General Data Protection Regulation)

CER Directive highlights shifting focus (from protection to resilience) while maintaining an all-hazards and all-risks approach. Identifying critical infrastructure across EU, in a uniform way. The CER Directive

	CER	NIS2	DORA	GDPR
Geographical reach	EU	EU	EU	EU+
Primary focus on protection vs resilience	Resilience, Protection	Protection (resilience, to some extent)	Resilience	Protection
Primary focus of protection / resilience on operation, infrastructure, or data	Infrastructure and Operations	Infrastructure and Operations	Operations	Data (customers' personal data, privacy)
Primary focus managed at	National level	National level	National level	EU-wide
Physical vs ICT (cyber) risks	Physical and ICT / Cyber (as provided for in NIS2)	ICT / Cyber	ICT / Cyber	ICT / Cyber (primarily)
Multi-industry (sector) vs single industry (sector)		Multi (wide selection)	Single (financial services)	Multi (All)
Most entities vs essential (critical, main) entities	Critical entities	Essential (critical) and Important entities	All, within the sector	All and any entity
Supply chain included?			Yes, 3rd party (ICT) providers	Yes (to some extent)
Risk management, risk assessment	Yes	Yes	Yes	
Incident Reporting	Yes	Yes	Yes	Yes (especially, notifications of breaches)
Incident Response	Yes	Yes	Yes	Only the need in having one
Data protection	To some extent with cybersecurity measures	To some extent with cybersecurity measures		Primary focus
Establishing compliance criteria and penalising non-compliance	Yes (detailed at national level)	Yes (detailed at national level)	Yes (detailed at national level)	Yes
Implementation timing	2024	2024 (but earlier for its predecessor NIS)	2025	2018
Remarks, specifics	Shift from Protection to Resilience, recognising cross-border and cross-realm (physical and cyber) dependencies	Focus on cybersecurity	Focus on financial sector	Focus on data, defining roles and responsibilities of organisations dealing with customers' (personal) data

recognises that the effects of significant disruptions are felt well beyond the virtual realm and can impact facilities, roads, railways, electricity generation and other infrastructure on which essential services depend. The CER Directive aims at improving and harmonising resilience strategies and plans of Member States and organisations. The Directive covers three priority areas: preparedness, response and international cooperation. It invites Member States to update their risk assessments to reflect current threats and calls on them to stress test undertakings operating critical infrastructure, with the energy sector being a priority. It also calls on Member States to develop, in cooperation with the Commission, a coordinated response plan to critical infrastructure disruptions of significant cross-border significance. The EU will support partner countries in strengthening their resilience.

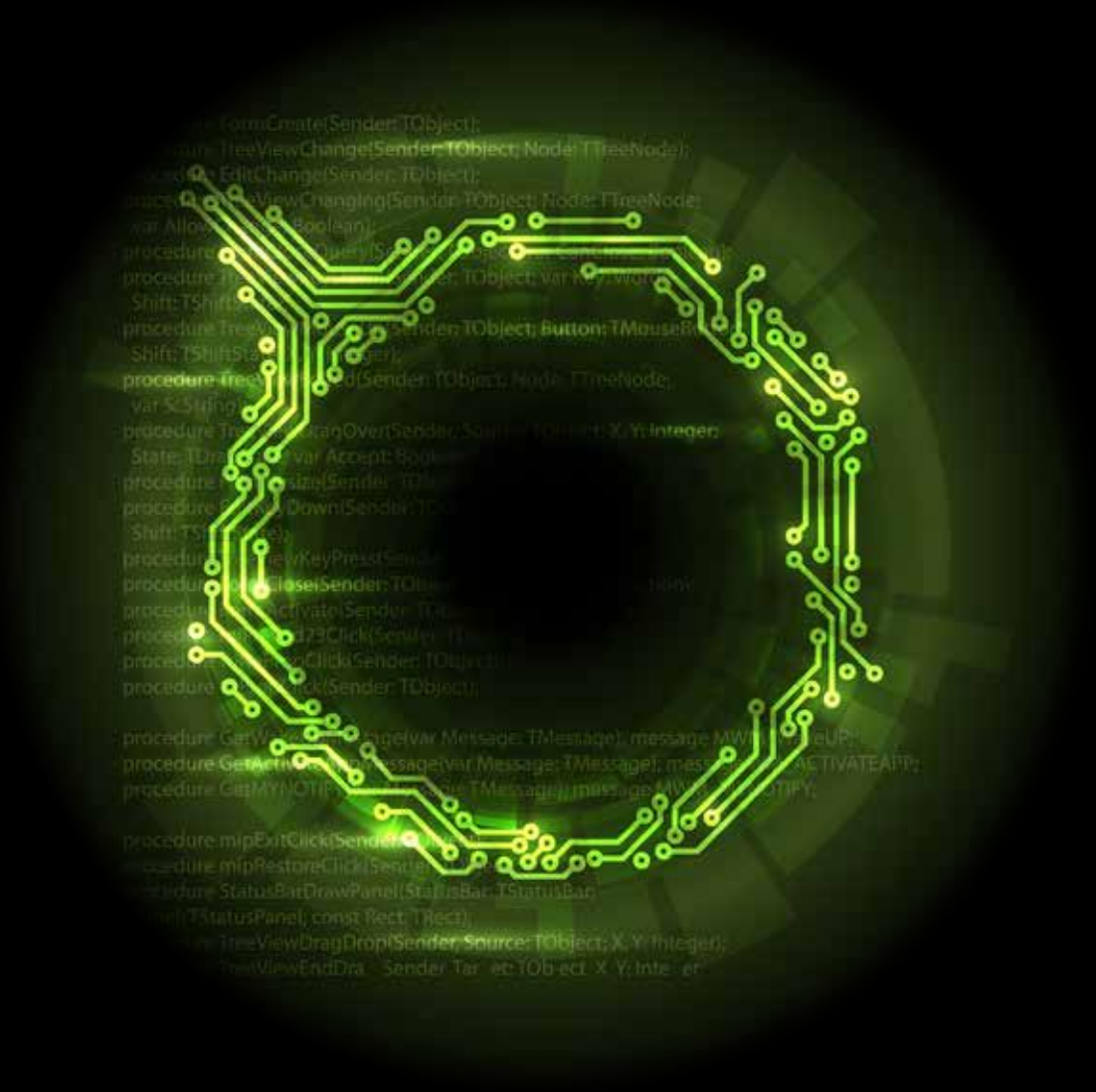
While the CER Directive defines critical infrastructure and related industries and takes an all-hazards, cross-domain approach, the other directives provide more specific guidance: NIS2 focuses on cybersecurity, DORA addresses the financial sector, while the GDPR takes a holistic view of customer (personal) data protection.

Conclusion

In today's world of conflicting cultural views, social interests, political agendas, individual career aspirations and risks, strong domestic, national, intra-national and geopolitical dependencies, finding common ground is a complex task. Reconciling interests and goals, values and visions requires long-term commitment and courage from those who usually work in short-term positions. Critical thinking is the key skill required to achieve this. It all starts with defining a goal (or set of goals with their interrelationships) that is equally clear and understandable. Goals and even core values such as free speech, security and prosperity must be honestly agreed upon.

It is very difficult, if not impossible, to create a comprehensive, perfectly coordinated and non-controversial legislation that covers all relevant topics at the same time. Interested parties can legislate on one or more topics at the same time. Over time, these individual pieces will hopefully form a puzzle without holes, without unevenness in approach, breadth and depth of coverage. As they say in science, a clear definition of the problem already contains half the solution. Each of the above-mentioned directives addresses one aspect or part of a larger problem. These are the pieces of the future illustrated puzzle that we should all strive to complete.

Deloitte.



Delivering America's Critical Infrastructure Future

Today's infrastructure challenges require an advisor that has the breadth of experience, technology capabilities, and demonstrated success working on some of the largest infrastructure projects of our time. Deloitte has the experience, tools, and methodologies to address major projects differently and to help our clients achieve breakthrough outcomes.

Learn more at deloitte.com/us/en/infrastructure

The US Defense Industrial Base Risks & Opportunities

By Bruce Andrews, Partner and Troy Medeiros, Vice President, Alderman And Company

In this article, we examine how supply chain disruptions in minerals, electronics, and skilled labor are creating risks and opportunities in the US Defense Industrial Base (USDIB).

Minerals: Rare Earth Elements

The USDIB relies on Rare Earth Elements (REEs). REEs, loosely defined, are a set of 17 nearly indistinguishable lustrous silvery-white soft heavy metals. The term 'rare-earth' is misleading because they are not actually scarce. REEs are common throughout the Earth's crust. However, because of their geochemical properties, most REEs are highly dispersed as trace elements. Geological regions with relatively high concentrations of REE are rare and even in these rare instances, obtaining usable quantities of pure REEs requires processing enormous amounts of raw material at great expense.

REE is mined by first removing rock from the ground that contains the REE. Most rare-earth ores are mined by conventional open-pit methods in which rock is broken by blasting, loaded onto trucks with large shovels, and hauled to a concentration facility.

Concentration is by physical separation of the REE-bearing minerals from all other minerals in the rock. The ore is crushed and ground in multiple stages until most of the rare-earth minerals interlocked with the other minerals are broken free. Next, in a method known as froth flotation, the rare-earth minerals are coated with a chemical that repels water and allows them to float to the surface attached to air bubbles in agitated tanks, where they are skimmed off as a concentrate. The remaining minerals are disposed of as waste and the REE concentrate is then ready for leaching.

The REE concentrate is then leached with an acid and the resulting REE-rich solution is then processed through sequential steps to recover individual REEs. For example, Cerium can be recovered by the addition of sodium hydroxide, which causes the cerium to drop out of solution as an oxide or hydroxide. The other REEs are typically separated by solvent extraction, a process in which an organic chemical specially designed to extract a particular REE is forced countercurrent to the REE-bearing leach solution. Mining and concentration of REE ores presents conventional problems of concentrate waste disposal. For every ton of REEs produced, the process yields an estimated 75 cubic meters of wastewater and one ton of radioactive residue.

From the mid-1960s to the early 1990s, the United States was the world's largest REE-producing country, with production coming entirely from the Mountain Pass mine in southeastern California. The mine was discovered in 1949 by a uranium prospector. The

mine is located in San Bernardino County, California, on the south flank of the Clark Mountain Range. The mine has been active since 1952, with production expanding in the 1960s. In 2020, the mine supplied 15.8% of the world's rare-earth production. Today the mine is owned by MP Materials Corp (NYSE: MP). At this time, MP Materials Corp. is the largest producer of rare earth materials in the Western Hemisphere. The company recently raised $1B to expand its capacity. The Mountain Pass mine is currently the only active REE mine in the United States.

In the late 1980s, China began mining their in-country REE deposits, processing their ore and extracting and separating the individual REEs for use in products, which they also manufactured. China quickly gained control of global REE production, providing 95 percent of the global market of processed REE by 2011. Between 2011 and 2017, China produced approximately 84 percent of the world's REEs.

China was able to establish dominance over the REE industry in large part because of its lower environmental regulations. Low cost, high pollution extraction methods enabled China to outpace competitors and create a strong foothold in the international REE market. The largest REE mine in the world at this time is the Bayan-Obo mine in China. At this mine, there are an estimated 70,000 tons of radioactive thorium waste in storage ponds in the area. These waste ponds are not far from the Yellow River and there is concern that they could eventually leach into the river, which is a key source of drinking water for a substantial population. To maintain its dominance in REEs, China is also in the process of expanding its REE mining operations outside of mainland China. China has obtained rights to the REE deposits in a handful of African countries in return for infrastructure investment, including but not limited to the Democratic Republic of the Congo in return for building national roads, highways, and hospitals. China has obtained commercial licenses for REE mines in Kenya by agreeing to build a $600+ million data center

President Trump's recent comments that he wants the US to "purchase Greenland" have made international headlines. While we

IULIIA KONOVALIUK/ISTOCK/GETTY IMAGES PLUS, ADAPTED BY E. OTWELL

1. Mountain Pass, Calif. (U.S.)
2. Araxá (Brazil)
3. Lovozero (Russia)
4. Khibiny (Russia)
5. Bayan Obo (China)
6. Weishan (China)
7. Maoniuping (China)
8. Longnan (China)
9. Northern Myanmar
10. Thai Peninsula (Thailand)
11. Chavara (India)
12. Karonge (Burundi)
13. Mandena (Madagascar)
14. Mount Weld (Australia)

SOURCE: E. DEADY/GLOBAL RARE EARTH ELEMENT (REE) MINES, DEPOSITS AND OCCURRENCES/BRITISH GEOLOGICAL SURVEY 2021

will not comment on the politics of this, we are glad to comment on one of the reasons why he said this. One reason was the Kvanefjeld deposit in Greenland is estimated by scientists to be one of the largest known REE deposits on earth. China has been in discussions with Greenland since 2017 about gaining rights to mine Kvanefjeld. To date, Greenland has rejected China's offers regarding Kvanefjeld. Given that much of the Island has not yet been fully explored for REEs, many scientists believe that Greenland may hold substantial REE deposits. Furthermore, with receding Artic Ice (due to global warming), the costs of extracting REEs from Greenland are expected to decline significantly.

Electronics: Computer Chips

Semiconductors and advanced electronics form the technological backbone of modern defense systems, powering communications, surveillance, and weapons guidance. However, the semiconductor industry has been plagued by significant supply disruptions. A global chip shortage that began with the COVID – 19 pandemic in 2020 has persisted, driven by surging demand, throughput constraints, and an overreliance on semiconductor fabs in Taiwan. Furthermore, China has made the leadership in the semiconductor industry a national strategic objective. According to the US based Semiconductor Industry Association, China has plans to invest more than $150 Billion in the sector between 2014 and 2030.

The U.S. government responded in 2022 with the Creating Helpful Incentives to Produce Semiconductors Act (CHIPS), which authorized $280 Billion to boost domestic research and manufacturing in the semiconductor industry in the US. In addition to this substantial amount of funding, the CHIPS Act also authorized Department of Commerce (DOC), Department of Defense (DoD), and Department of State (DOS) the authority to waive certain regulations to expedite the development of onshore domestic manufacturing of semiconductors critical to U.S. competitiveness and national security. The Act also includes safeguards to ensure that companies that receive Federal funds from the Act cannot use those funds to build advanced semiconductor production facilities in countries that present a national security threat to the US. When announcing the Act, congress noted that only 12% of chips are currently manufactured domestically, compared to 37% in the 1990s.

Other specific provisions of the Act included:

- $39 billion in immediate financial assistance to build, expand, or modernize domestic facilities and equipment for semiconductor fabrication
- $11 billion for DOC research and development.
- $2 billion for the DoD to implement the Microelectronics Commons, a national network for onshore, university-based prototyping, lab-to-fab transition of semiconductor technologies
- Waivers of certain environmental and other regulatory requirements necessary to construct and operate new semiconductor fabrication facilities

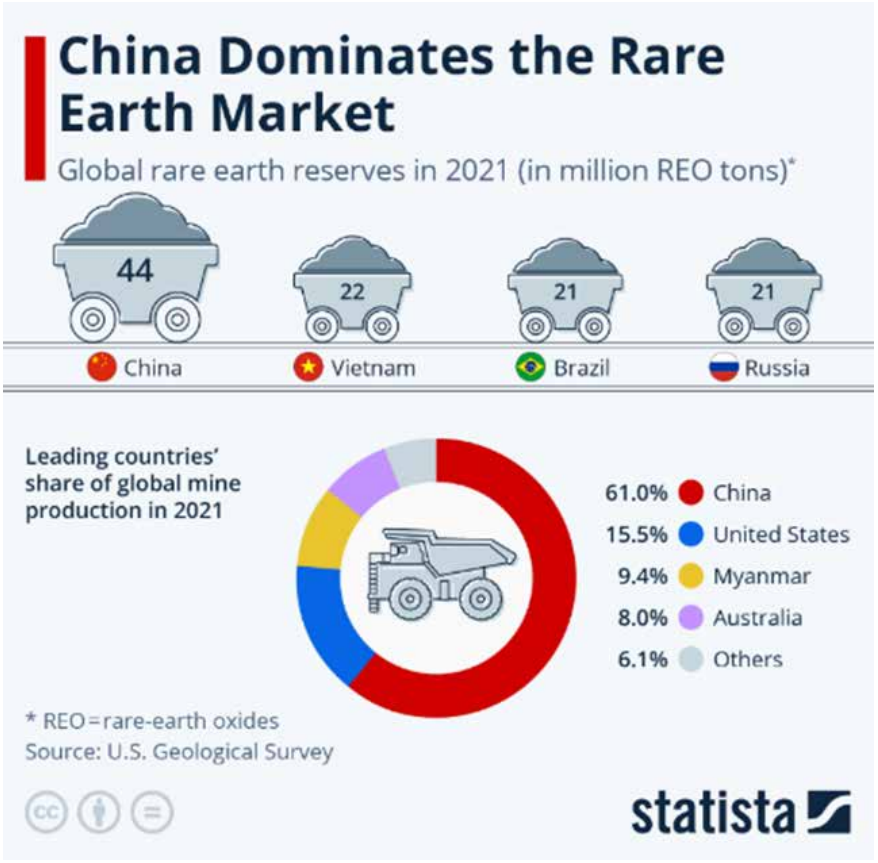
Skilled Labor

While supplies of REEs and

advanced semiconductors are crucial to the USDIB, a skilled workforce in manufacturing remains the most essential component of the defense supply chain. The USDIB is experiencing a severe shortage of qualified manufacturing professionals, from engineers to machinists. Several factors contribute to this challenge, including an aging workforce and insufficient training pipelines for specialized defense roles. This talent gap not only hampers production schedules but also slows innovation.

Today, the manufacturing sector is not a top choice for the newest generation of workers. Just 14% of Gen Zers say they would consider a career in manufacturing, because of expectations of: low pay and dangerous work conditions. Their disinterest has resulted in a rapidly aging workforce. About 51% of manufacturing jobs are held by employees ages 45-65 or older (Clear Company, manufacturing-workforce-trends-development-strategies, 2025).

There are some near-term solutions to this problem. Employers can establish apprenticeship programs in collaboration with local technical schools to build a pipeline of future talent. These programs are increasingly recognized as critical for addressing the workforce shortages in defense manufacturing. The Department of Defense's Manufacturing Education and Workforce Development (M-EWD) Program, for instance, collaborates with industry stakeholders to create skilled professionals who are equipped to meet the demands of advanced manufacturing. This initiative focuses on bridging the gap



between educational systems and real-world manufacturing needs. Also, ensuring that workers are prepared for the technology-driven advancements in defense sectors such as artificial intelligence, robotics, and advanced materials. This proactive approach not only helps close the skills gap but also strengthens the pipeline of human capital for middle market defense companies by providing students with valuable, career-oriented training in high-demand fields. Employers can partner with higher education institutions to create specialized training initiatives tailored to defense sector needs. Such partnerships are essential for ensuring that the talent entering the defense industry has the precise skills required for the evolving technological landscape. The Aerospace Industries Association (AIA) plays a leading role in advocating for the development of specialized training, reskilling, and educational programs that align with the needs of the defense industry. By working with colleges and universities, defense companies can ensure that curricula are closely aligned with current and future technological demands, such as cybersecurity, artificial intelligence, and aerospace engineering. These initiatives also help cultivate a more adaptable workforce, equipped to handle the rapid pace of innovation in the sector.

Weapons Manufacturing Capacity

In 2024, the Center for Strategic & International Studies (CSIS) reported that China's defense industrial base is operating on a wartime footing, while the U.S. defense industrial base is largely operating on a peacetime footing. The report went on to state that "the U.S. defense

industrial ecosystem lacks the capacity, responsiveness, flexibility, and surge capability to meet the U.S. military's production and warfighting needs." Unless there are urgent changes, the United States risks weakening deterrence and undermining its warfighting capabilities. China is heavily investing in munitions and acquiring high-end weapons systems and equipment five to six times faster than the United States. China is also the world's largest shipbuilder and has a shipbuilding capacity that is roughly 200 times larger than the United States. According to the CSIS 2024 report, China's largest shipyard, Jiangnan, has more capacity than all U.S. shipyards combined.

While the pandemic was not the only cause of this problem, it was certainly a catalyst. Lockdowns and business closures set off supply chain disruptions that led to a 43% decline in all US manufacturing output and a 38% drop in hours worked, the largest since World War II, and manufacturers were forced to lay off their employees. Some of the 1.4 million workers across all sectors, who lost their jobs left permanently, whether they retired early, began working in a different industry, or left the workforce for other reasons.

In the years since, US manufacturing has had an impressive recovery. The industry has added nearly 800,000 jobs since 2021. According to the National Association of Manufacturers (NAM) Manufacturers' Outlook Survey, companies' optimism about their future is rising. Even with growth, manufacturing still anticipates a long struggle with the talent shortage. Despite the addition of so many jobs, almost 550,000 are currently vacant, and research from Deloitte and The Manufacturing Institute indicates that this number will increase. An estimated four million manufacturing employees will be needed by 2030 in the US.

What This Means for Middle-Market Defense Contractors

From our vantage point as M&A bankers in the middle market of the aerospace & defense industry, we have a unique view. We can see what is happening in real-time in the supply chain. We hear from the owners of these companies - what keeps them up at night. And we hear from the buyers of these companies - what opportunities they see and why they are making substantial investments.

The Risks

There are three risks facing the middle market of the USDIB that we keep hearing:

- First, China is the biggest single threat to the US, not just terms of the risk of kinetic attack, but moreover in terms of non-kinetic warfare, including but not limited to the disruption of critical supply chains.

- Second, behind 'China Risk', is the risk of an aging USDIB manufacturing workforce

- Third, is the lack of investment into USDIB manufacturing infrastructure for decades

The Opportunity

While the risks facing the USDIB are substantial, the opportunity facing the middle market of the USDIB is even greater. Today, we are hearing repeatedly and loudly, especially from active buyers in the sector, the following:

- Manufacturing throughout the USDIB will experience a significant resurgence over the next 3-5 years, in terms of demand from the Department of Defense, the influx of new workers, and the flow of investment capital.

Improve Security Resilience with Radar

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

EchoGuard®

EchoShield®

Radar for Critical Infrastructure Protection

ECHODYNE

RADAR REINVENTED™

Predicting When the Predictable Will Happen:

Heathrow Airport Outage

The huge disruption at Heathrow Airport in March is the perfect exemplar of how exposed we all are to any major incident that effects critical infrastructure, not just nationally but internationally. Travel consultant Paul Charles told Reuters that the disruption could cost an estimated £20 million ($26 million) for each day, but could be much more!

The power outage was caused by a fire at a single electricity sub-station.

We've all seen them, sub-stations sitting in the middle of an urban sprawl with not much more than a chain link fence topped with barbed wire to protect them.

Commentators have been predicting an incident like this for years. But who would have predicted that it would have happened to Heathrow, Europe's busiest airport, one right at the top of the UK's governments critical infrastructure priorities. The vulnerability of critical infrastructure to outages at substations has been so well signposted for so long, that it seems inconceivable that a CNI site as important and high profile as Britain's number one international airport, would not have resilience built on resilience built on resilience!

The initial problem was a transformer on fire at the North Hyde 275kV substation, causing a power outage. But this failure alone should not have been catastrophic, however it was then further compounded by a failure in a power distribution unit at the airport, which is essential for managing the electricity supply throughout the site. This failure disrupted the power supply to various terminals and operations. Airport staff were quickly able to assess the situation and restore power and engage backup systems, but they were not sufficient to manage the full load required for operations. This resulted in the complete closure of the airport and disruption worldwide.

Heathrow's management have since announced plans for infrastructure upgrades to enhance the reliability of power systems. This included exploring more robust backup power solutions and redundancy measures to ensure critical operations remain unaffected during outages in future.

But in the immediate aftermath of the substation fire, resilience experts told New Civil Engineer magazine that critical national infrastructure (CNI) managers need to consider previously "unthinkable" risks.

For more precise details on what went wrong at Heathrow we must await the National Energy System Operator (Neso) report, due out very soon. But whatever the report says about Heathrow, CNI managers everywhere should take this as a salutary lesson and already be doing a deep dive into their systems and their dependencies, looking for those as yet unknown 'single points of failure' that could lead to their own 'Heathrow embarrassment' or worse!

Power outage in Iberian Peninsular

The widespread power outage that struck Spain and Portugal on Monday, April 28, 2025, is still under scrutiny to determine its exact origins. Around midday, Spain experienced a rapid loss of approximately 15 gigawatts of electricity, a substantial 60% of the national demand, within mere seconds. Portugal was similarly affected by extensive power disruptions.

Several potential causes are currently under investigation. Portugal's grid operator, REN, initially proposed that extreme temperature fluctuations in inland Spain created unusual oscillations in very high voltage (400 kV) lines, a phenomenon they termed "induced atmospheric vibration." Their theory suggests these oscillations led to a failure in synchronization between the electrical systems, triggering cascading failures across the interconnected European network.

In Spain, the grid operator, Red Eléctrica de España (REE), reported two rapid and significant "disconnection events." While the system recovered from the first, the second proved more damaging, causing interruptions originating from France's electrical system and a "massive, temporary disconnection." They also noted a "very strong oscillation in the electrical network." A technical malfunction within the high-voltage transmission lines or at a major substation remains a possibility as the initial trigger.

Although authorities and grid operators initially downplayed the idea of a cyberattack, the Spanish High Court has since mandated a preliminary investigation into this as a potential act of terrorism. Despite some initial speculation is the high proportion of renewable energy sources in Spain's grid as the primary cause, whilst some experts suggest that the outage might have been the result of a confluence of several minor issues interacting and escalating across the interconnected grid.

Crucially, the precise sequence of events leading to the initial failure is still unknown, and the specific nature of the "atmospheric phenomenon" and its impact on the high-voltage lines requires further verification. The exact cause of the grid instability and the disconnection from the French network also remains under investigation. The European Union Agency for Cybersecurity (ENISA) initially suggested a cable fault as a possible factor. Both the Spanish and Portuguese governments have launched investigations and are collaborating with grid operators to pinpoint the root cause and implement measures to prevent future occurrences.

A definitive explanation is anticipated following a comprehensive analysis of grid data, a process that could extend over several weeks or months.

Whatever the actual cause of the mass outage, it resulted in significant chaos, including grounded flights and substantial airport delays, the shutdown of metro systems and train services leaving tens of thousands stranded, disruptions to mobile and internet services, non-operational ATMs and payment systems, traffic lights failing and causing road congestion, and the cancellation of many events, emphasising the need for greater resilience in our power networks, a diverse range of sources of power and greater cooperation between agencies and operators to ensure risk is reduced any future mass outage, and better contingencies are in place as a result of this failure.

Unlocking the Potential of Public-Private Partnerships for Enhanced Security

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

Public-Private Partnerships (PPPs) are essential in enhancing security across various environments, including critical infrastructure. In its new White Paper, CoESS, the European Private Security Employers' Representation, demonstrates how collaboration between Law Enforcement Agencies (LEAs) and Private Security Companies (PSCs) can strengthen overall security and societal resilience. The paper draws on theoretical sources and showcases best practices to highlight the benefits of PPPs but also describe the challenges that hinder their effectiveness. It offers recommendations for all stakeholders involved to overcome barriers, implement key success criteria and optimise the potential of PPPs. The White Paper is jointly published by CoESS and its Dutch member, Nederlandse Veiligheidsbranche, with the support of the International Security Ligue.

The White Paper was officially launched at the European Security Summit, on 10 October 2024 in The Hague.

This article outlines the key takeaways from the White Paper, which will drive the policy and advocacy actions of CoESS, among others when contributing to EU policies such as the Preparedness Union and the Internal Security Strategy.

An Opportunity for Complementarity and Increased Efficiency

Public-Private Partnerships considered in this paper are all forms of cooperation between LEAs and PSCs. As such, they combine the strengths and resources of public security forces with the specialized capabilities of private security companies. This collaboration addresses complex security challenges efficiently, ensuring a comprehensive approach to the protection of people, assets and infrastructure, and thus society as a whole. The synergy allows for an extended security reach, leverages advanced technologies, and enhances the strategic allocation of resources across the security spectrum.

Significance and Impact

PPPs are shown to optimize the use of resources, allowing LEAs to focus on their core tasks while PSCs address the prevention and detection dimensions. The partnerships enhance operational capabilities, provide scalability in response to changing security demands, and introduce innovative solutions to security management. This strategic collaboration leads to improved flexibility in operations and a proactive stance in security planning.

Highlights

Surprisingly, PPPs are legally possible in only 9 out of 27 EU Member States and mostly in Western European countries, where they cover different realities. While some Member States have advanced partnerships based on formal frameworks, others are informal, local and temporary. The type of protected objects and events also vary, as do the missions that are given to the PSCs.

There is a correlation between the level of professionalism of the industry, the maturity of the legal framework, and the depth of cooperation between LEAs and PSCs. The White Paper describes the advantages in operating PPPs, including:

• Resource Efficiency: Private companies support LEAs by handling preventive and surveillance tasks, freeing up public resources for LEAs to concentrate on their core missions.

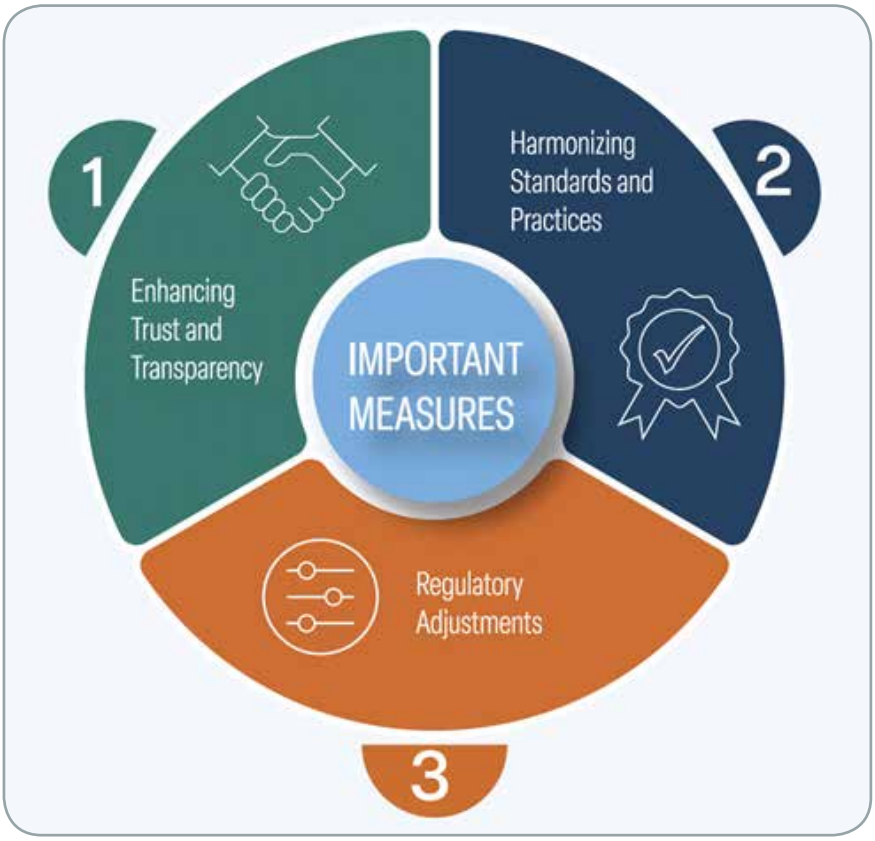
• Advanced Specialization: PPPs bring state of-the-art technology and specialized skills, particularly valuable in areas in which they have developed particular know-how, such as access control, distance surveillance and monitoring, protecting certain infrastructure (critical and others), etc.

• Strategic Flexibility: The ability to dynamically scale security measures in response to situational analyses enhances both proactive and reactive capabilities.

Implications for the Security Landscape

The increased complexity and diversity of threats require a shift towards a more integrated and responsive security framework. This approach not only improves immediate responses to threats but also supports a sustained security strategy that adapts to future challenges. The implications extend beyond immediate security enhancements, suggesting long-term benefits in public safety and trust.

Challenges and Strategies for Overcoming Obstacles in PPPs



While Public-Private Partnerships offer substantial benefits, they also face specific challenges that can hinder their effectiveness. Key obstacles include issues of trust and information sharing, differing operational cultures between public and private entities, and regulatory constraints that can stifle collaborative efforts.

To overcome these challenges, the White Paper recommends several measures, of which the following are particularly important:

1. Enhancing Trust and Transparency: Building trust is fundamental. Initiatives such as joint training sessions, shared operational planning, and regular stakeholder meetings can foster a mutual understanding and strengthen trust. Clear communication and transparency in operations and decision-making processes are crucial for developing a reliable partnership.

2. Harmonizing Standards and Practices: Developing common standards and practices across public and private sectors within PPPs can alleviate cultural and operational discrepancies. Areas to look into may include training, security protocols, data interoperability, vulnerability assessments and complementarity in response strategies to optimise cooperation.

3. Regulatory Adjustments: Modifying existing laws and regulations to support PPP frameworks and allow for the exchange of information between PSCs and LEAs is essential. Legislation should support best value procurement, collaborative actions and facilitate rather than inhibit information sharing, ensuring that both public and private entities operate under a supportive legal framework that will help reinforce mutual trust and promote cooperation. Finally, legislation should also provide that LEAs have a good understanding of what PSCs can and can't do. This could be included in basic LEA staff training.

By addressing these challenges through targeted strategies, PPPs can not only enhance their operational effectiveness but also achieve a more resilient and adaptive security infrastructure. These efforts require ongoing commitment and adaptation from all stakeholders involved to ensure the continued success and evolution of PPPs in the security sector.

In conclusion, Public-Private Partnerships are indispensable in the modern security apparatus. By effectively combining the unique strengths of LEAs and PSCs, PPPs not only enhance current security measures but also prepare organizations for emerging threats. This White Paper supports the continued development and refinement of PPP frameworks to maximize their positive impact on public security.

About the Author:

Catherine Piana is the Director General of both CoESS and the Aviation Security Services Association – international (in short ASSA-i) and the co-owner and Managing Director of the internationally acclaimed e-learning platform on the Insider Threat, Help2Protect.

The White Paper can be downloaded free of charge at https://coess.org.

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

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

for the international border management and security industry

Co-hosted by:

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

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

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

Supported by:

European Association of Airport and Seaport Police

Media Partners:

Border Security Report

World Security-index.com

An Interview with the Association of American Railroads (AAR)

Operating over a private, 140,000-mile network stretching across the far reaches of North America, AAR members include the major freight railroads in the United States, Canada and Mexico, as well as Amtrak. Working with elected officials and leaders in Washington, D.C. on critical transportation and related issues, AAR ensures that the freight rail industry will continue to meet America's transportation needs today and tomorrow.

Ben Lane, CIPRNA event manager, met Janet St. John, Director Cyber Security at Association of American Railroads (AAR).

Ben Lane (BL): Janet, thanks for joining us today and we're pleased to announce you're going to be joining us in CIPRNA in Houston (March 11-13) as one of our speakers on the Transport Sector Symposium: https://ciprna-expo.com/session/transport-sector-symposium/

We are very much looking forward to seeing you there. Let's start off with a quick question about you, and your career to date.

Janet St. John (JSJ): I really appreciate the opportunity to speak to you, and I'm also very much looking forward to the speaking engagement in Houston. I'm the director of cybersecurity at the Association of American Railroads. I have worked in the transportation sector, focused on both physical and cybersecurity for going on 25 years.

I started out as a geographic information systems crime analyst and then made my way to working within transportation, and the highway sector. And then working

with the information sharing and analysis centers that we have through our National Council of ISACs. And then I made my way to the AAR, where I have been employed as their director for around six years.

I get to work with some fantastic people. I manage one of the committees through the AAR, which is the Rail Information Security Committee, that is comprised of our CISOs and their senior leadership within their information technology and OT departments. We get together bi-weekly to discuss cybersecurity issues, whether it be the threat actors that we're monitoring or best practices, but there's collaboration and cooperation in keeping our industry safe from cyber threats that I'm going to be very happy to talk about in Houston.

BL: A key point of the conference is to bring parties together, particularly with the incidents we talked about earlier about the horrific air incident in America (January 29, 2025). It's at times like this that collaboration and cooperation come to the front, even more so. We're thinking about everyone involved in that horrific incident and our condolences go out to everyone.

Where and what does the AAR see as the challenges for security on the railroads and in terms of resilience? What are the main challenges you are seeing?

JSJ: Well, right now with a change in administration there have been challenges impacting on what I think is a very, very important component, which is our public-private partnerships that we have worked on and put together for

decades now. Since 9/11, there has been a lot of collaboration and a lot of trust built between the critical infrastructure, key resource community, and with DHS, Department of Homeland Security, and Federal Bureau of Investigation.

These components have worked very hard to build up this trust that allows for a robust information sharing collaboration, and we're worried about where this is going to go, and that is one of our concerns. As far as the industry is concerned, we have a very robust security program that we manage through the AAR, that consists of not just our members of the Class 1 railroads, but Amtrak, our passenger rail and regional railroads, and also our short lines and regional railroads through the American Short Line and Regional Railroad Association.

And within the security program, we have the rail security working committee, which is our DHS liaisons, our law enforcement, and the focus there is on physical security within the railroads. They have been around for over 20 years. And within those committees we have a broader security program that is managed with an overall industry-wide security plan.

We also operate a common operating environment where we can share security information, not just within the rail industry, railroad to railroad, but also with our government partners. And that's one of the things that we have worked on and that we want to see continue and to grow, is that collaboration with our government partners. So, we focus on areas of where the threat is, what are our vulnerabilities, what is the risk, and we assess our risk all the time through the AAR and through these committees.

BL: Yes, and "collaboration" was a key word I took out from that. And again, we're back on that idea of collaboration and without that or without effective collaboration, the system won't work.

You have a large area to cover and different environments across this area. How is this managed from an economic point of view?

JSJ: First, railroads are mindful of all antitrust laws when it comes to information that could create a competitive advantage, and we

begin each meeting of the Rail Information Security Committee with a statement of our obligations under those laws. When it comes to cyber threat information sharing to enhance security, the public has a vested interest in railroad collaboration across carriers to share best practices and evolving threats.

Collaboration is important because freight trains move across the country, and may travel across lines owned by different railroads between origin and destination. So a train that is owned and operated by Norfolk Southern, for example, may use track that is owned by BNSF and vice versa. And then we have Amtrak that shares some of those tracks as well. So, there's certain collaboration and cross-pollination involved in being able to get goods from point A to point B.

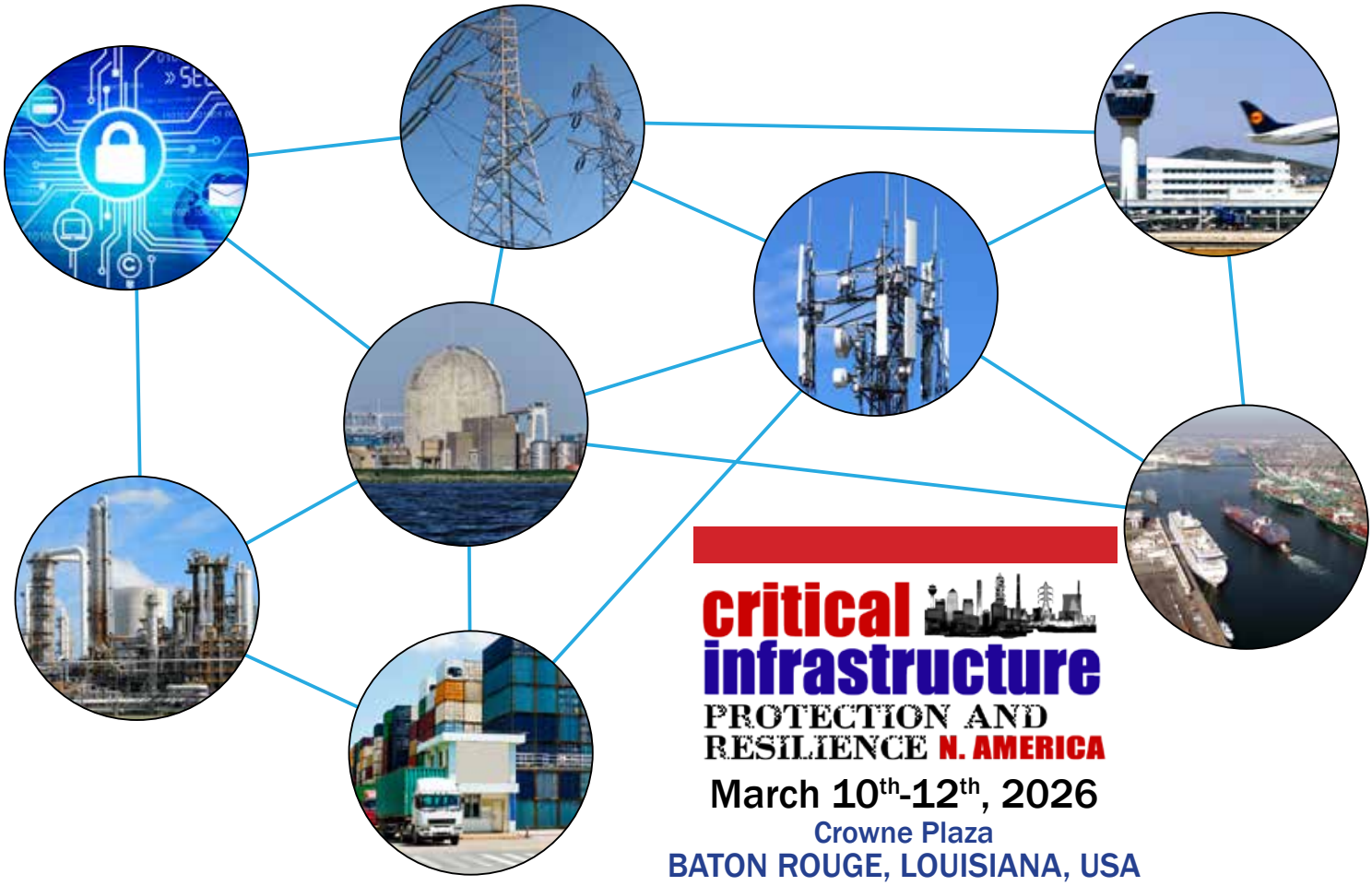
As far as our economic impact, we're very important to the supply chain in the United States and in Canada and Mexico. There are a lot of commodities that railroads transport that other modes of transportation cannot or have a very limited space in that area. We are also a military transport of personnel and equipment. Therefore, there is a lot of focus on the railroad industry for our economic importance to the United States, our consumers, our citizens, and our role that we play in national security.

BL: One question I would like to add, just to get a bit of personal insight. What keeps you awake at night?

JSJ: Railroads understand and take seriously our responsibility to our people and the communities we serve. One thing that we don't want to see is the aviation accident that happened last night (January 29, 2025) here in Washington, DC where many people perished. It's those type of accidents that keep us up at night. We are also concerned with and keep monitoring a lot of the geopolitical aspects, because in some ways those do impact our security, whether it be the protests that might spill over into or onto our railroad tracks or within the ports against military shipments. So geopolitical events have an impact on all critical infrastructure and so that is something that we are very keen to keep an eye on.

BL: Thank you so much and we look forward to seeing you in Houston giving your talk at our Transport Sector Symposium.

JSJ: Thank you. I look forward to the opportunity.



critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 10th-12th, 2026

Crowne Plaza

BATON ROUGE, LOUISIANA, USA

A Homeland Security Event

CALL FOR PAPERS

Securing the Inter-Connected Society

Abstract submittal deadline - 30th June 2025

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 8th 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**

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

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

ISIO

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Rapid Reconnaissance Surveillance for Energy Infrastructure: A new era of energy site security

Energy infrastructure faces an evolving and increasingly complex threat landscape. From theft and vandalism to cybersecurity breaches and physical attacks, energy sites are frequent targets due to their critical role in national infrastructure. In fact, in 2023, the U.S. Department of Energy reports at least 175 instances of physical attacks or threats against critical grid infrastructure.

These sites are often located in remote or expansive areas, making security coverage a significant challenge. As such, traditional security methods—such as fixed surveillance cameras and human patrols—are proving insufficient. Fixed cameras offer only limited visibility, are susceptible to tampering, and require constant monitoring, while human patrols are expensive, reactive, and difficult to scale across large or remote energy sites.

New advancements in modular, mobile, and intelligent surveillance are transforming the way energy companies monitor and protect their assets. With new tools, like AI-driven detection, radar-based tracking, autonomous drone surveillance, and remote real-time monitoring, sites are able to take a 'set and forget' approach to proactive security, while reducing operational costs, improving resilience, and ensuring continuous protection.

The True Cost of Energy Infrastructure Security

Securing an energy site requires careful consideration of both direct and indirect costs. The financial impact of security decisions can be substantial, and companies must weigh upfront investments against long-term operational savings.

When evaluating security options, you'll need to consider what will best meet your needs and the associated costs. For example, traditional surveillance systems require significant investment in fixed camera infrastructure, while modular mobile solutions adapt to site conditions and offer less costly deployment options. In addition to set up costs, there are costs associated with keeping your systems operating. When deploying teams to manually investigate incidents, you'll need to account for travel costs, labor expenses, and delayed response times. Meanwhile, real-time remote monitoring allows for immediate assessment and intervention, minimizing costs and optimizing resource allocation.

While properly securing a site can be costly, not securing your site can have severe consequences. Business disruptions caused by theft, vandalism, or sabotage can result in power outages, equipment failure, and lost revenue. Moreover, regulatory non-compliance could result in fines and penalties under industry regulations, like NERP CIP. And in the event of a breach, sites with inadequate insurance and liability coverage face higher premiums and potential lawsuits.

By investing in proactive security, including next-gen, autonomous surveillance companies save time, money, and resources by preventing costly incidents before

they escalate. These investments can mitigate risks, reduce operational costs, and ensure compliance while maintaining uninterrupted service.

A Convergence of Technologies: Smarter, Faster, More Effective

Modern surveillance has given rise to a multi-layered defense system that leverages cutting-edge technology to detect, analyze, and respond to threats faster and more efficiently than ever before. Recent advances in AI, thermal imaging, radar, and drone detection are revolutionizing security capabilities, providing a more accurate, automated, and adaptable approach to energy site security.

What sets modern surveillance apart is its ability to integrate various technologies into a single system. Security is no longer just about cameras— modern surveillance is an integrated ecosystem that provides real-time intelligence, proactive threat detection, and operational efficiency. These systems operate autonomously, minimizing the need for human intervention and reducing reliance on security personnel. Today's systems are highly mobile and easily deployed, making them easier to use in remote locations. And with the advent of AI-driven detection and response, there is greater accuracy, which reduces false alarms and enables swift response to incidents.

Radar and AI are both technologies, beyond cameras, that you should be exploring to improve your surveillance. Radar and AI-driven analytics enhance security capabilities by offering wide-area detection, multi-sensor

integration, and real-time threat assessment. Unlike traditional cameras, radar can detect movement at long distances regardless of weather or lighting conditions, while AI minimizes false positives and optimizes response times. This combination results in a more effective and reliable security solution.

Features That Make a Difference

Modern surveillance solutions integrate multiple technologies, such as drone detection, thermal imaging, and radar, to provide comprehensive security for energy infrastructure. By combining these tools with AI-driven analytics, real-time monitoring, and autonomous response capabilities, these systems enhance situational awareness and reduce human intervention. They proactively detect, assess, and neutralize threats before they escalate, ensuring a robust, scalable defense for critical assets.

These different technologies enhance security solutions by offering new capabilities to enhance detection, eliminate blind spots, and provide continuous protection. Drone detection and mitigation can be used to prevent unauthorized aerial threats that could compromise security. Thermal imaging detects intrusions in total darkness, fog, or extreme weather conditions. Meanwhile, radar-based motion detection covers large areas (150m–1km) with high accuracy in all weather conditions, minimizing blind spots. Secure cloud connectivity enables real-time, remote monitoring, allowing security teams to react instantly. Furthermore, these systems are designed to withstand extreme weather, ensuring continuous operation in remote or volatile environments.

All of these features offer great benefits, but the best fit depends on your site. High-risk areas may require radar and AI-driven analytics to detect unauthorized movement and reduce false alarms. While more remote sites could benefit from thermal imaging and cloud connectivity for uninterrupted monitoring. Critical assets, such as substations, may need additional protection, like ballistic protection and drone detection, to prevent sabotage.

Compliance & Future-Proofing

Energy Security

Regulatory bodies such as NERC CIP and FERC impose strict security standards on energy infrastructure to mitigate risks associated with cyber and physical threats. Compliance is no longer optional—it is an operational necessity.

Energy companies that fail to meet these standards face significant financial and reputational damage. The financial impact alone can include penalties ranging from thousands to millions of dollars. Operational downtime from non-compliance can lead to forced shutdowns or restrictions, impacting grid stability and profitability. Additionally, lax security measures expose systems to cyberattacks, leading to data breaches and infrastructure vulnerabilities.

To avoid these types of damages, companies need to invest proactively in their security systems to ensure compliance. Modular surveillance solutions offer a viable way to minimize risk exposure by providing continuous monitoring, ensuring compliance with security mandates, all while seamlessly integrating into existing infrastructure. Additionally, automating compliance monitoring using AI-powered analytic reduces human error and streamlining audits.

Investing in the right technology today prevents costly compliance headaches tomorrow, ensuring seamless adherence to regulatory standards while enhancing operational security.

Security Without Compromise

Energy companies are under increasing pressure to safeguard critical infrastructure from both

physical and operational threats. Traditional security solutions often fall short in providing the necessary coverage, efficiency, and cost-effectiveness required to protect these high-value assets, and technological advances (drone technology, for example) underscore the need for high-tech, strategic surveillance.

Rapid Reconnaissance Surveillance solutions offer a smarter, more adaptable approach by integrating AI-driven analytics, modular mobility, and real-time threat detection into a single, scalable system. With features such as drone detection, radar-based motion tracking, and extreme weather resilience, these solutions provide unmatched intelligence, automation, and ease of use for energy security teams.

By implementing modular, AI-powered surveillance, energy companies can minimize operational burdens, enhance compliance efforts, reduce financial risk, and ensure 24/7 protection for remote or high-risk locations – all while maximizing protection and minimizing cost and oversight.

NETSCOUT Reports DDoS Attacks Targeting Critical Infrastructure Play a Dominant Role in Geopolitical Conflicts

NETSCOUT Systems has released its 2H2024 DDoS Threat Intelligence Report, revealing how Distributed Denial of Service (DDoS) attacks have become a dominant means of waging cyberwarfare linked to sociopolitical events such as elections, civil protests, and policy disputes. The findings show how attackers exploit moments of national vulnerability to amplify chaos and erode trust in institutions, as they target the critical infrastructure of governments, commercial entities and service providers.

Throughout the year, DDoS attacks were intricately tied to social/political events, including Israel experiencing a 2,844% surge tied to hostage rescues and political conflicts, Georgia enduring a 1,489% increase during the lead-up to the passage of the "Russia Bill," Mexico having a 218% increase during national elections, and the United Kingdom experiencing a 152% increase on the day the Labour Party resumed session in Parliament.

"DDoS has emerged as the go-to tool for cyberwarfare," stated Richard Hummel, director, threat intelligence, NETSCOUT. "NoName057(16) continues to be the leading actor for politically motivated DDoS campaigns targeting governments, infrastructure, and organizations. In 2024, they repeatedly targeted government services in the United Kingdom, Belgium, and Spain."

AI and Automation Drive Scale and Impact

DDoS-for-hire services have become more powerful using AI for CAPTCHA bypassing, with about nine in ten platforms now offering this capability. Additionally, many employ automation to enable dynamic, multi-target campaigns and offer infrastructure exploitation techniques such as carpet bombing, geo-spoofing, and IPv6 to expand attack surfaces. Even the most novice operators can launch significant DDoS attack campaigns causing substantial harm.

DDoS attacks are evolving and adapting faster than ever, creating a challenge for defenders and those entrusted with protecting critical infrastructure networks and service availability. Enterprises, government organizations, and service providers are all targets for DDoS attacks.

CLOSING COMMENTS FROM CRITICAL INFRASTRUCTURE PROTECTION & RESILIENCE NORTH AMERICA (CIPRNA)

11th-13th March 2025, Houston, TX

The Critical Infrastructure Protection and Resilience North America Conference took place in Houston in March 2025. It was a timely event with both a new political administration in place in the Untitled States and the uncertainties around the processes being delivered through the work of the Department of Government Efficiency -DOGE.

The conference was a great event attracting representation from across all relevant Government Agencies, Industry, Operators and Academia, alongside over 300 delegates and 30 plus exhibitors. It was Chaired by John Donlon QPM FSyI and detailed below are his closing comments reflecting on the success of CIPRNA 2025.

It has been a great pleasure to be able to bring CIPRNA to Houston Texas for the first time and fantastic that the conference has coincided with the Rodeo taking place in the city. I am told that this is the largest Rodeo in the world. Then again, I am also told everything is bigger in Texas than anywhere else.

Events such as these provide a fantastic opportunity to network with like-minded friends and colleagues and I always go away having learned something new and worthwhile and I do hope you have found the last few days to have been informative, enjoyable and of real value.

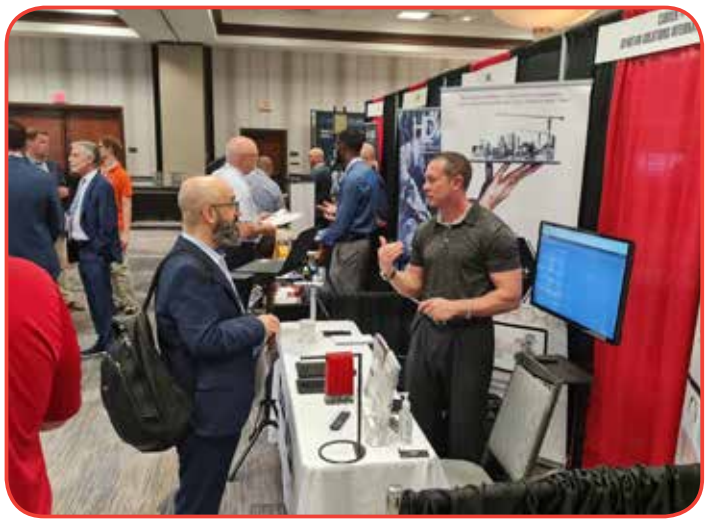
We have had some insightful presentations by some very distinguished and experienced professionals and some great discussions across a whole range of issues which are affecting the international infrastructure and information communities.

We are extremely grateful to all the people and the organisations who have supported us and shared their knowledge, expertise and enthusiasm with us. In particular, I need to thank InfraGard Houston and their President, Marco Ayala and Jeremy Hansen from the Cybersecurity & Infrastructure Security Agency-CISA.

We are also grateful to our exhibitors and sponsors without whom it would be almost impossible to deliver events such as this.

We had a great start on Tuesday afternoon with the keynote session being led by Chief Larry Satterwhite, the Director of Public Safety and Homeland Security here in Houston. Chief Satterwhite welcomed us all to the city and provided an overview of the complexities around the protection and resilience of infrastructure within Houston. He had a clear message on the necessity of constant planning and the enormous benefits of developing and maintaining effective partnerships.

Chief Satterwhite spoke of the need to make effective use of new and emerging technologies, stating that we all need the 'New Widgets' to help us going forward but not on their own, it always comes back to people and people working together.



In fact, the theme of collaboration and partnerships continued throughout the conference being a constant item of discussion and this was reflected through our final session this afternoon. There is little doubt that everyone realises the need for greater levels of cooperation together with the enhancement of Public Private Partnerships. However, it is also recognised that it is a 'tough nut to crack' and requires significant continuous effort and the building of trust. One presenter put it posed it quite succinctly when he said, "Some people need a wake-up call to the effort required but the trouble is too many people hit the Snooze Button".

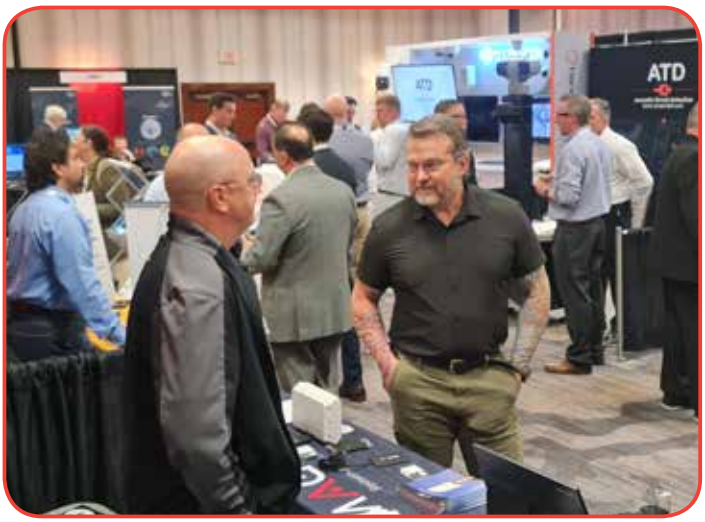
The Plenary Session later on Tuesday afternoon was led by Paul Titus the Director of Critical Infrastructure Security and Resilience from Idaho National Laboratory. Paul together with a very knowledgeable panel examined NSM-22 the National Security Memorandum which updates national policy on how the U.S. government protects and secures critical infrastructure from cyber and all-hazard threats.

This was a very lively and interactive session delving into how the risk landscape has changed over the past decade and emphasising how NSM-22 prioritises collaborating with partners to identify and mitigate sector, cross sector and nationally significant risk. We even, at one point, had Paul inviting one of his staff members in the audience to demonstrate his skills at 'interpretive dance'. Unfortunately, this didn't happen!

So, over the three days we have covered a whole range of topics which included:

- Emerging Threats
- Emergency Management
- Strategic Resilience Planning and Mitigation
- New Technologies and
- Innovation, Good Practice and Standards.

These themes were examined in some depth and were reflected across the Industry Sector Sessions on Oil & Gas, Maritime and



Ports, Food and Agriculture, Power and Energy Communications and Transport.

There was, as expected, a significant degree of focus on Cyber Security issues. State sponsored cyber-attacks drew a lot of attention with reference to both Russia and China having the International 'A' Teams followed by the level of concern also associated with Iran and North Korea.

Artificial Intelligence and Quantum Computing was very topical balancing out the potential as a force for good alongside the potential as a force for harm. However, no matter which side of the fence you sit on, it was reassuring to note the amount of national effort and innovation currently being put in place and also the practical support available to infrastructure owners and operators.

I was a little surprised that we did not hear more on extreme weather events given the experiences of Texas and surrounding States. We had some references to terrorism dotted throughout the conference but again not as much as I expected. The issue of Insider Threats was referred to on a couple of occasions and although not a major feature this year I think it will be in years to come.

What I was not surprised about was the number of new acronyms entering the world of the protection and resilience of our infrastructure. I make myself a promise each year before I Chair this event not to mention acronyms but you guys here in the USA are just so good at making them up that it would be remiss of me to not reflect on a few of the best new ones that I have heard during this conference.

We had:

TILOP – Texas Infrastructure Liaison Officer Programme

PSAC – Private Sector Advisory Centre

HSIN – Homeland Security Information Network - and

RATs – Recovery asset Teams

My favourite however, was;

TRAINS – Testing Risks of AI for National Security

I thought the United Kingdom were well skilled when it comes to putting a good acronym together but I have to say the USA are without doubt, world leaders. I can't wait to see what we hear next year at CIPRNA in Baton Rouge.

As with any good conference there is a great deal to be gained through the questions asked and discussions that follow and this was certainly the case here this week. As an audience you were both engaged and knowledgeable and didn't shy away from challenging our speakers nor did you miss the opportunity to follow up on issues during the coffee/lunch breaks.

As I said on day one, the world is an unpredictable place and is constantly and rapidly changing. The protection and resilience of our infrastructure and information requires us all to continually change, adapt and innovate and though events such as this we have the opportunity to:

- Learn something new
- To make new professional contacts who may be able to assist you in some way in the future – and importantly –
- To make new friends

Once again, I just want to thank our supporters, our exhibitors, our sponsors and of course all the great speakers for giving us their time and sharing their knowledge and expertise. But most of all I want to thank all of you for your attendance and your active participation which has made this conference such a worthwhile and great event.

Next year, as I said earlier, Critical Infrastructure Protection and Resilience North America will take place in Baton Rouge in March next year, the 12 to the 14th and our European event will be in Brindisi in Italy in October this year.

I hope to see some of you at one, if not both these events.

John Donlon QPM FSyL
Conference Chairman
Chairman, IACIPP

Bhutan: Protecting hydropower and water from climate and other risks

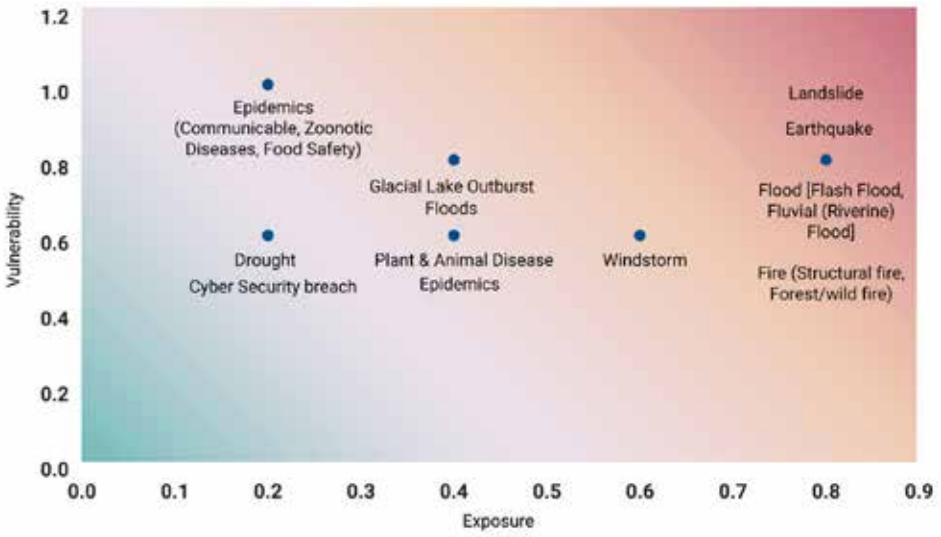
By UNDRR and CDRI

Nestled in the eastern Himalayas, Bhutan is a small, landlocked Buddhist kingdom bordered by India and China. Known for its monasteries, fortresses and dramatic scenery, its landscapes range from subtropical plains to steep mountains and valleys. One of its mountains, Gangkhar Puensum, is the highest unclimbed mountain in the world.

This mountainous terrain brings both challenges and opportunities. The abundant water resources and limited population of less than one million, for example, means that the country's hydropower sector can generate enough electricity for almost 100 percent of its population, exporting the surplus to India. Combined with the revenues from tourism, Bhutan has been able to invest in its people, providing free education and healthcare, while reducing extreme poverty and promoting gender equality too.

On the other hand, Bhutan's geography - its scattered population, high altitudes, and narrow valleys - also complicates socio-economic development since it increases the country's

vulnerability to a range of risks such as floods, earthquakes, landslides, and even droughts during the dry season. Since Bhutan relies on water for energy and agriculture, which are key sources of both revenue and employment, climate change will likely bring a range of more intense and frequent hazards.



Exposure and Vulnerability of Infrastructure Systems for Hazards

To reduce the risks of disaster damage to its infrastructure and continue its socioeconomic development, Bhutan joined Chile, Madagascar, and Tonga, as one of four countries pioneering the Global Methodology for Infrastructure Resilience Review [link once it's available]. Developed by the UN Office for Disaster Risk Reduction (UNDRR) and the Coalition for Disaster Resilient Infrastructure (CDRI), the methodology helps countries to identify and prioritize the strategies that will enhance the resilience of their infrastructure.

Using this process, Bhutan developed its National Plan for Infrastructure Resilience, outlining the key hazards for its infrastructure, as well as the necessary strategies and actions to mitigate disaster risk.

Advancing Infrastructure Resilience in Bhutan

Aligning with the five year plan

Bhutan's journey began by mapping the key stakeholders – including 21 agencies across seven ministries - and engaging with them in a series of workshops.

In steps two and three of the Global Methodology, Bhutan's policies and regulations were reviewed, then stakeholders analyzed the vulnerabilities across six key sectors – transport, energy, water, and information, communication, and technology (ICT), as well as health and

5 Steps of the Global Methodology for Infrastructure Resilience, UNDRR

education. The stakeholders focused on 10 key hazards.

In step four, stakeholders then evaluated Bhutan's infrastructure resilience against UNDRR's Principles for Resilient Infrastructure, which sets out the key conditions for sustainable infrastructure resilience. By complying with the six Principles for Resilient Infrastructure, Bhutan's infrastructure would support the Sendai Framework for Disaster Risk Reduction as well as the Sustainable Development Goals and G20 Principles for Investing in Quality Infrastructure.

In step five, an implementation plan is developed using information and analysis from the early steps. Stakeholders later validated this plan, the Bhutan National Plan for Infrastructure Resilience, via extensive consultation in order to ensure broad support and alignment with national policies, specifically Bhutan's 13th Five Year Plan, 2024-2029.

When stakeholders agreed to incorporate recommendations of the National Plan into their own sectoral plans, they were therefore also agreeing to support implementation of Bhutan's 13th Five Year Plan.

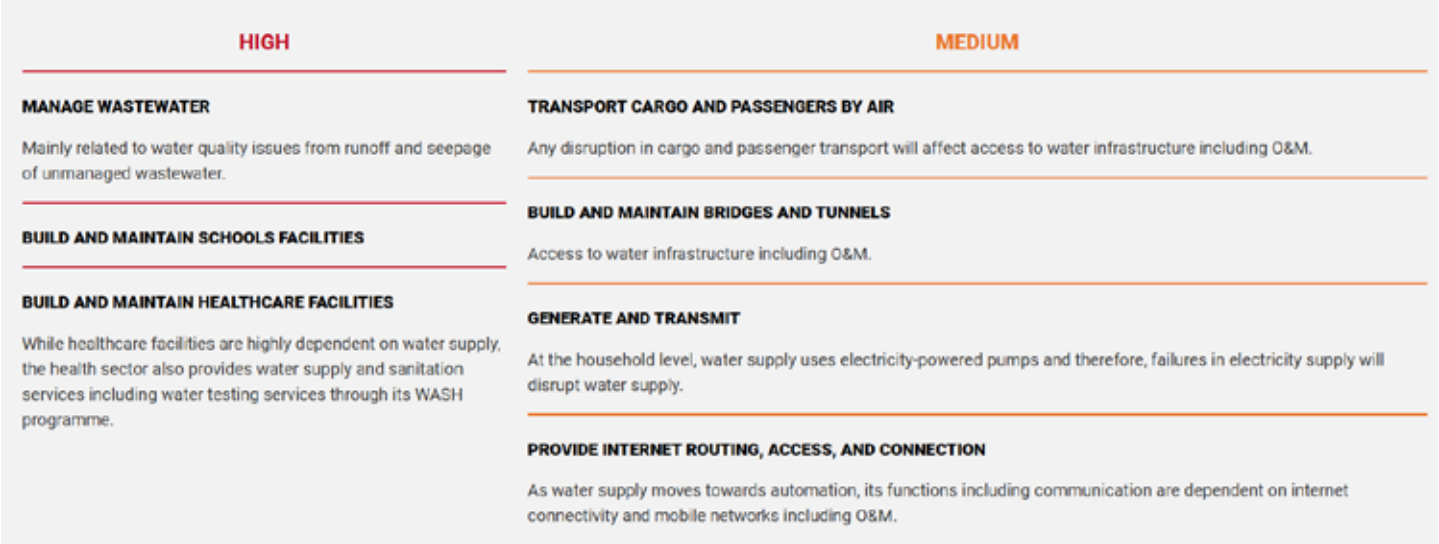
These recommendations and action plan were both cross-sectoral and sector-specific. One core recommendation, for example, was to build technical capacities for Geographic Information Systems (GIS), remote sensing surveying, and climate-resilient infrastructure design.

It was also recommended that a national database be developed in order to track critical infrastructure systems and performance, share key infrastructure data across sectors, and improve decision-making and infrastructure services continuity.

Protecting water from growing risks

The database may be especially valuable to the water sector – one of the key sectors examined – since managing Bhutan's water resources involves multiple agencies with challenging inter-agency coordination.

Bhutan receives abundant monsoon rains, but the steep terrain means that this water quickly drains away, generating significant water shortages during the dry months. The combination of expanded irrigation, urbanization, and water-dependent industries means that water scarcity and demand are



Water Supply Dependencies on Other Critical Functions

rising. The need to address these challenges has become an urgent issue.

Climate change is expected to place even further pressure on Bhutan's water resources by increasing the frequency and intensity of extreme weather events. The stress test analysis identified drought as the most significant risk to water supply, affecting households, agriculture, water-based industries, and public health. Other hazards, such as floods, glacial lake outburst floods (GLOF), earthquakes, landslides and waterborne epidemics, also present significant risks.

Meanwhile, the analysis further showed that Bhutan's water supply is vulnerable to cascading risks in the transport, electricity and ICT sectors, meaning that any disruptions to these functions could also impact the supply of water. In addition, a comprehensive assessment of the water sector was conducted, bringing together key water infrastructure stakeholders to discuss challenges and resilience needs.

To address these vulnerabilities, the National Plan recommended targeted solutions for Bhutan's risk management strategies in the water sector. Bhutan currently lacks a comprehensive understanding of its water resources, including the supply, quality, and condition of its water. To address this, the plan recommends a GIS-based inventory of the country's water and wastewater infrastructure. In addition, it suggests an assessment of the drying water sources as well as the creation of a plan to restore springs and take proactive measures to protect the sources at risk.

The National Plan also recommends that water and wastewater infrastructure should be made more resilient through targeted investments that account for climate risks, safety, and redundancy. The proposed activities include updating infrastructure standards to align with the ASCE (American Society of Civil Engineers) Risk Category IV or an equivalent national standard, accessing climate and development funds, and strengthening financial capacity to meet the requirements of operations and maintenance.

Building energy resilience

Water also plays a vital role in Bhutan's hydropower sector, which serves as the backbone of both its energy generation and exports.

Indeed, Bhutan's human and economic development is closely tied to the growth of its hydropower. Some 99.7 percent of households have access to electricity, which is also essential for hospitals, schools, and communication networks. Besides supporting domestic sectors, hydropower also enables industrial growth.

But Bhutan's hydropower sector faces increasing risks linked to the growing challenges to its water supply. Climate change is expected to exacerbate challenges such as droughts, glacial lake outburst floods (GLOFs), heavy rainfall, and flash floods. Additionally, Bhutan's seismic activity makes hydropower assets vulnerable to loss and damage.

The country's electricity transmission and distribution

and landslides, as well as from fires and flash floods. At the same time, this network itself is a potential fire hazard, which could endanger surrounding infrastructure, settlements and forests.

The Assessment identified several resilience measures, including some which are already well-advanced and which reflect a proactive approach to risk reduction. Bhutan is exploring example, to increase its water storage capacity.

However, the Assessment also highlighted several areas for improvement. It noted gaps in grid stability, real-time monitoring, and the ability to respond quickly to transmission and distribution outages. To address these challenges, the assessment recommended upgrades to safety standards and the introduction of mandatory risk reporting as a regulatory requirement for electricity transmission and distribution. Establishing feedback loops and mechanisms will also help to improve the network's resilience.

Next steps

With multiple recommendations in the National Plan, stakeholders from government, business, and the state-owned enterprises worked together to identify priority recommendations. Prioritization was based on national resilience objectives and specific sectoral needs that align with sector priorities outlined in the Five Year Plan.

Some stakeholders expressed their hope for the data platform to be successful and to expand it to include new sectors and new hazard risks as resources become available.

UK critical systems at increased risk from 'digital divide' created by AI threats

A new report, launched by Pat McFadden, the Chancellor of the Duchy of Lancaster at the National Cyber Security Centre's (NCSC) CYBERUK conference, outlines how artificial intelligence will impact the cyber threat from now to 2027, highlighting how AI will almost certainly continue to make elements of cyber intrusion operations more effective and efficient.

It warns that, by 2027, AI-enabled tools are set to enhance threat actors' ability to exploit known vulnerabilities, adding that whilst the time between the disclosure and exploitation has already shrunk to days, AI will almost certainly reduce this further, posing a challenge for network defenders.

The report also suggests that the growing incorporation of AI models and systems across the UK's technology base, particularly within critical national infrastructure and where there are insufficient cyber security controls, will almost certainly present an increased attack surface and opportunities for adversaries.

As AI technologies become more embedded in business operations, organisations are being urged to act decisively to strengthen cyber resilience and mitigate against AI-enabled cyber threats.

The integration of AI and connected systems into existing networks requires a renewed focus on fundamental security practices. The NCSC has published a range of advice and guidance to help organisations take action, including by using the Cyber Assessment Framework and 10 Steps to Cyber Security.

The report also highlights, in the rush to provide new AI models, developers will almost certainly prioritise the speed of developing systems over providing sufficient cyber security, increasing the threat from capable state-linked actors and cyber criminals.

Enable efficiency in O&G

Optimize operational uptime with AI-driven monitoring.

LEARN MORE

AXIS COMMUNICATIONS

AI, standards, and future disaster resilience

Artificial intelligence (AI) could not have stopped the 7.7 magnitude earthquake in Myanmar at the end of March — nor the immeasurable destruction it caused to the greater region. AI cannot prevent natural hazards like earthquakes. It can, however, support faster, smarter, and more targeted interventions that help lessen the impact for people when a disaster occurs.

As a complement to existing disaster risk reduction (DRR) systems, AI shows enormous potential – from real-time damage mapping and rapid flood assessments to climate forecasting, landslide detection, and monitoring systems.

Early tsunami detection

One recent example comes from the University of Paris (France), where researchers have developed an AI system that detects subtle atmospheric signals caused by earthquakes and tsunamis.

When an undersea earthquake or landslide takes place, they can trigger a tsunami that sends small waves through the ionosphere – ripples that AI can analyse in real time. The research team converted satellite data into images and trained the AI system on past occurrences.

The resulting tool can spot nascent tsunamis forming even where traditional warning systems – like sensor-equipped buoys – don't reach.

Mapping landslides

Landslides are another area where AI makes difference. When a magnitude 5 earthquake hit Italy in July 2024, it triggered thousands of landslides across the region. Within three hours of satellite data becoming available, researchers at the University of Padua (Italy) had used AI to map more than 7,000 scars across 3,300 square kilometres – an analysis that would have taken days or even weeks using traditional methods.

Fast mapping like this gives emergency teams on the ground a clearer view of the crisis and helps scientists understand how the events are connected, improving future preparedness.

Accelerating flood response

In the Philippines, AI is being used to map flood zones. Researchers from the University of the Philippines have developed a deep-learning model that automatically processes satellite data with minimal human input.

The system combines radar data from the European Union's Sentinel-1 satellite and optical imagery from the Dove nano-satellite constellation run by US-based Planet Labs. Based on those key inputs, it can map floods across up to five disaster zones in under four hours, helping emergency teams respond quickly when a flood hits.

Global cooperation on AI-enhanced hazard resilience

Access to AI capabilities has started transforming how countries prepare for and respond to disasters. The challenge now is to ensure these tools are reliable, responsible, and interoperable – in different regions, across national borders, and for varying socio-economic circumstances.

This is the focus of the Global Initiative on Resilience to Natural Hazards through AI Solutions.

The Global Initiative brings together five UN agencies: the International Telecommunication Union (ITU), the World Meteorological Organization (WMO), the UN Environment Programme (UNEP), the UN Framework Convention on Climate Change (UNFCCC), and Universal Postal Union (UPU).

It aims to pave the way for standards development and lay the foundation for ethical and effective AI use across the disaster management cycle.

This work forms a part of the global effort at standardization and to share solutions that can be scaled.

The Global Initiative, started in 2024, builds on an earlier ITU/WMO/UNEP focus group.

By Monique Kuglitsch, Innovation Manager at Fraunhofer HHI and Chair of the Global Initiative on Resilience to Natural Hazards through AI Solutions

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

Myanmar earthquake: Investing in disaster risk reduction to save lives and protect sustainable development

By United Nations Human Settlements Programme (UN-HABITAT) - Headquarters United Nations Office for Disaster Risk Reduction (UNDRR)

Earthquakes are among the deadliest natural hazards and are responsible for some of the most devastating disasters in human history. Their sudden nature means proactive disaster risk reduction is essential to reducing deaths and economic losses. And as it is often said, it is not earthquakes that kill people, but the collapse of buildings. Hence, countries in earthquake-prone zones must proactively invest in building their resilience. This means updating and enforcing building codes to ensure all new structures are earthquake-resistant as well as retrofitting old ones to meet resilience standards.

The impact of the earthquake in Myanmar, which as of 24 April resulted in the death of over 3,700 people, injuries of nearly 4,800, and the destruction of almost 65,000 structures, including homes, schools, and hospitals, is a sad reminder of the terrible cost of disasters. Moreover, the existing vulnerabilities, from years of conflict and instability, worsened the earthquake's impact, highlighting the importance of disaster risk reduction in countries

affected by conflict, violence, or fragility.

However, there is an opportunity for Myanmar to emerge from this disaster more resilient if the recovery process is based on the "build back better" approach, as called for in the Sendai Framework for Disaster Risk Reduction 2015-2030. UN-Habitat and UNDRR are committed to supporting countries to accelerate the implementation of the Sendai Framework in the remaining five years to help them avoid the worst impacts of disasters.

This includes recognizing the vital role of housing in resilience building, as Anacláudia Rossbach, Executive Director of UN-Habitat, states: "In these challenging times, our unwavering commitment is to support the communities affected by the earthquake. Since establishing our office in Myanmar following Cyclone Nargis, we have focused on risk-sensitive urban development to enhance resilience. Earthquakes do more than just damage buildings; they profoundly affect lives and the fabric of communities. Together with our partners and the communities themselves, we are dedicated not only to rebuilding housing and infrastructure but also to instilling hope, ensuring that each step we take makes the rebuilt areas stronger and more resilient than before."

UN-Habitat has been engaged in a range of projects across Myanmar, as detailed in the Country Programme Overview 2024–2026, which include essential initiatives such as solid waste management, climate action, and the implementation of nature-based solutions for disaster risk reduction. These efforts are complemented by upcoming initiatives aimed at developing nature-based solutions, climate-resilient schools, and resilient villages. This integrated approach ensures that resilience-building activities are both comprehensive and inclusive, addressing the immediate and long-term needs of Myanmar's communities.

Enhancing bilateral and multilateral cooperation is key to responding to these challenges, and the United Nations stands ready to support on this front. That is why international assistance to Myanmar must be increased to address urgent humanitarian needs, in urban and in hard-to-reach rural areas, and to support recovery efforts. This includes support to help Myanmar better understand the climate and disaster risks it faces and to strengthen its early warning system, which was impacted by the earthquake.

Kamal Kishore, Special Representative of the UN Secretary-General for Disaster Risk Reduction and Head of UNDRR, echoed the call made by the UN Resident Coordinator and Humanitarian Coordinator, urging the international community to step up its support in this critical time: "The people of Myanmar urgently require unwavering support from the international community in these trying times. I call on all nations to redouble their efforts in reducing disaster risks and bolstering resilience, ensuring that communities are better protected against all hazards."

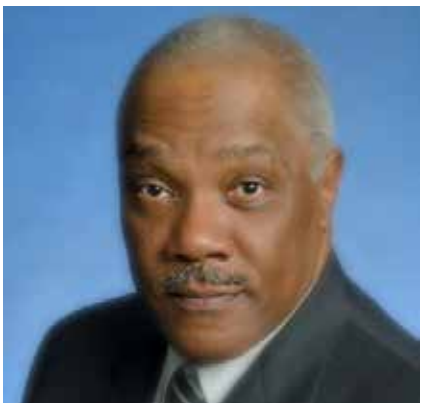
He also emphasized the importance of proactive measures to reduce earthquake disaster losses, noting: "Our understanding of the physics of earthquakes has improved. We also understand how buildings and infrastructure respond to earthquakes, and we know how to make them safer. From designing a simple structure to a complex physical infrastructure, engineering knowledge is at an all-time high. Yet the risk of losses from earthquakes is rising in most seismic countries. But trend is not destiny. It can be arrested. It can be reversed."

UN-Habitat and UNDRR are committed to supporting countries to build their disaster resilience and are cooperating in several areas. UN-Habitat has been an active member of the UNDRR-hosted International Recovery Platform since its inception. Additionally, both UN agencies are co-organizing sessions on resilient housing and reconstruction ahead and during the 8th Session of the Global Platform for Disaster Risk Reduction (GP2025), which will be held this June in Geneva.

Little can be done to prevent hazards like earthquakes from occurring. However, plenty can be done to prevent the damage they cause. Investing in disaster risk reduction and urban resilience building is the best way to save lives and protect sustainable development.

Cyber Preparedness and Incident Response to Critical Infrastructure

Every organization worldwide must protect its cyber resources from unauthorized intrusions. Cyber preparedness against attacks is essential. Recently, NIST released the Cybersecurity Framework (CSF) 2.0. The CSF suggests that each organization acquire knowledge of six core functions: Govern, Identify, Protect, Detect, Respond, and Recover. NIST also released Special Publication (SP) 800-61 Revision 3, titled " Incident Response Recommendations and Considerations for Cybersecurity Risk Management. " The purpose of NIST SP 800-61r3 is to assist organizations in incorporating cybersecurity incident response recommendations and considerations throughout their cybersecurity risk management activities. This integration aims to help organizations:



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

1. Prepare for incident responses by improving readiness.

2. Reduce the number and impact of incidents that occur.

3. Enhance the efficiency and effectiveness of incident detection, response, and recovery activities.

The article will focus on showing a nexus between these two publications. Before we discuss the initiatives outlined in SP 800- 61r3, let's summarize CSF 2.0. The CSF provides guidance for organizations to manage and reduce cybersecurity risks. One important addition to the framework is the GOVERN function. Governance establishes a risk management strategy that establishes roles and responsibilities and enforces policies and procedures. Another function is the implementation of safeguards that can reduce the likelihood and impact of cybersecurity incidents.

Organizations must adopt CSF 2.0 because it will provide a flexible framework to effectively manage and reduce cybersecurity risks. It assists organizations of all sizes to understand, assess, prioritize, and communicate their cybersecurity posture. CSF 2.0 allows organizations to tailor their approach to unique risks, missions, and objectives by focusing on desired outcomes rather than prescriptive actions. It integrates cybersecurity with enterprise risk management, supports continuous improvement, and enhances communication between executives, managers, and practitioners. Its supplementary online resources, such as Quick Start Guides and Implementation Examples, make it accessible and actionable for organizations at any stage of cybersecurity readiness.

NIST SP 800-61r3's purpose is to assist organizations in incorporating cybersecurity incident response recommendations and considerations into their cybersecurity risk management activities.

It organizes its recommendations and considerations using the NIST Cybersecurity Framework (CSF) 2.0 Functions.

Critical Infrastructure Protection Mechanisms are similar globally. They are part of a country's legal requirements, and the basic tenets of protection, preparedness, and incident responses are similar.

The incident response life cycle model described in NIST SP 800-61r3 is based on the six NIST Cybersecurity Framework (CSF) 2.0 Functions. It reflects the integration of incident response into broader cybersecurity risk management activities.

Importance of Cybersecurity Risk Management Incident Response is outlined below:

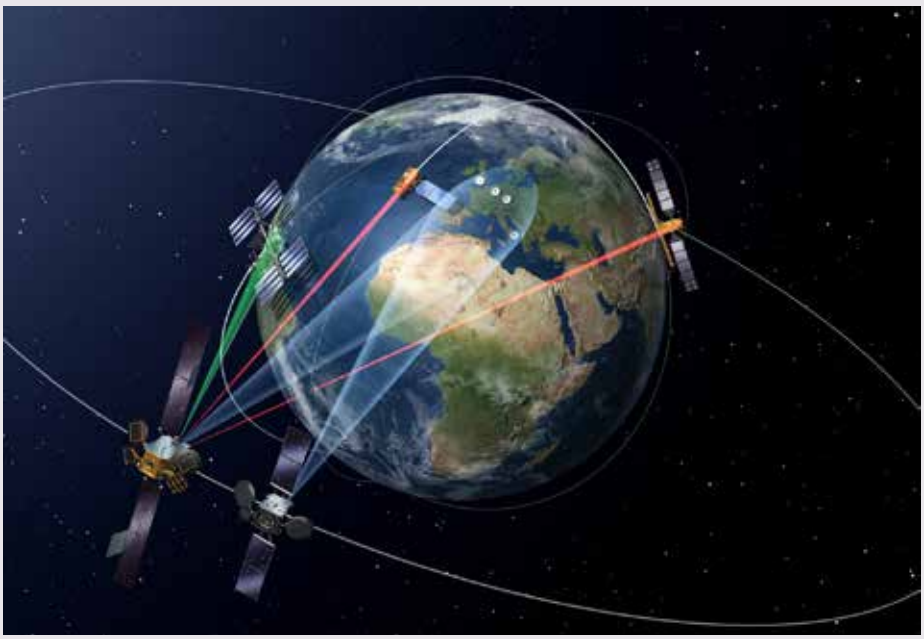
- Minimizing Damage
- Ensuring Business Continuity
- Proactive Risk Management
- Improved Detection and Response
- Compliance with Regulations
- Building Stakeholder Confidence
- Learning and Continuous Improvement
- Reducing Long-Term Costs
- Adapting to Evolving Threats
- Protecting Sensitive Data

Cybersecurity risk management and incident response are essential for protecting an organization's assets, ensuring operational resilience, and maintaining trust in an increasingly threat-prone digital environment. Critical infrastructure protection practitioners should review these documents to enhance their organizations' cybersecurity posture.

SP 800-61r3 contains community profiles in Table 2, which outline CSF preparation and lessons learned. Table 3 contains the second part of the Community Profile: Incident Response. Both tables recommend an element priority with suggested considerations.

Since many NIST Publications are reviewed and used internationally, NIST provides translations of key publications to support the global understanding of cybersecurity and privacy resources. I recommend that the English version be reviewed alongside the translation.

UN agencies warn of satellite navigation jamming and spoofing



Global satellite navigation systems are at risk from increasingly frequent jamming and spoofing of signals, threatening the safety and security of ships and aircraft worldwide.

The United Nations agencies for telecommunications, aviation and maritime shipping have called for urgent protection of the radio navigation satellite service (RNSS) that supports accurate global navigation and timekeeping.

ITU, together with the International Civil Aviation Organization (ICAO) and International Maritime Organization (IMO), issued a joint statement expressing "grave concern" about the rising cases of harmful interference.

Reported RNSS jamming and spoofing incidents indicate a growing threat to positioning, navigation and time services on land, at sea and in the air.

- Jamming refers to unauthorized transmissions of radio signals at the same frequency as authorized services, often to evade tracking or for security or defence purposes or.
- Spoofing involves fake signals mimicking authorized services, potentially misleading and endangering ships or aircraft.

The ITU Radio Regulations Board, on 21 March, urged specific administrations to abide by the ITU Constitution, the Radio Regulations, and take necessary actions to investigate and stop harmful interference affecting neighbouring territories.

Vital navigation services

Satellites transmit precise navigation, positioning, and timing information, making them vital for civil and humanitarian purposes worldwide. Global navigation satellite systems – namely the US-owned Global Positioning System (GPS), the European Union's Galileo, Russia's GLONASS, and China's BeiDou – all hinge on reliable RNSS.

Key radio navigation functions include:

- Navigation and positioning – used to determine precise locations in aviation, maritime, and land-based transportation.
- Timing and synchronization – providing accurate time signals for financial transactions, communication networks, and power grids.
- Civil and humanitarian applications – supporting disaster response, search-and-rescue operations, and various scientific applications.

However, growing dependence on satellite-based navigation heightens the risk of interference – whether accidental or intentional.

Reinforcement needed

In response to increasing incidents, the specialized agencies have laid out a multi-pronged approach for countries to keep the radio navigation satellite service operating reliably.

Together, they are calling for:

- Protection against harmful interference:
  ITU, ICAO, and IMO urge their member states worldwide to take necessary measures to prevent satellite systems from suffering harmful interference. Such interference can degrade, interrupt, or mislead signals, with potentially catastrophic consequences for aviation, maritime operations, and other civilian uses.
- Enhancing system resilience:
  Nations are encouraged to reinforce the resilience of systems that depend on satellite systems for navigation, positioning, and timing. This includes implementing strategies to withstand and mitigate the effects of interference on these critical services.

- Maintaining conventional navigation infrastructure:
  Recognizing the risks of service disruptions, the organizations call for the retention of sufficient conventional navigation infrastructure as a contingency support system in the event of radio navigation satellite service outages or misleading signals. Additionally, they recommend developing mitigation techniques to counteract service loss.
- Fostering interagency collaboration:
  Effective coordination is needed between radio regulatory bodies, civil aviation authorities, maritime organizations, defence agencies, and law enforcement to enhance monitoring, strengthen response efforts, and tackle interference threats more efficiently.
- Reporting and monitoring interference incidents:
  To better understand and combat harmful interference to RNSS satellite systems, national administrations are advised to report cases of harmful disruptions to relevant international telecommunication, aeronautical, and maritime authorities. All such reports should also go to the ITU Radiocommunications Bureau, which continuously monitors and assesses interference trends globally.

Global implications

Satellite-based navigation supports security and economic activities globally.

The collective call to action from ITU, ICAO, and IMO underscores the urgency of preserving RNSS integrity to safeguard critical navigation services from disruption.

Continued safety and efficiency in aviation, maritime, and other essential sectors depends on enhanced protective measures, infrastructure resilience, and global cooperation.

As technology continues to evolve, countries worldwide must take proactive measures to maintain the reliability of satellite systems and mitigate the risks associated with interference.

The future of global navigation, transportation, and communication depends on it, according to the three UN specialized agencies issuing the call to action.

More than 600 Global Data Centers Certified Under TIA-942 Standard, which Delivers Improved Performance and Efficiency

The Telecommunications Industry Association—the trusted industry association for the connected world — today announced that approximately 100 global facilities have been certified under TIA's latest revision to the Telecommunications Infrastructure Standard for Data Centers, ANSI/ TIA-942 Revision C. Since its inception more than 600 data centers across 51 countries and 6 continents have been certified under TIA-942.

The third and latest revision American National Standards Institute (ANSI) TIA-942-C standard, sets forth the requirements and recommendations for designing and implementing data centers worldwide to ensure the appropriate level of reliability and availability and provides enhancements to previous versions by incorporating new technologies that offer improved performance and efficiencies. TIA 942-C was published by TIA's TR-42 Committee in May 2024.

"The enhancements in TIA-942-C, which are aligned with industry best practices and include new and updated requirements for new technologies (including AI), and added considerations for sustainability, have been well received by our members and are key to the rapid adoption of this latest edition," said Tom McGarry, vice president of standards at TIA. "This significant milestone is further validation of the value our members are receiving from TIA-942-C, especially since it was introduced less than a year ago. We are extremely proud of the fact that more than 600 data centers around the world are performing better, operating more efficiently and experiencing improved service delivery by implementing the TIA-942 standard."

"The release of TIA-942-C marked a significant step forward in ensuring data centers meet the highest standards of reliability, efficiency, and security," said Edward van Leent, Chairman & CEO, EPI Group of Companies. "This updated framework is empowering organizations to enhance resilience, optimize performance, and future-proof their infrastructure. Every certification represents a commitment to excellence, and as we reach 100 TIA-942-C certified data centers, it is clear that the industry recognizes the immense value of this standard. By adopting TIA-942-C, organizations are not just meeting requirements—they are reinforcing trust, driving continuous improvement, and setting a new benchmark for the future of data centers."

The European Union Agency for Cybersecurity's first NIS360 report identifies areas for improvement and tracking of progress across NIS2 Directive sectors.

The NIS360 is a new product by the EU Agency for Cybersecurity, ENISA, that assesses the maturity and criticality of NIS2 sectors, providing both a comparative and a more in-depth analysis.

The goal of the NIS360 is to help national authorities and cybersecurity agencies in the Member States tasked with the implementation of the NIS2, (1) to understand the overall picture, (2) to help them with prioritisation, (3) to highlight areas for improvement, and (4) to facilitate monitoring of sectors' progress. The NIS360 also aims to support policy makers at national and EU level, to give input on policy and strategy development, and initiatives to build up cyber resilience.

The report sets out three main priorities.

Firstly, it recommends that collaboration, within and between sectors is strengthened, through community-building events and cooperation at sector, national and EU level.

Secondly, within this NIS2 transposition period, it is becoming more of a priority to develop sector-specific guidance on how to implement the key NIS2 requirements in each sector. The report notes that national sectorial authorities are stepping up to implement the NIS2. While investments are increasing across sectors, further upskilling is required.

Thirdly, the NIS360 emphasises the need for both alignment of requirements across borders in each NIS sector,

and for cross-border collaboration.

Key Findings at a Glance

Main findings include the following:

• **Electricity, telecoms and banking** are the three most critical and most mature sectors that stand out above the rest. These sectors have benefited from significant regulatory oversight, funding and investments, political focus, and overall a robust public-private partnership.

• **Digital infrastructures**, which includes critical services like internet exchanges, top-level domains, data centres, and cloud services, are a step below in terms of maturity. This NIS sector is very heterogeneous in terms of maturity of entities, and has a strong cross-border nature which complicates supervision, information sharing and collaboration.

• **Six NIS sectors fall within the NIS360 risk zone**, suggesting that there is room for improvement in their maturity relative to their criticality.

• ICT service management: The sector faces key challenges due to its cross-border nature and diverse entities. Strengthening its resilience requires close cooperation between authorities, reduced regulatory burdens for entities subject to both NIS2 and other legislation, and close cooperation in cross-border supervision.

• **Space**: Stakeholders' limited cybersecurity knowledge and its heavy reliance on commercial off-the-shelf components present challenges for the sector. Enhancing its resilience requires better cybersecurity awareness, clear guidelines for pre-integration testing of components, and stronger collaboration with other sectors.

• **Public administrations:** Being very diverse, it is challenging for the sector to achieve a higher common level of maturity. The sector lacks the support and experience seen in more mature sectors. Being a prime target for hacktivism and state-nexus operations, the sector should aim to strengthen its cybersecurity capabilities leveraging the EU Cyber Solidarity Act and exploring shared service models among sector entities on common areas e.g., digital wallets.

• **Maritime**: The sector continues to face challenges with Operational Technology (OT) and could benefit from tailored cybersecurity risk management guidance that focuses on minimising sector-specific risks, as well as an EU-level cybersecurity exercise to enhance coordination and preparedness in both sectorial and multi-modal crisis management.

• **Health**: The health sector with an expanded coverage under NIS2, continues to face challenges such as the reliance on complex supply chains, legacy systems, and poorly secured medical devices. Strengthening its resilience requires the development of practical procurement guidelines to help organisations acquire secure services and products, tailored guidance to help overcome common issues, and staff awareness campaigns.

• **Gas:** The sector needs to continue working towards developing its incident readiness and response capabilities, through the development and testing of incident response plans at national and EU levels but also through enhanced collaboration with the electricity and manufacturing sectors.

The report is based on data from national authorities with a horizontal or sectorial mandate, on self-assessment by companies within the NIS2 sectors, and on EU data sources such as Eurostat. In the ENISA NIS360, the strengths, sectorial challenges, gaps are identified, and recommendations are made to improve sectorial maturity and resilience across the Union.

CISA, DHS S&T, INL, LSU Help Energy Industry Partners Strengthen Incident Response and OT Cybersecurity

The Cybersecurity and Infrastructure Security Agency (CISA), Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Idaho National Laboratory (INL) hosted Louisiana State University (LSU) and several energy industry and critical infrastructure partners to train against simulated, high-impact cyberattacks on operational technology (OT) and traditional information technology (IT) at CISA's Control Environment Laboratory Resource (CELR) in Idaho Falls, Idaho, last week. LSU is the first university in the U.S. invited to participate in the CELR exercise, as part of CISA and INL's efforts to strengthen cyber talent development and research partnerships.

Cybersecurity threats exploit the increased complexity and connectivity of critical infrastructure systems. The potential incapacitation or destruction of assets, systems and networks, whether physical or virtual, could have a debilitating effect on national security, economic security and on public health and safety. As the nation's cyber defense agency, CISA is committed to growing operational and strategic partnerships to increase collaboration across the OT and industrial control systems (ICS) community.

On April 15-17, energy industry partners and the CISA-INL-LSU team used the CELR chemical processing platform, located at and operated by INL on behalf of CISA. CELR platforms are benchtop models of critical infrastructure with integrated industrial processes to represent how real-world components and facilities might be compromised through cyber-physical attacks. The participants were positioned in a live environment with IT and OT traffic and attacked by a technical team posing as a sophisticated adversary. The training participants' mission was to detect and respond to kinetic cyberattacks through ICS elements, including supervisory control and data acquisition (SCADA) systems, human-machine interfaces (HMIs), programmable logic controllers (PLCs), OT and IT systems and other key components widely used in industrial facilities.

"Collaborating with LSU and industry partners is extremely beneficial in strengthening the nation's cybersecurity knowledge and ability to respond to threats. This training is another step in our shared vision to expand the opportunity for critical infrastructure entities to strengthen their cybersecurity using CELR," said Matt Hartman, CISA Deputy Executive Assistant Director for Cybersecurity. "Malicious cyber actors and nation-state adversaries are a persistent, highly capable threat to critical infrastructure operations, functionality and safety. CELR is a valuable resource for critical infrastructure owners and operators seeking to improve the security of their ICS/OT networks."

"INL's Controls Laboratory hosts five CISA-sponsored ICS testbeds, offering immersive environments for partners to experience realistic cyberattack scenarios against critical infrastructure," said Tim Huddleston, INL's Cybersecurity Program Manager. "We were proud to host industry partners and academia in this exercise, helping them improve their skills in cyber hunting and incident response, which reduces the risk from malicious cyber actors."

Through a Cooperative Research and Development Agreement, LSU will operate and maintain the Oil and Natural Gas platform and host similar trainings for energy sector partners, state cyber defenders, and LSU faculty, staff and students.

This agreement will provide government and industry security professionals in the Louisiana gulf region an extremely valuable, local opportunity to hone their OT/ICS cybersecurity skills.

Primary Mitigations to Reduce Cyber Threats to Operational Technology

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), Environmental Protection Agency (EPA), and Department of Energy (DOE)—hereafter referred to as "the authoring organizations"—are aware of cyber incidents affecting the operational technology (OT) and industrial control systems (ICS) of critical infrastructure entities in the United States. The authoring organizations urge critical infrastructure entities to review and act now to improve their cybersecurity posture against cyber threat activities specifically and intentionally targeting internet connected OT and ICS.

Mitigations

The authoring organizations recommend critical infrastructure asset owners and operators implement the following mitigations[1] to defend against OT cyber threats.

- Remove OT connections to the public internet. OT devices are easy targets when connected to the internet. OT devices lack authentication and authorization methods that are resistant to modern threats and are quickly found by searching for open ports on public IP ranges with search engine tools to target victims with OT components [CPG 2.X].

- Cyber threat actors use simple, repeatable, and scalable toolsets available to anyone with an internet browser. Critical infrastructure entities should identify their public-facing assets and remove unintentional exposure.

- Change default passwords immediately and use strong, unique passwords. Recent analysis of this cyber activity indicates that targeted systems use default or easily guessable (using open source tools) passwords. Changing default passwords is especially important for public-facing internet devices that have the capability to control OT systems or processes [CPG 2.A][CPG 2.B][CPG 2.C].

- Secure remote access to OT networks. Many critical infrastructure entities, or contractors working on their behalf, make risk-based tradeoffs when implementing remote access to OT assets. These tradeoffs deserve careful reevaluation. If remote access is essential, upgrade to a private IP network connection to remove these OT assets from the public internet and use virtual private network (VPN) functionality with a strong password and phishing-resistant multifactor authentication (MFA) for user remote access.

- Document and configure remote access solutions to apply principles of least privilege for the specific asset and user role or scope of work [CPG 2.H]. Further, disable dormant accounts.

- Segment IT and OT networks. Segmenting critical systems and introducing a demilitarized zone for passing control data to enterprise logistics reduces the potential impact of cyber threats and reduces the risk of disruptions to essential OT operations [CPG 2.F].

- Practice and maintain the ability to operate OT systems manually. The capability for organizations to revert to manual controls to quickly restore operations is vital in the immediate aftermath of an incident. Business continuity and disaster recovery plans, fail-safe mechanisms, islanding capabilities, software backups, and standby systems should all be routinely tested to ensure safe manual operations in the event of an incident.

The authoring organizations recommend that critical infrastructure organizations regularly communicate with their third-party managed service providers, system integrators, and system manufacturers who may be able to provide system-specific configuration guidance as they work to secure their OT.

- Misconfigurations may be introduced during standard operations, by the system integrator, by a managed service provider, or as part of the default product configuration by the system manufacturer. Working with the relevant groups to address these issues may prevent future unintentional vulnerabilities from being introduced.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

Help2Protect.info

Protect your company from Insider Threats

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

Axis Communications reveals new video surveillance industry perspectives on AI

Axis Communications, the global industry leader in video surveillance, has released its latest report, 'The state of AI in video surveillance', which explores industry perspectives on the use of AI in security, safety and beyond.

Primary Mitigations to Reduce Cyber Threats to Operational Technology

The report reveals the top critical insights on AI technologies, their integration, and opportunities and challenges with regard to security, safety, business intelligence, and operational efficiency.

AI deployment has surged over the past two years, notably due to increased customer demands, improved knowledge of applications and the emergence of new use cases.

Mats Thulin, Director AI & Analytics Solutions, Axis Communications commented, "AI remains one of the most powerful and transformative technologies within the video surveillance industry. This new research reveals that while there are significant opportunities for AI to improve safety and security, operational efficiency and business intelligence, there must be a focus on ethical implementation and meaningful integrations which drive value.

Through qualitative research interviews with AI experts from the Axis global partner network, several thematic insights regarding AI technologies were uncovered in this new report.

The transition to cloud and edge AI continues to accelerate

The research findings highlight that the move from on-premise server systems to hybrid architectures continues at pace. This development is driven by the need for greater scalability, faster processing, and improved bandwidth usage. The hybrid model, which combines the immediate processing capabilities of edge AI on cameras with the scalability and long-term data storage of the cloud, is emerging as the preferred approach by many. This balance allows organizations to harness the strengths of both technologies.

Commvault and SimSpace Launch Unprecedented Cyber Recovery Range, Delivering Real-World Attacks, Real Skills, and Real Recovery

Commvault, a leading provider of cyber resilience and data protection solutions for the hybrid cloud, and SimSpace, a global leader in high-fidelity cyber range solutions, announced the Commvault® Recovery Range™, powered by SimSpace.

Commvault Recovery Range is the first hands-on cyber range that will enable defenders to battle sophisticated cyber threats and real-world attacks while also equipping them with the skills required to navigate and rapidly recover from cyber crises.

Traditional cyber ranges focus on detecting and containing attacks, leaving response and recovery scenarios outside of their scope. Commvault Recovery Range goes much farther in a setting that models the defender's own production environment. Utilizing SimSpace's award-winning cyber range platform and Commvault's exceptional recovery offerings, Commvault Recovery Range will provide an immersive learning experience where defenders can practice the entire end-to-end incident lifecycle, from detection through validated cleanpoint recovery.

The need for this type of end-to-end cyber resilience training has never been greater. Research shows an organization falls victim to ransomware every 14 seconds1, and the average downtime from an attack can span upwards of 24 days2 – costing enterprises millions of dollars in lost revenue, reputational damage, and operational disruption. Preparation that starts with the attack and ends with a rapid, clean recovery can make all the difference in reducing downtime and helping organizations run in a state of continuous business.

"Together with SimSpace, we are offering companies something that's truly unique in the market – the physical, emotional, and psychological experience of a real-world cyberattack and the harrowing challenges often experienced in attempting to rapidly recover," said Bill O'Connell, Chief Security Officer, Commvault. "In combining SimSpace's authentic cyberattack simulations with Commvault's leading cyber recovery capabilities, we're giving companies the ability to strengthen their security posture, cyber readiness, and business resilience."

HID Redefines Physical and Digital Security Integration with New Service Platform

HID, global leader in trusted identity and access management solutions, today announced the launch of HID Integration Service, a platform that integrates physical security, cybersecurity and digital identity management.

This integration platform-as-a-service (IPaaS) was designed to empower application developers, solution integrators and software vendors to seamlessly and rapidly integrate essential physical security solutions, streamlining processes and enhancing system interoperability. By doing so, the platform aims to ease the burden of maintenance and upgrades associated with managing and implementing integrations between physical security and cybersecurity systems, thereby lowering costs, streamlining operations and significantly reducing implementation time.

"Organizations have long struggled with brittle, complex integrations and the costs to maintain them," said Martin Ladstaetter, senior vice president and head of Identity and Access Management Solutions at HID. "HID Integration Service eliminates these pain points by providing an integration platform that connects physical and digital security products, reducing time to market for development partners who are building the next generation of security solutions with greater speed, quality, resilience and value."

HID Integration Service directly addresses the top benefits security leaders seek from unified management solutions—improved efficiencies, simplified management and enhanced visibility.

Bosch Building Technologies introduces the FLEXIDOME 8100i camera

Bosch Building Technologies continues its commitment to delivering innovative security solutions with the launch of the FLEXIDOME 8100i motorized pan-tilt-roll-zoom (PTRZ) camera.

The FLEXIDOME 8100i delivers reliable, high-quality video data for informed decision-making, thanks to edge-based AI video analytics, significantly improving security and operational efficiency across various applications. The uses include detecting personal protective equipment, safeguarding privacy, gathering details about an individual's physical characteristics for forensic searches, and even recognizing potential threats like firearms, among other critical applications. The camera excels in daylight and challenging nighttime conditions, providing exceptional image quality. In addition to the camera's AI and imaging capabilities, features such as smart installation, compliance with government regulations, and data security distinguish it as the ultimate fixed dome camera for mission-critical surveillance needs.

The camera's edge-based AI, Intelligent Video Analytics Pro (IVA Pro), provides over 95% accuracy for object detection, classification, and counting, enabling real-time safety and security enhancements with increased efficiency. Pre-installed IVA Pro software licenses for Buildings, Perimeter, and Privacy offer tailored solutions for diverse environments.

The camera's performance can be enhanced further with one of many IVA Pro software licenses. The versatility of IVA Pro enables users to optimize the camera's functionality and maximize its potential for their security system.

ESET Transforms Cyber Threat Intelligence Offering with New Feeds and APT Report Tiers

ESET, a global leader in cybersecurity solutions, has expanded its award-winning Cyber Threat Intelligence services, including new feeds and APT Report tiers.

ESET's offerings address modern cybersecurity needs with features like APT monitoring, threat hunting, and built-in AI that automates threat investigation. Announced at ESET World 2025 in Las Vegas, ESET has enhanced its services to accommodate the requirements of companies of all sizes that now view threat intelligence as an essential component of a next-gen, prevention-focused cybersecurity stack.

"ESET continues to expand its cyber threat intelligence offerings to accelerate incident response and reduce data breach impacts — delivering a holistic view of threat actors, attack vectors, indicators of compromise, and malware behaviour," said Juraj Malcho, Chief Technology Officer at ESET. "Because cyber attacks know no borders, many organisations mix and match multiple threat intelligence services to gain global visibility and leverage best-in-class capabilities. ESET's renowned visibility across Europe and Asia gives organisations a distinct advantage in preempting sophisticated threat actors and safeguarding their critical assets."

ESET has expanded its Cyber Threat Intelligence from eight to 15 threat feeds, delivering actionable, highly curated, metadata-rich, detailed data to defend against timely threats, including ransomware, malicious email attachments, cryptoscams, phishing URLs, smishing, SMS scams, and more. Quality is better than quantity in threat intelligence. Rather than struggling to sift through huge, noncurated external datasets, ESET telemetry is carefully deduplicated and delivered in real time — enabling threat analysts to act immediately and quickly identify emerging business risks and previously unknown threats.

ESET is enhancing its APT Reports to cover new tiers, extending this crucial intelligence to SMBs. The tailored formats cater to various organisational roles. SOC or threat analysts can use Technical Analysis reports and Activity Summary reports for in-depth details on attacks and post-compromise activity along with details about attacks, Indicators of compromise (IoCs), YARA rules, Snort rules, Shodan, Censys queries, and more. Beyond just IoCs, these reports provide context and expert advice.

Spirent Introduces Industry-First Automated Test Solution for New Era of Wi-Fi Devices

Spirent Communications plc, a leading provider of test and assurance solutions for next-generation devices and networks, today announced the release of the Octobox STA Automation Package, the industry's first solution to fully automate comprehensive performance testing and validation of client stations and devices on Wi-Fi 6/6E and Wi-Fi 7 networks.

The new automation package is designed to dramatically accelerate Wi-Fi station testing by replacing time consuming, inconsistent, and resource-intensive manual testing with structured, repeatable, and scalable validation automated workflows.

Wi-Fi technologies are evolving rapidly with Wi-Fi 6 and 6E implementations projected to exceed 80 percent of market share in 2025, and next generation Wi-Fi 7 adoptions making significant inroads. This rapid uptake of the new era of wireless technology is presenting challenges for manufacturers, eager to ensure reliable performance of increasingly sophisticated Wi-Fi connected devices.

"The complexity and time required to test next-generation Wi-Fi devices has increased exponentially with advancements like 320 MHz channels, 4096 QAM, and Multi-Link Operation," says James Kimery, Spirent's VP of Wireless Product Management. "Our new STA Automation Package is designed to help quality assurance teams tackle these challenges head on, with comprehensive automated performance testing workflows that can reduce test time by up to 70 percent compared with manual methods and enable the execution of dozens of test scenarios in the time it once took to run just a few."

Spirent's Octobox testbed is a customizable set of isolated chambers and instruments for testing over-the-air (OTA) Wi-Fi equipment and devices and the new STA Automation Package provides a fully automated test suite that ensures optimal performance in real-world conditions. It enables manufacturers to automate repeatable, overnight and parallel multi-station test execution to eliminate inconsistencies associated with manual testing, and enable validation of more devices, across more environments, more frequently.

critical infrastructure PROTECTION AND RESILIENCE EUROPE

T S I M E

ADVERTISING SALES

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

Jina Lawrence
Rest of World
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234750

Critical Infrastructure Protection Week *in Europe*

14th-16th October 2025 - Brindisi, Italy

International Association of CIP Professionals

critical infrastructure PROTECTION AND RESILIENCE EUROPE

T S I M E

INVITATION TO ATTEND

Securing the Inter-Connected Society

The International Association for CIP Professionals is delighted to be hosting the 2025 CIP Week in Europe with the patronage of the City of Brindisi.

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

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

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

To discuss sponsorship opportunities:

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