critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

SUMMER 2024
www.cip-association.org

FEATURE:
Perspective: Artificial Intelligence

FEATURE:
As cyberattacks increase, physical security should remain a top priority

FEATURE:
Solving the Puzzle of Protection

CROWDSTRIKE OUTAGE: A FAULTY UPDATE CAUSES WORLDWIDE PROBLEMS

INVITATION TO ATTEND

Securing the Inter-Connected Society

The premier event for the critical infrastructure protection and resilience community.

EARLY BIRD RATES CURRENTLY APPLY

Register today and save with the Early Bird discount - deadline 12th October.

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Project' conference as the first events as part of this initiative.

Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

The conference will look at the developing themes and challenges facing the industry, including the importance of the implementation of the **NIS2 Directive and Directive on the Resilience of Critical Entities** and the obligations of CI owner/operators and agencies, as well as create a better understanding of the issues and the threats, helping to facilitate the work to develop frameworks, good risk management and strategic planning.

Join us in Madrid, Spain for the the 9th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure, part of CIP Week in Europe.

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

Leading the debate for securing Europe's critical infrastructure

Speakers include:

- **Jose Luis Perez Pajuelo**, Director General, National Center for Critical Infrastructure Protection, MOI
- **Dr. Enrique Belda Esplugues**, Director General, Port of Valencia
- **Luca Tagliaretti**, Executive Director European Cybersecurity Competence Center (ECCC)
- **Daniel Golston**, Associate Programme Officer Organization for Security and Co-operation in Europe
- **Dr Monica Cardarilli**, Project Officer European Commission Joint Research Centre, Italy
- **Rodrigo Brito**, Global Head of Cybersecurity Portfolio Nokia, Portugal
- **Frederic Petit**, Project Officer European Commission Joint Research Centre, Italy
- **Peter Nilsson**, Police Commissioner Head of Airpol, Europe
- **John Laene**, Managing Director RAILPOL
- **Dr Victor Vevera**, General Director ICI Bucharest, Romania
- **Alessandro Lazari**, Fellow in Critical Infrastructure Protection and Resilience University of Salento, Italy & International Association of CIP Professionals

For full speaker line up visit www.cipre-expo.com/speakers-2024

Supporting Organisations:

Platinum Sponsor:

Digital Security Progress. Protected.

Flagship Media Partner:

ARE YOU KEEPING ON TOP OF GLOBAL EVENTS?

What a year so far! Have you managed to keep up with global events to enure you are utilising every tool at your disposal to mitigate the seemingly never ending onslaught of threats, whether malicious or not, to our critical infrastructures?

From a seemingless innocent software patch update, causing a massive global IT outage, to increasing tensions between the Middle East and Western nations, it's been an interesting few months.

We take a deeper look into the Crowdstrike Outage and it's impact on global systems, posing the question whether we have we come too dependent on few large companies that manage the global networks. Or is it time to ensure more solution providers are involved to create natural resilience in the system. Both have the advantages and disadvantages, but this summer perhaps has proven the status quo does not work when a problem occurs.

If we (and more pointing the finger towards governments) are not careful, the skirkishes in the Middle East could quite easily escalate into a much more serious situation. Combined with the on-going conflict between Ukraine and Russia, a likelihood of increased attacks, from bith cyber and physical perspectives, against critical infratructures increases - are we truly prepared?

We are delighted to be seeing CIP Week in Europe take place in Madrid, giving the CI community the opportunity to meet, network and share ideas and experiences. Something that is needed more now than ever. These are indeed testing and challenging times!

We hope to see you in Madrid, Spain on 12th-14th November at the CIP Week in Europe and help expand your network, ideas and strategies for securing your CI.

Enjoy reading this issue, we hope you once again find it interesting and informative.

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.

CrowdStrike Outage: A Faulty Update Causes Worldwide Problems

CIPR News caught up with Dr. Gregory Bird, Professor of Cybersecurity for Liberty and Southern New Hampshire Universities, to discuss the world's biggest IT outage in recent years.

Critical infrastructure and other organisations worldwide suffered large-scale disruption caused by a defective content update.

As a leading cybersecurity firm, CrowdStrike's software is used by countless organizations across the globe, from small businesses to multinational corporations. On July 19, 2024, a faulty update to CrowdStrike's Falcon Sensor security software caused a widespread IT outage affecting millions of Microsoft Windows computers worldwide, after the initial panic of what seemingly appeared to be thought a cyber attack.

The faulty update targeted Windows systems, a platform used by a majority of computers worldwide. This widespread reliance amplified the impact of the outage. This incident was unprecedented in scale and caused significant disruptions to businesses and individuals globally.

So, how did we get here and are we in a more secure, or less secure position, as a result of so much IT infrastructure under the control of so few companies?

The interconnectedness of global systems means modern businesses rely heavily on digital infrastructure, with many systems interconnected and interdependent. A disruption at one point can create a ripple effect throughout various industries.

Many critical infrastructure sectors, such as healthcare, finance, and transportation, depend on robust IT systems. This outage affected these sectors, leading to disruptions in essential services, some for many days or even weeks.

CIPR News discussed the situation with Dr. Gregory Bird, Professor of Cybersecurity for Liberty and Southern New Hampshire Universities.

"The global outage was caused by one of Crowdstrike Falcon's regular updates, much like your antivirus type of updates. And because it's updated more frequently, it doesn't go through the same type of review process that the actual sensor content updates do, it actually bypasses all of those staging controls within CrowdStrike Falcon.

"The reason for this is it's really designed to get out to the users as fast as possible to help ensure that whatever virus malware is blocked as fast as possible, and help reduce the likelihood that zero-day type of attacks are able to actually get through. Unfortunately, many of the system administrators out there, they did not understand how the staging protocols actually worked in CrowdStrike Falcon. Many of them assumed that it was for all updates that would actually follow that, not realizing that there's two different parts to the updates, and only one followed that staging protocol." Dr Gregory Bird explained.

It's perceived at this stage as being a genuine human error of testing and deployment, and not the possibility it could have been an insider threat or a malicious insider cyber attack.

Why was it being pushed out so quickly without its proper tests?

This is not an unusual phenomena and has caused issues with other updates from other IT companies in the past, but just not as noticeable as this recent global outage.

Although it did go through the company's testing, it's just their automated testings failed. The whole reason they want to push these updates out faster and not go through your typical certification and signing type protocols, like you would have for many things that end up like drivers and whatnot for many of the systems, it's because the longer it takes, the more susceptible the systems are to potential cyber attack. Because these updates, much like your typical antivirus and malware type updates, they are very time sensitive to get them out there to help ensure that the systems are properly protected.

Crowdstrike has come out and they've actually released a number of protocols that they're going to implement to help ensure, one, these updates do get more proper testing, get better validation to help ensure that this particular error doesn't happen again, and two, to help avoid future potential for things like insider threats.

They're also planning to include this in a staging protocol within that system. And they're also planning to stage future releases so that not all their users get it at the exact same time, so that if something like this were to happen, it allows them a little more time to respond before it propagates out to the entire world.

So how can this be avoided in future, better training of staff in terms of process?

"Yes. Well, I would say better training of staff. They're supposed to be looking at some of their automated processes to help ensure that when errors do occur, they're properly getting kicked out and not pushed out. And the other thing is really getting their staff to provide more attention to detail

so that they aren't allowing these type of errors to proceed forward." added Dr Gregory Bird.

So, if this had been a cyber attack, it affected so much of the global IT infrastructure, how have we got to the position that so much of the vulnerable global IT infrastructure is in the hands of so few?

What could be done with these organisations without compromising security?

How can we better build in protection into such a small number of companies?

"So, this incident is a glaring reminder that relying on a single entity for service, regardless of the vendor's reputation, it creates a very serious and dangerous single point of failure. So, companies really need to regularly take this into account when they're assessing their incident response and disaster recovery plans."

"While implementing multiple layers with multiple vendors can benefit from a business continuity and protecting your critical operations. The downside to that is they can also dramatically increase the complexity of your architecture and can inject issues as far as compatibility. So this type of event will happen again and it can happen with any vendor, any products."

"The big thing organizations need to not only look at building in more redundancy to their architectures, but also focus on resiliency. This type of event isn't new. We've seen it before." continued Dr Bird, referring to similar impacts of the SolarWinds incident and what happened with McAfee back in 2010.

You always have elements like ransomware that can definitely have the potential to have a similar attack.

Organizations need to have long-term memory when they're assessing their organizations. They need to ensure they're properly conducting a business impact analysis, create their disaster recovery plans and incident response plans.

But not only create them, they need to ensure that they're actually testing and validating those plans. Along with that, conduct training to ensure the employees know not only how to enact those various protocols, but they know their individual role. And going through the actual training and live exercise of those plans really helps to identify and highlight the gaps that they may have in.

"Tabletop exercises are an excellent way that organisations can actually test all of these in a safe type of setting without potentially actually impacting their environment. And while there are some great companies out there actually creating all these tabletop exercises that companies can procure, the Cybersecurity & Infrastructure Security Agency (CISA) also offers tabletop exercise packages or their CTEPs, which are basically exercises in a box. So they're a comprehensive set of resources designed to really assist the stakeholders in conducting their own exercises." commented Dr Bird.

So how does a company build in a resilience and business continuity plan if there are so few alternatives?

Well, in this case, fortunately, there are other alternatives out there in the market. In fact, almost once this incident happened, you immediately started seeing advertisements for many of those companies.

In fact, one of Crowdstrikes top competitors stock price jumped about 6% so far within the first week. So, you can see there's definitely some interest in those alternatives.

There are things that companies really need to look at when they're selecting their vendors though.

While many may tend to gravitate to whoever that biggest name is, taking elements like this incident into account are things that you do need to evaluate. The other piece is, as you're working to build in more resiliency to your environment, ensure that you actually have backups for your systems and ensure the backups work and ensure they remain current.

Dr Gregory Bird noted, "Companies need to be more proactive. They need to work with their third-party suppliers, question them about their processes and what they do to ensure events like this don't happen. They need to also assess their existing change management and test validation procedures."

"Do they actually have systems that allow you to stage and stagger your deployments, or does everything just go out at once? Do they have actual staging environments to test this? Do they have their canary-type users that they can do limited deployments on? So, if their tools don't have the ability to stage those, look at possibly going to a vendor that does, or advocate with the vendor to add those type of capabilities."

"Many companies I end up talking to, they don't realize the power that they do have to help influence future features with these companies. Many times, going out and talking to your service advisors or account representatives can go a long way towards actually getting these type of capabilities." added Dr Bird.

One of the big key sectors that impacted was air travel, with the system being used for transmitting

of API P&R data across the world. So what does the airport do, for example, in that particular instance?

"I can't necessarily speak for everybody throughout the entire world, but definitely here in the U.S., work with your sector risk management agency, as well as those various governing bodies that you have to help influence many of those decisions. When they get forced on you, test them. Ensure you have personnel that are very fluent in that individual systems or tools to help ensure that you can potentially avoid events and incidents like this."

"When you don't have a choice of what tools you use, definitely play with them extensively and work that into your various disaster recovery plannings and continuity of operations. In cases like this, the companies that didn't, say, have all Windows machines, that had mixes with Linux and iOS, that they were able to still continue doing work. So for the areas that you can actually affect change and determine what type of products you're using, look to expand the diversity of that." commented Dr Bird.

Could this recent Crowdstrike caused global IT outage lead to introduction of whether it's legislation or anything to introduce more competition, break up the big boys so that we're not so reliant on them?

Well, it definitely has the potential to increase overall competition within that particular cybersecurity niche, we shall have to wait and see whether policymakers take the initiative for less reliance on a small number of large players, or if the market itself makes the move.

Any significant issue like this tends to open up the market to other companies, as well as the creation of new companies to step in that now see various gaps that they can meet.

"It's very unfortunate when incidents like this happen, it definitely does open up the market more. And I think it helps kind of spark some interest in the actual users to assess what type of products they're using. For the companies that don't have that long-term memory issue, and they actually start remembering when these events are happening, they many times will go assess, okay,

how are we actually deploying this software? What software packages are we using? What can we actually do to build in redundancy and resiliency into our overall architecture and our plans?"

"I will say that while quite tragic and unfortunate that this happened, I am impressed with the current response that CrowdStrike has had as far as their action plan to actually address this to ensure it doesn't happen again in the future. I would love to advocate that other cybersecurity companies that are out there take note of this." concluded Gregory Bird.

In essence, the combination of CrowdStrike's widespread use, the reliance on Windows, and the interconnected nature of global systems created a perfect storm for a massive outage with far-reaching consequences. Something we need to guard against in the future, as the consequences could be even more severe.

CREWS Initiative launched in Djibouti to strengthen early warning systems and disaster preparedness

The Climate Risk and Early Warning Systems Initiative (CREWS) project has been launched in Djibouti to enhance the nation's resilience against climate-related hazards. This collaborative initiative, led by the World Meteorological Organization (WMO) and the United Nations Office for Disaster Risk Reduction (UNDRR), is set to strengthen the capacities of Djibouti's national hydrometeorological and disaster management agencies over the next four years.

Djibouti, located in the Horn of Africa, faces significant vulnerability to climate change, with increasing temperatures, prolonged droughts, and a heightened risk of flooding impacting its population and economy. Approximately 33% of the population lives in high-risk zones, and 35% of the economy is chronically vulnerable to these climate hazards.

The CREWS Djibouti project aims to address these challenges by improving the capacity of key institutions. The project's key outcomes include enhancing service delivery, developing risk information for early warning systems, strengthening ICT, bolstering response plans and awareness programs, and providing capacity-building programs and gender-sensitive training.

Speaking at the launch, Nora Achkar, Chief of the UNDRR Regional Office for Arab States, highlighted the importance of the project in safeguarding the future of Djibouti. This project is not just about technology and systems; it is about empowering people and institutions, she said. "By ensuring that early warning information is accessible, actionable, and tailored to the needs of all, particularly the most vulnerable, we can save lives, protect livelihoods, and reduce the devastating impacts of disasters."

The launch event, held in Djibouti City, highlighted the importance of the initiative in enhancing early warning systems and preparedness for extreme weather events. The agenda featured presentations on the project structure, current status, and expectations for implementation by various national institutions.

Sense threats against our critical infrastructure better than ever

with on-edge analytics.

LEARN MORE

AXIS COMMUNICATIONS

The Secure SatCom Hub for All-Missions

The Caribbean is the second-most What happens when a disaster like an earthquake causes ground networks to collapse, effectively shutting down communications within the disaster area?

For situations like this, there's GOVSATCOM.

When disaster strikes, having ready access to secure satellite communications (SatCom) is critical to emergency response and mitigation efforts.

The European Union Governmental Satellite Communications GOVSATCOM programme is set to provide secure, cost-efficient and highly reliable communications capabilities to security and safety critical missions and operations managed by the EU and its Member States.

"By pooling the services, capacities and resources of existing providers, GOVSATCOM will offer a secure SatCom solution for authorized governmental users," says EUSPA Executive Director, Rodrigo da Costa.

At the centre of this one-stop-shop is the GOVSATCOM Hub.

The heart of the GOVSATCOM ecosystem

As the secure ground infrastructure of the GOVSATCOM programme, the Hub is a unique cutting-edge innovative core IT system bringing together commercial and governmental satellite communications capabilities and services. These are then shared with EU Member States, who can use them for such security-related missions as surveillance, protecting critical infrastructure and crisis management.

"The Hub is the heart of the GOVSATCOM ecosystem, linking the programme's pool of SatCom service providers and operators with authorised government users," explains EUSPA GOVSATCOM programme manager Dr Georgios Synnefakis.

EUSPA, responsible for procuring the GOVSATCOM Hubs, recently announced that the Hub will be implemented by a consortium led by GMV.

"The GOVSATCOM Hub will create a symbiosis between best-in-class delivery of secure satellite communication services and critical user mission needs by ensuring reliably available and always resilient satellite communications" adds Dr Synnefakis.

In addition to managing the GOVSATCOM Hub's implementation, EUSPA will oversee its operations and coordinate the user-related aspects of the programme, all in close collaboration with Member States, the European Commission and other involved EU agencies. The Agency also regularly works with DG DEFIS to support such ongoing GOVSATCOM-related activities as defining the programme's security baseline and drafting relevant implementing acts.

The GOVSATCOM Hub will also pool resources for the IRIS2 programme, the EU's forthcoming constellation providing secure communication services to the EU and its Member States. This will expand the Hub's service portfolio to include applications that require low latency and global coverage (e.g. aerospace, maritime).

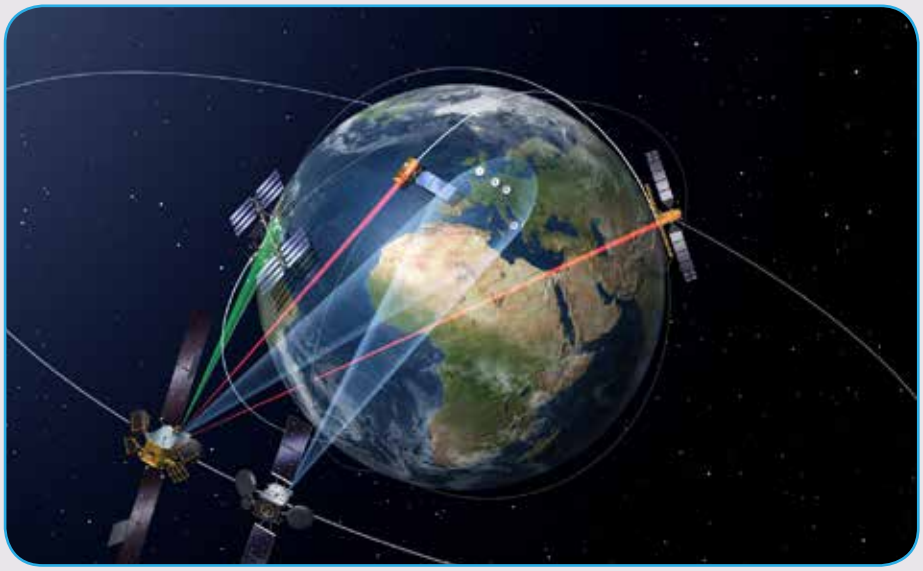
Serving EU governments, benefiting Europe

While GOVSATCOM's users may

be governments, its beneficiary is clearly Europe. For instance, in addition to its use during natural disasters, the service will play an important role in securing critical infrastructure like dams and air traffic control. It can also be used to support such governmental operations as border and maritime monitoring, especially in remote areas that lack ground-based connectivity.

"By helping governments in managing disasters and other emergencies, GOVSATCOM supports the safety, security and wellbeing of all EU citizens," concludes Rodrigo da Costa.

GOVSATCOM initial services will be gradually launched in the coming months, with full operational capability to follow by mid-2027.



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

LockBit power cut: four new arrests and financial sanctions against affiliates

Europol supported a new series of actions against LockBit actors, which involved 12 countries and Eurojust and led to four arrests and seizures of servers critical for LockBit's infrastructure. A suspected developer of LockBit was arrested at the request of the French authorities, while the British authorities arrested two individuals for supporting the activity of a LockBit affiliate. The Spanish officers seized nine servers, part of the ransomware's infrastructure, and arrested an administrator of a Bulletproof hosting service used by the ransomware group. In addition, Australia, the United Kingdom and the United States implemented sanctions against an actor who the National Crime Agency had identified as prolific affiliate of LockBit and strongly linked to Evil Corp. The latter comes after LockBit's claim that the two ransomware groups do not work together. The United Kingdom sanctioned fifteen other Russian citizens for their involvement in Evil Corp's criminal activities, while the United States also sanctioned six citizens and Australia sanctioned two.

LockBit full infrastructure in the crosshairs of law enforcement

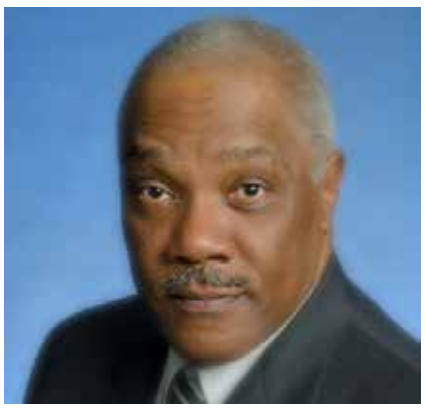
These are some of the results of the third phase of Operation Cronos, a long-running collective effort of law enforcement authorities from 12 countries, Europol and Eurojust, who joined forces to effectively disrupt at all levels the criminal operations of the LockBit ransomware group. These actions follow the massive disruption of LockBit infrastructure in February 2024, as well as the large series of sanctions and operational actions that took place against LockBit administrators in May and subsequent months.

Between 2021 and 2023, LockBit was the most widely employed ransomware variant globally with a notable number of victims claimed on its data leak site. Lockbit operated on the ransom as a service model. The core group sold access to affiliates and received portions of the collected ransom payments. Entities deploying LockBit ransomware attacks had targeted organisations of various sizes spanning critical infrastructure sectors such as financial services, food and agriculture, education, energy, government and emergency services, healthcare, manufacturing and transportation. Reflecting the considerable number of independent affiliates involved, LockBit ransomware attacks display significant variation in observed tactics, techniques and procedures.

With Europol's support, the Japanese Police, the National Crime Agency and the Federal Bureau of Investigation have concentrated their technical expertise on developing decryption tools designed to recover files encrypted by the LockBit Ransomware.

The support from the cybersecurity sector has also proven crucial for minimising the damage from ransomware attacks, which remains the biggest cybercrime threat. Many partners have already provided decryption tools for a number of ransomware families via the 'No More Ransom' website.

Perspective: Artificial Intelligence



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

The European Union (EU) achieved a significant milestone in the field of Artificial Intelligence by releasing a draft of the EU Artificial Intelligence Act in March of this year. This 458-page document, a cornerstone in AI governance, outlines the deployment and use of AI and categorizes initiatives based on risk. The Act sets a standard for the responsible use of AI in the EU, keeping us all informed and current in this rapidly evolving field. Its size and detail have set the stage for a comprehensive investigation, and I am eager to share my perspective with you once I reach a conclusive research stage.

My journey into the realm of Artificial Intelligence (AI) has been marked by a series of challenges, the first and foremost being the understanding of its definition. The diverse viewpoints, ranging from an ability to a theory, have made it a complex subject. To

align my lectures and perspective, I turned to the definition from the United States Code, a source that provides a relevant and important understanding of AI. In 15 U.S.C. 940 (3), AI is defined as:

The term "artificial intelligence" or "AI" has the meaning set forth in 15 U.S.C. 9401(3): a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. Artificial intelligence systems use machine- and human-based inputs to perceive real and virtual environments, abstract such perceptions into models through analysis in an automated manner, and use model inference to formulate options for information or action.

As I tried to distinctly categorize the recent Executive Order (EO) 14110 signed on October 30, 2023, in the United States, the definition of the term under the United States code was most appropriate. Against this background, I shall present my perception of the premise of AI and the directive. Based on this loosely defined approach, I required a better definition of AI. Looking at it, I discovered that there are two main supporting sublevels of AI.

AI entails enhancing systems' functionality by integrating computational procedures. Machine learning (ML) is a lower level, which builds procedures and strategies that let computers learn and draw conclusions on their own.

The subsequent level of ML is

the Advanced Level, which is also called Deep Learning (DL). DL applies artificial neural networks to create layers, which allow the DL model to learn and extract high-level features of representations from the data. To explain it in layman's terms, a neural network is a subset of ML that embeds a thinking pattern akin to the human brain while concluding.

As context for the directive provided to the Executive Branch of the U. S. Government, the EO concentrates on the safe, secure, and trustworthy application of AI. The key protective measures outlined in the order: The key protective measures outlined in the order:

1. Risk Management Framework: NIST released 'An AI Risk Management Framework publication' to Establish a framework for addressing risks that come with Artificial Intelligence, for instance, privacy, security, and ethical issues.

2. Transparency and Accountability: AI developers need to make the decision-making process explicit in their algorithms and approaches and take responsibility for the consequences that AI-affecting systems produce.

3. Data Protection: This requires rigorous measures to protect the information processed through AI systems and the individual information used in the system.

4. Bias Mitigation: Provides solutions for eliminating bias in AI systems, enabling companies to produce fairly and equally effective AI algorithms.

5. Collaboration and Standards: The companion document to the EO is a roadmap from the Cybersecurity and Infrastructure Security Agency that promotes active partnership between the government, industry, and academia in establishing and following standards and best practices for timely industrial AI application.

6. Public Awareness and Education: Organizations should include AQ's instructions on how to use AI or when they intend to use AI.

They all seek to establish proper values so safe and ethical AI

technologies can be developed and implemented.

Machine Learning and Deep Learning are the subcategories of AI. The supervision learning algorithms let computers learn from data and prediction problems; the deep learning algorithms are effective on complicated and unformatted data problems, as they use deep neural networks. In cybersecurity, both ML and DL are applied to increase threat identification, anomaly identification, and the overall performance of a security system. Every organization and individual "MUST" must undertake their own AI research depending on their proposed application and justification. Now, the United States and the European Union offer a relatively high level of AI development and utilization governance.

Dr. Ron Martin is a Professor of Practice at Capitol Technology University, specializing in the functional areas of Critical Infrastructure, Industrial Control System Security, Identity, credentials, and Access Management. Ron is an IEEE Senior Member, an active contributor at the Cloud Security Alliance, and a member of the International Association of CIP Professionals.

Intuitive Security Solution for 24/7 Mission Critical Security

Make the right decision at the right time to keep people, property, and business operations safe and running smoothly. Built on a cybersecure web platform, C·CURE IQ lets you manage and monitor access control and video surveillance from anywhere in the world.

Johnson Controls

As cyberattacks increase, physical security should remain a top priority

By Sunil V. Mudholkar is vice president of product management, physical security, for Hexagon's Safety, Infrastructure & Geospatial division.

We are living in an era where sinister cyberterrorism threats dominate the headlines. Sadly, critical infrastructure is a prime target, and unforeseen attacks can have far-reaching impacts. Although cybersecurity is often the topic of conversation, the importance of physical security measures to protect the world's critical infrastructure cannot be forgotten.

According to the U.S. Department of Homeland Security's Homeland Threat Assessment 2024, domestic terrorists are calling for more physical attacks on critical infrastructure this year to disrupt commerce, the economy, the electoral process and the public's sense of safety. Just since 2022, there have been 2,800 reported incidents of gunfire, vandalism and other physical assaults on the electric power grid in North America, according to the North American Electric Reliability Corp.

In Moore County, N.C., in 2022, a deliberate shooting of electric power substations resulted in a multi-day power outage for more than 45,000 people.

Schools and college campuses are also considered critical infrastructure and have seen more than their share of attacks. So far in 2024 year, there have been 35 incidents of school and college campus shootings in the U.S. alone.

There are also numerous incidents

at railway stations and subways each year, along with attacks on the trains themselves. Between 1970 and 2017, there were 282 attempts to derail trains deliberately and 817 additional attacks on railway infrastructure worldwide.

Since 1980, there have been at least 75 terrorist attacks on airports, according to the RAND-MITP Terrorism Incident Database.

Our critical infrastructure -- be it power plants, rail lines, seaports, airports, communication hubs and even schools -- is the backbone of our global economy and society.

Rightfully so, governments are pouring money into cybersecurity in the face of highly publicized cyberattacks, but it is imperative to ensure physical security as well. Even data centers, the heart of IT infrastructure and cybersecurity measures, need physical security protection.

Governments worldwide have worked to harden critical infrastructure protection regulations and protocols. In the U.S., the National Infrastructure Protection Plan outlines a collaborative approach involving government, industry, and other stakeholders. Separate regulations exist for various critical infrastructure sectors—energy, transportation, water, and communications. The European Union, meanwhile, has its own directives to enhance the security of critical infrastructure across member states.

A comprehensive security strategy must integrate both physical and cyber defenses to create a resilient infrastructure. This includes employing surveillance systems, security personnel and response systems, and access control measures that work in tandem with cybersecurity protocols. Doing so

ensures a multi-layered defense that addresses all aspects of security.

That integrated line of defense must include modern surveillance, upgraded from simple security cameras connected to recorders. Today's modern surveillance cameras, complemented by 3D light detecting and ranging (LiDAR) remote sensors, allow for precise detection and tracking of intruders to critical infrastructure sites. These high-tech surveillance systems can be connected to video management systems that allow the infrastructure operator to monitor incidents in real time, activate multi-agency emergency response through computer-aided dispatch systems and analyze any threats, successful or not.

During an incident, information sharing and collaboration are key to developing response strategies within single teams as well as across organizations. For example, if a power plant or seaport came under physical attack, multiple public safety agencies need to respond. Web-based collaboration portals enable them to be on one interface, receiving the same information at the same time. Together, with a streamlined, intuitive workflow, collaborating agencies can create and adapt response plans in real-time. In these highly regulated environments, today's systems can also help create detailed and accurate after-action reports.

Investing in physical security is not merely a cost; it's an investment in the stability and continuity of essential services. The repercussions of failing to secure our critical infrastructure are not just immediate but can also undermine public trust and economic stability.

As we continue to advance technologically, the need for physical security in critical infrastructure remains as relevant as ever. It is a fundamental aspect of national security and public safety. By prioritizing and investing in physical security measures along with cybersecurity protections, we can safeguard the very systems that enable our modern way of life.

UN cybersecurity report assesses global progress in providing a safe and secure digital future for all

Countries strengthening cybersecurity efforts, but increased action still required

Countries around the globe are improving cybersecurity efforts, but stronger actions are needed to meet evolving cyberthreats, according to the Global Cybersecurity Index 2024, released by the International Telecommunication Union (ITU).

On average, countries have taken more cybersecurity-related actions and improved their cybersecurity commitments since the last index was released in 2021.

Worrisome threats highlighted in the report include ransomware attacks targeting government services and other sectors, cyber breaches affecting core industries, costly system outages, and breaches of privacy for individuals and organizations.

"Building trust in the digital world is paramount," said Doreen Bogdan-Martin, ITU Secretary-General. "The progress seen in the Global Cybersecurity Index is a sign that we must continue to focus efforts to ensure that everyone, everywhere can safely and securely manage cyberthreats in today's increasingly complex digital landscape."

A new assessment with sharper focus

ITU's Global Cybersecurity Index 2024 (GCI 2024) assesses national efforts across five pillars, representing country-level cybersecurity commitments: legal, technical, organizational, capacity development, and cooperation.

GCI 2024 also uses a new five-tier analysis, a shift that allows a greater focus on each country's advances with cybersecurity commitments and resulting impacts.

The report places 46 countries in Tier 1, the highest of the five tiers, reserved for "role modelling" countries that demonstrate a strong commitment in all five cybersecurity pillars.

Most countries are either "establishing" (Tier 3) or "evolving" (Tier 4) in terms of cybersecurity. The 105 countries in these tiers have largely expanded digital services and connectivity but still need to integrate cybersecurity measures.

A "cybercapacity gap" – characterized by limitations in skills, staffing, equipment and funding – was evident in many countries and across all regional groups.

"The Global Cybersecurity Index 2024 shows significant improvements by countries that are implementing essential legal measures, plans, capacity building initiatives, and cooperation frameworks especially in strengthening incident response capabilities," said Cosmas Luckyson Zavazava, Director of ITU's Telecommunication Development Bureau. "ITU's cybersecurity projects and programmes are supporting those national efforts to more effectively manage cyberthreats, and I hope that the progress demonstrated by this latest index encourages countries to do more in developing secure and trustworthy digital systems and networks."

Regional and national assessments

According to GCI 2024, the Africa region has advanced the most on cybersecurity since 2021. All world regions show improvement since the last report.

The world's least developed countries (LDCs) have also started

making gains, though they still need support to advance further and faster. GCI 2024 data shows that the average LDC has now reached the same level of cybersecurity status that many of the non-LDC developing countries had in 2021.

Land-locked developing countries (LLDCs) and small island developing states (SIDS) continue to face resource and capacity constraints on cybersecurity efforts.

GCI 2024 includes individual assessments and provides a clear status report and a roadmap of activities to make further progress on cybersecurity.

Other key findings of the GCI

Legal measures are the strongest cybersecurity pillar for most countries: 177 countries have at least one regulation on either personal data protection, privacy protection, or breach notification in force or in progress.

Computer Incident Response Teams (CIRTs) are crucial for national cybersecurity: 139 countries have active CIRTs, with various levels of sophistication, up from 109 in the 2021 index.

National Cybersecurity Strategies (NCS) are becoming more prevalent: 132 countries have a National Cybersecurity Strategy as of 2024, up from 107 in the 2021 index.

Cyber awareness campaigns are widespread: 152 countries have conducted cyber awareness initiatives targeting the general population, with some also targeting specific demographics such as vulnerable and underrepresented populations, to create a culture of cybersecurity and address potential risks.

Incentives for the cybersecurity industry continue evolving: Governments are promoting the cybersecurity industry through incentives, grants, and scholarships, aiming to enhance cybersecurity skills and foster research in the field, with 127 countries reporting some form of cybersecurity-related research and development.

Many countries cooperate on cybersecurity through existing treaties: 92% of countries (166) reported being part of an international treaty or comparable cooperation mechanism for cybersecurity capacity development, or information sharing, or both. Putting cybersecurity agreements and frameworks into practical operation remains challenging.

Capacity development and technical pillars are relatively weak in most countries. 123 countries reported having trainings for cybersecurity professionals, up from 105 in 2021. In addition, 110 countries had frameworks to implement nationally or internationally recognized cybersecurity standards, up from 103 in 2021.

Capacity development initiatives need to be reinforced: 153 countries have integrated cybersecurity into national curricula at some level, but cybersecurity trainings and awareness-raising varies widely across regions. Developing a strong domestic cybersecurity industry is essential to sustain progress.

Countries need to focus on protecting children online: 164 countries have legal measures in place for child online protection; only 94 countries reported associated strategies and initiatives, indicating a gap in implementation.

Cybersecurity assessments leading to action

As cybersecurity continues to evolve, GCI offers a clear picture of where countries are and a roadmap of activities to make progress. The report offers 11 key recommendations, from enhancing critical infrastructure to providing cybersecurity training.

GCI 2024 suggests that countries can prioritize high-impact activities, including:

- implementing legal measures applicable across all sectors;

- developing and regularly updating a comprehensive national cybersecurity strategy and a practical, concrete action plan;

- enhancing incident-response capabilities;

- delivery of capacity building and training to cybersecurity professionals, youth and vulnerable groups to strengthen cybersecurity skills;

- fostering domestic and international cooperation and collaboration on information-sharing, training opportunities, and capacity development.

ITU, the UN Agency for Digital Technologies, aims to connect the estimated 2.6 billion people who currently remain offline. Most of the globe's offline population live in developing countries, with the widest gaps in the least developed countries.

Solving the Puzzle of Protection

By Joe Morgan, Business Development Manager for Critical Infrastructure at Axis Communications

With how quickly our world has become interconnected, whether it's security, smart home devices, or social media sites, the traditional approach to security is no longer sufficient. Because threats can come from all directions, organizations now need to combine different levels of security into a cohesive and impenetrable framework, forming a resilient wall of protection.

When we speak about resiliency in security, we mean the ability to withstand attacks or recover from them. This concept of resilience is crucial as it addresses both proactive and reactive measures in security. So how do we build a toughness to either withstand or recover—or even prevent attacks that come from all directions?

Joe Morgan, Business Development Manager for Critical Infrastructure, Axis Communications

The Cyber Side

The biggest emerging threat in the cyber realm is hackers' ability to take control of critical infrastructure and change processes.

In a particularly alarming example, hackers managed to alter the water treatment process at a facility in Oldsmar, Florida to add more lye, which would have been fatal to many people had it not been caught in time.

Malware can be introduced into such systems and then stay dormant for long periods— it can activate, gather information, and then go dormant again, waiting for the best time to strike. This stealthy nature of malware makes it a persistent threat that is difficult to detect and eliminate. For how complex these attacks can be, defense is simple: systems must be upgraded and compliant. This means every device or piece of software on a network, no matter what.

Let's Get Physical

Attacks on critical infrastructure, such as chemical refineries, power grids, and oil and gas installations, are not solely cyber-based; they also come from traditional physical attacks. Specifically, there's been a rise in airborne attacks via drones. Attacks and surveillance mapping potential drone attacks have been observed in key energy sectors like substations, chemical plants, and data centers.

To defend against these kinds of attacks, organizations have had to invest in the best drone detection technology possible. Advanced drone detection systems are essential in identifying and neutralizing potential threats before they can cause harm. In addition to that, there's enhanced edge processing for our more traditional security devices like cameras. This edge processing improves optical acuity, image stabilization, low-light abilities, and overall deep learning

abilities that can adjust as necessary for whatever threat is approaching. Edge processing enhances the capabilities of traditional security cameras by incorporating AI and ML technologies. These improvements enable cameras to analyze and respond to threats in real-time, providing a crucial layer of defense against physical attacks.

Layered Protection

As we well know, cyber-attacks don't exactly wait in line for a physical attack to finish, or vice versa. This means all of these security provisions need to be layered on top of each other, and be able to exist and work simultaneously. Effective security requires an integrated approach that combines multiple layers of protection to address the full spectrum of potential threats.

Further, IT and OT are no longer separate environments. Security technology needs to consider IT and OT as a singular environment to prevent gaps in security posture, so that wide-ranging attacks that could come down on either side can be detected. Integrating IT and OT security ensures that there are no weak points in the overall security framework, providing a more comprehensive defense.

And it's not just new security technology that needs to be layered—we also need to layer new technologies in with the old, not tear everything down. This approach allows organizations to build on existing investments while incorporating the latest advancements in security technology. By integrating new tech with the old, organizations can enhance their overall security posture without incurring unnecessary costs.

This also means up-leveling employees and considering them another "layer" of the security technology system—right alongside the technology itself. When an organization integrates new tech with the old, the ability and education of the end users must be taken into account. Employee training is crucial to ensure that staff are equipped to use new technologies effectively and are aware of best practices for maintaining security.

Putting the Pieces Together

This is how we solve the "puzzle of protection." Even with a picture on the box—like knowing what

the threats might be—we still have to put together the "pieces" that will make up our protection puzzle. These pieces include new technologies, new processes, and new integration abilities, all layered together to create the defense organizations need for now and the future.

Building a resilient security framework requires a holistic approach that addresses both cyber and physical threats. By integrating multiple layers of protection, leveraging advanced technologies, and ensuring that employees are well-trained, organizations can create a robust defense system better suited to build resilience.

Power grids cybersecurity ascending to prominence

The Association of European Distribution System Operators (E.DSO), the European Energy Information Sharing and Analysis Centre (EE-ISAC), the European Network for Cyber Security (ENCS) and the European Union Agency for Cybersecurity (ENISA) joined forces for the organisation of the 7th Cybersecurity Forum.

The longstanding efforts of the European cybersecurity community regarding cybersecurity regulations for energy grids have reached a significant milestone with the implementation of various new regulations, such as the NIS2, NCCS, revised RED and CRA. Previous editions of the Forum have highlighted the expectations of stakeholders and identified challenges ahead.

Considering the recent regulatory changes, discussions focused on next steps of the implementation process, in conjunction with developments in the cybersecurity threat landscape. Key challenges to address along the way include the emergence of new sophisticated threats targeting critical sectors, such as the supply chain, and bureaucratic overload.

Experts provided real-world examples of the complex issues that need to be resolved and apply a practical approach to risk management to effectively mitigate threats, such as the development of risk management methodology. Participants' discussions also examined the establishment of the execution power required to deal with advanced attacks and rapid recovery. Industry representatives underlined the challenges of creating generic standards fit for the diverse use cases. Additionally, regulators and authorities revealed how scarce resources are constraining the speed of capacity building needed to achieve the required execution performance. A key output of the conference was the significance of effective supply chain management to prevent cybersecurity risks, especially as supply chains become longer and more complex.

The implementation of the new EU cybersecurity regulatory framework is expected to challenge end users, regulators, manufacturers and electricity sector entities and the rest of the electricity community, in their efforts to harmonise resources and create a new, cyber-secure reality. The conference concluded that adopting a results-focused, collaborative approach provides the opportunity to set a worldwide benchmark for grid system security.

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

JOIN US AT 'CIP WEEK' IN EUROPE

12th-14th November 2024, Madrid, Spain

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

With the imminent implementation of The Critical Entities Resilience Directive (CER Directive), 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. The deadline of 17th October 2024 is set for when Member States shall adopt and publish the measures necessary to comply with this Directive.

The NIS2 Directive, also known as the Network and Information Security Directive, is also a significant piece of legislation being implemented by 17th October 2024, aimed at improving cyber security and protecting critical infrastructure across the European Union (EU).

It builds upon the previous NIS Directive, addressing its shortcomings and expanding its scope to enhance 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.

In light of the forthcoming challenges with the Directives, and the ever increasing threats against European critical infrastructures, IACIPP is launching 'CIP Week' in Europe to help raise awareness and promote greater collaboration amongst operators, agencies and the CI security community.

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Project' conference as the first two events as part of the initiative.

John Donlon QPM, Chairman of The International Association of Critical Infrastructure Protection Professionals, said, "IACIPP is delighted to be hosting this new initiative in Europe, with the important aim of encouraging greater information sharing, collaboration and co-operation within the industry."

"The CER and NIS2 Directives are two of the most important pieces of legislation to arrive in Europe in recent years, and IACIPP along with other professional bodies have a degree of concern over the lack of preparation of some of the operators and agencies for the October deadline, and believe more needs to be done to ensure these minimum standards are met, and indeed exceeded in subsequent years."

"We are delighted the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Europe Project' conference are the first two events to contribute towards CIP Week, which we aim to be an annual event. Madrid is an excellent location for the launch of this program, with the CN-PIC driving Spain's efforts to meet the Directives' deadlines and be prepared." Added Mr Donlon.

Critical Infrastructure Protection & Resilience Europe (CIPRE) is the premier conference in Europe to discuss the operational threats and challenges, delivering though leadership and strategies for operators and agencies to plan security and resilience to their operations and assets.

The **EU-CIP Horizon Europe Project*** is set up to establish a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs).

IACIPP is inviting the industry to join in CIP Week in Madrid on 12th-14th November 2024.

With a leading line up of international experts speakers, from across industries, offering their experiences and expertise to highlight and inform of the challenges facing the CI industries, their interdependencies, cascading effect impacts and thoughts on collaboration to mitigate risks and threats, there is much to be discussed and learnt.

Registration Open - Early Bird Rates Currently Apply

Registration for the event is now open with Early Bird Registration Fees available until 12th October. You can book your delegate ass at www.cipre-expo.com.

Further details available at www.cip-association.org, www.cipre-expo.com and www.eucip.eu.

**The EU-CIP project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101073878*

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is a global fraternal association of CIP professionals, dedicated to sharing ideas, information experiences, technology and good practise. We continue to develop our range of activities in relation to addressing the security and resilience challenges which industry and governments face and seek to create a centre of excellence promoting communication and cooperation for all those within the infrastructure community.

Our latest and most exciting initiative to date is the launch of 'Critical Infrastructure Protection Week' in Europe as part of our ongoing activity focused towards enhancing collaboration and cooperation amongst the infrastructure industry and all relevant stakeholders.

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

In pursuance of this we see the imminent implementation of The Critical Entities Resilience Directive (CER Directive), 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. The deadline of 17th October 2024 is set for when Member States shall adopt and publish the measures necessary to comply with this Directive.

The NIS2 Directive, also known as the Network and Information Security Directive, is also a significant piece of legislation being implemented by 17th October 2024, aimed at improving cyber security and protecting critical infrastructure across the European Union (EU).

It builds upon the previous NIS Directive, addressing its shortcomings and expanding its scope to enhance 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 will be enforceable on agencies and operators for non-compliance.

In light of the forthcoming challenges with the Directives, the ever-increasing threats and the developing complexities of the threat environment against European critical infrastructure it is essential that all within the infrastructure community work together to continue to enhance the security, protection and resilience of our vital services.

IACIPP is launching 'CIP Week' in Europe to help raise awareness and promote greater collaboration amongst operators, agencies and the Critical Infrastructure security community.

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain in November 2024 and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' (CIPRE) conference and exhibition alongside the 'EU-CIP Horizon Project' 2nd annual conference as the first two major events as part of the initiative.

The CIPRE conference and exhibition events have developed significantly over the past few years providing an excellent networking opportunity for like minded individuals to get together to discuss the latest challenges and innovations across the infrastructure environment.

The combination of CIPRE and the EU-CIP Horizon Project is, I believe, the first of its kind to seek to develop and inform thinking around the current challenges and the impact of the new EU directives.

EU-CIP was launched in October 2022 and is an EU-funded project under Horizon Europe which brings together 20 partners under the coordination of Engineering Spa to establish a novel pan European knowledge network for Resilient Infrastructures.

The main goal of EU-CIP is to establish a novel pan European knowledge network for Resilient Infrastructures, which will enable policy makers to shape and produce data-driven evidence-based policies, while boosting the innovation capacity of Critical Infrastructures (CI) operators, authorities, and innovators (including SMEs).

In this direction, EU- partners have already established the European Cluster for Securing Critical infrastructures

(ECSCI), which brings together more than 40 projects that collaborate in CI Resilience. EU-CIP will leverage the achievements of the ECSCI cluster to establish an EU-wide knowledge network with advanced analytical and innovation support capabilities.

Its main objectives are to:

- Enhance Europe's analytical capability regarding research outcomes, technologies, and policies - fostering data-driven evidence based policy and innovation development
- Maximize the impact of R&I CIP/CIR activities in Europe through innovation support and solution validation services
- Establish a knowledge-hub and create a vibrant ecosystem of interested and committed stakeholders around the project's results.

The EU-CIP Project have, to date, produced a number of whitepapers (available to download from their website) that analyse critical infrastructure challenges in different sectors and propose solution guidelines. These relate to the areas of:

- Telecommunications
- Finance
- Space
- Transport

They have also introduced several community groups designed to explore, exchange, and create ideas in various key areas such as, Innovation, Project Synergies and Policy and Standardisation and launched an EU-CIP Knowledge Hub seeking to establish a new era in collaboration and knowledge sharing across the Critical Infrastructure Protection (CIP) and Critical Infrastructure Resilience (CIR) sectors.

The combination of CIPRE and EU-CIP at one event will bring together leading stakeholders from industry, operators, governments, agencies and academia to collaborate on the issues to be addressed in securing infrastructure across Europe.

IACIPP is delighted to be the initiator of 'Critical Infrastructure Protection Week' in Europe and we are grateful for the support of so many within the infrastructure community who have come together to assist us in bringing this event together.

John Donlon QPM FSyI
Chairman
IACIPP

Securing the Inter-Connected Society

Preliminary Conference Programme

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

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Project' conference.

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

Co-Hosted by: International Association of CIP Professionals

Co-located with: EU-CIP

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Supporting Organisations: PESI, EE-ISAC, ENISA, E.DSO, CCNE, CNPIC, CoESS, Help2Protect, ISIS, ASD

Platinum Sponsor: ESET Digital Security Progress. Protected

Flagship Media Partner: critical infrastructure PROTECTION AND RESILIENCE NEWS

CIPRE – Where CIIP/Cyber and Physical Security Meet

With the imminent implementation of The Critical Entities Resilience Directive (CER Directive), 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.

The NIS2 Directive, also known as the Network and Information Security Directive, is also a significant piece of legislation being implemented by 17th October 2024, aimed at improving cyber security and protecting critical infrastructure across the European Union (EU).

It builds upon the previous NIS Directive, addressing its shortcomings and expanding its scope to enhance 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.

In light of the forthcoming challenges with the Directives, and the ever increasing threats against European critical infrastructures, IACIPP is launching 'CIP Week' in Europe to help raise awareness and promote greater collaboration amongst operators, agencies and the CI security community.

Attacks on critical infrastructure sites are now a fact of life not simply a potential threat. The potential effects not only in terms of loss of life but also in terms of damage to infrastructure, economic disruption and costs, can be enormous.

We must be prepared!

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

The integrity of critical infrastructures and their reliable operation are vital for the well-being of the citizens and the functioning of the economy. The implementation of the EPCIP, under Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the need to improve their protection, has not been completely successful.

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

Why the Need for Such a Discussion?

Article 196 of the Lisbon Treaty enshrines in law that the Union shall encourage cooperation between Member States in order to improve the effectiveness of systems for preventing and protecting against natural or man-made disasters.

The Union's action shall aim to:
(a) support and complement Member States' action at national, regional and local level in risk prevention, in preparing their civil-protection personnel and in responding to natural or man-made disasters within the Union;
(b) promote swift, effective operational cooperation within the Union between national civil-protection services;
(c) promote consistency in international civil-protection work.

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 demands.

Follow us:

Critical Infrastructure Protection & Resilience Europe

Critical Infrastructure Protection / Physical Security

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

Critical Information Infrastructure Protection / Cyber Security

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

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

Why Attend?

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

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

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

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

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

Join us in Madrid for Critical Infrastructure Protection and Resilience Europe and join the great debate on securing Europe's critical infrastructure.

Who Should Attend

Critical Infrastructure Protection and Resilience Europe is for:

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

HOW TO REGISTER

1. Online at **www.cipre-expo.com.**

EARLY BIRD DISCOUNT - deadline 12th October 2024
Register yourself and your colleagues as conference delegates by 12th October 2024 and save with the Early Bird Discount.

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

- Spanish Technological Platform for Safety and Industrial Resilience (PESI)
- Europe's Distribution System Operators (E.DSO)
- Europe's Electricity Information Sharing and Analysis Centre (EE-ISAC)
- The International Emergency Management Society (TIEMS)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- Confederation of European Security Services (CoESS)

Check the Registration Fees at the back of this booklet for further details.

On-Site Registration Hours

Tuesday 12th November	1.00pm to 6.30pm
Wednesday 13th November	8.30am to 5.00pm
Thursday 14th November	8.30am to 3.30pm

Schedule of Events

Tuesday 12th November 2024

2.00pm - 3.30pm - Opening Keynote

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

4.00pm-5:30pm - Session 1: Implementation and Impacts of CER Directive and NIS2 Directive

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

Wednesday 13th November 2024

Track One

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

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

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

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

2:00pm-3:30pm - Session 4a: Transport Sector Symposium

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

4:15pm - 5:30pm - Session 5a: Power & Energy (Grid Resiliency) Sector Symposium

Track Two

9:00am-10:30am - Session 2b: Cyber Regulations, Standards and Best Practice

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

11:15am - 12:30pm - Session 3b: Critical Industries / ICS SCADA Symposium

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

2:00pm-3:30pm - Session 4b: Information Technology (CIIP) Sector Symposium

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

4:15pm - 5:30pm - Session 5b: Crisis Management, Coordination & Communication

Thursday 14th November 2024

Track One

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

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

11:15am - 12:30pm - Session 7a: Collaboration, Information Sharing and Enhancing PPPs

Track Two

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

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

11:15am - 12:30pm - Session 7b: Case Study – Training Exercise of an incident at an electrical distribution facility

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

2pm-3:30pm - Session 8: Workshop - What If: Exploring Critical Infrastructure Cascading Effects

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

Tuesday 12th November

Conference Programme

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

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

Jose Luis Perez Pajuelo, Director General, National Center for the Protection of Critical Infrastructures (CNPIC)

Dr Belda Esplegues, Director General, Port of Valencia

Senior Representative, Spanish National Cybersecurity Institute (INCIBE)*

Mayor of Madrid*

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

4:00pm-5:30pm - Plenary Session 1: Implementation and Impacts of CER Directive and NIS2 Directive

The CER and NIS2 Directives come into force in October 2024, where failing compliance could bring hefty fines, operational restrictions, or even shutdowns for critical infrastructure owner/operators. Non-compliance exposes vulnerabilities to cyberattacks and disruptions. What are the implications on the operator/owners and agencies and what impacts could there potentially be on public safety and economic stability? How has implementation gone to date and what more needs to be done?

CER and NIS2 Implementation experience, case study from Spain - Ángel Flores Alviz, Chief of the Intelligence and Coordination Service, National Center for the Protection of Critical Infrastructures (CNPIC)

Transposition of the CER Directive - Frederic Petit, Project Officer, European Commission Joint Research Centre (ECJRC)

The European Infrastructure Simulation and Analysis Center (EISAC.it) initiative: a support to the national implementation of the EU CER Directive - Vittorio Rosato, Research Associate, University Campus Biomedico Roma, Italy

NIS2 Implementation experience, case study from Romania - Senior Representative, Romanian National Cyber Security Directorate*

Implementation Challenges of NIS2 and Network Code on Cybersecurity - Anjos Nijk, Managing Director, European Network for Cyber Security, Netherlands

---

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

**invited*

Wednesday 13th November

Track One

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

The threats to critical infrastructure are like a chameleon. Cyberattacks evolve, threat of terrorism activities are on the increase, natural disasters worsen due to climate change, and new threats like drone attacks and AI manipulation emerge. This constant shift demands continuous updates to security measures. How can we identify, monitor and manage their levels of potential damage?

Consideration of Hybrid and Emerging Threats for the Resilience of Critical Entities - Frederic Petit, Project Officer, European Commission Joint Research Centre (ECJRC)

Developing threat of Drones - Juan David Nieto Sepulveda, Director of Airports and Aviation Security, AESA

Evolving Threat Landscape: Organised Crime and CI - Lina Kolesnikova, Fellow/Director of European & International Affairs, ICPEM (UK)

Cybersecurity threats and challenges - Senior Representative, ESET

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

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

Across Europe, communication networks are the lifeblood of communities and critical infrastructure. Disruptions cripple businesses and leave emergency response in chaos. With the internet central to all sectors, safeguarding communication assets and building resilience is essential for European businesses, governments, and all critical infrastructure.

Rodrigo Brito, Global Head of Cybersecurity Business line, Nokia

Alexandru Georgescu, Scientific Researcher, Department for Cybersecurity and Critical Infrastructure Protection, National Institute for Research and Development, Informatics ICI Bucharest

GOVSATCOMM Update - Senior Representative, European Union Agency for the Space Programme (EUSPA)

How can AI be used for improving cybersecurity in Critical Communications? - Aleksi Helakari, Head of Technical Office - EMEA, Spirent Communications

Track Two

9:00am-10:30am - Session 2b: Cyber Regulations, Standards and Best Practice

Escalating cyberattacks by state actors and persistent criminal activity necessitate urgent action. Robust cyber regulations, clear standards, and effective best practices are required to fortify defenses. So what are the latest regulations and how can we raise standards and standardise best practices in cyber defense?

Adrian Victor Vevera, General Director of the National Institute for Research and Development in Informatics ICI Bucharest

Luanda Domi, Cybersecurity, Governance and Security Policy Analyst, Global Forum on Cyber Expertise (GFCE)

Senior Representative, Spanish National Cybersecurity Institute (INCIBE)*

Grigore Stamatesc, ELECTRON and University Polithehnica of Bucharest, Romania

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

11:15am - 12:30pm - Session 3b: Critical Industries / ICS SCADA Symposium

Across Europe's critical industries, security practices increasingly integrate due to converging physical and cyber threats. Four main categories guide these practices: physical security, cyber resilience, personnel training, and robust supply chains. Integrating secure manufacturing (or other key processes) with resilient logistics, including IT/OT and SCADA systems, is essential for reliable deliveries and a thriving European economy.

Protecting Legacy OT Components in Critical Infrastructure from Advanced Cyberattacks: A Eurasian Resources Group Case Study - Vsevolod Shabad, Chief of Information Security Growth, Eurasian Resources Group

Redefining cyber resilience in ICS/OT - Sharon Caro, Business Strategy Executive, Salvador Tech

Safeguard-PLC: Cybersecurity in Industrial Automation - Dr Tommaso Aliberti, Cybersecurity Line Manager, NIER Ingegneria SpA Società Benefit

Threat-Intelligence based Defense-In-Depth implementation in OT environments - Matan Dobrushin, Field CTO, OTORIO

12:30pm - Delegate Networking Lunch

Wednesday 13th November

Track One

2:00pm-3:30pm - Session 4a: Transport Sector Symposium

The movement of goods and people is vital to a local and national thriving economy. Without a safe, secure and resilient transport network, an economy will crumble. The transport network, from rail, road, air and sea, is at threat from cyber attacks, terrorist threats and natural hazards and its protection and resilience is key for communities and countries to maintain their economies.

John Laene, Managing Director, RAILPOL

Pauline Mieze, Secretary General, AQUAPOL

Peter Nilsson, Head of AIRPOL

Securing a site that is both CNI and a Crowded Place - Sara Jane Prew, Senior Security Expert, Arup UK

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

4:15pm - 5:30pm - Session 5a: Power & Energy (Grid Resilience) Sector Symposium

Europe's energy sector, reliant on oil, gas, and renewables, is paramount. Without it, other critical infrastructure fails. Recent and regular cyberattacks and changing weather patterns highlight the need to safeguard our energy assets, including IT/OT and SCADA systems. How can we minimize outage or attack impacts and fortify Europe's grids?

Moderator: Aurelio Blanquet, Secretary General, EE-ISAC

Felipe Castro Barrignon, European Commission

Thomas Krauhausen, E.ON & EE-ISAC Board Member

Annkika Waegenbauer, International Stakeholder Relations Officer , Institute for Security and Safety (UNISS), Germany

Javier Simon, European Utilities Telecom Council (EUTC) & Iberdrola

Elisa Constant, VP of Research, Forescout, Netherlands

Track Two

2:00pm-3:30pm - Session 4b: Information Technology (CIIP) Sector Symposium

Safeguarding Europe's digital backbone is paramount. Information technology underpins our workforce, businesses, and access to crucial data. Robust Critical Information Infrastructure Protection (CIIP) through cybersecurity and network security is vital. Recent ransomware attacks and evolving threats like malware (Stuxnet remains a stark example) necessitate heightened vigilance to shield Europe's information assets.

Luca Tagliaretti, Executive Director, European Cybersecurity Competence Centre and Network

Conducting Impactful Geographically Scaled Critical Infrastructure Cyber Risk Assessments - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory

Andres Castillo, Head of Technological Innovation Department, Nino Jesus Childrens Hospital

TBC

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

4:15pm - 5:30pm - Session 5b: Crisis Management, Coordination & Communication

Regular exercises combined with clear communication protocols between operators and agencies/emergency responders ensure everyone's on the same page. Open information sharing creates a shared understanding of threats provide a more effective response. How do we better coordinate and co-operate to enhance protection and resilience?

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

María Luisa Moreo, General Director, Señor Lobo & Friends & Dr Francisco Pérez Bes, Partner at Digital Law, Ecix Tech, Spain

Unveiling the Power of AI: Transforming Resilience - Benjamin White, Principal Consultant, 4C Strategies

Tabletop Exercises for Disaster Resilience: Methodological Insights from Southern Germany's Rural Region - Lisa Becher, Research Assistant & Henriette Model, Project Assistant, OTH Regensburg, Germany

Thursday 14th November

Track One

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

What are some of the latest and future technologies, from ground, land or underwater technologies, access controls, and space based or cyber technology, to predict or detect the wide range of potential physical and cyber threats to CNI. How is AI being utilised in technology to enhance performance.

Underwater Security - The Unseen Threat - Simon Goldsworthy, Wavefront Systems, UK

Who's guarding access to your access control system in critical infrastructure - Richard Moser, Business Development Manager, LEGIC Identsystems

Modern security and management solutions for critical infrastructures: Access and control technologies as the key to resilience and efficiency - Senior Representative, STUV

Electromagnetic Protection of Critical Infrastructure - Senior Representative, MPE

10.30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7a: Collaboration, Information Sharing and Enhancing PPPs

Effective risk, resilience, and emergency plans rely on open information sharing across Europe. Knowledge empowers informed decisions for CI protection. How can we dismantle barriers to information exchange and foster trust between governments, operators, and communities? Stronger PPPs hinge on this collaboration.

Best practices in Public-Private Partnerships - Catherine Piana, Secretary General, Confederation of European Security Services (CoESS)

Enhancing Critical Infrastructure's Preparedness: A Comprehensive Risk Map for Strengthening Public-Private Cooperation - Jarna Hartikainen, Head of Preparedness Planning, National Emergency Supply Agency

Javier Larrañeta, Secretario General, Spanish Technology Platform on Industrial Safety (PESI)

Alvaro Rodriguez-Gaya, Manager Global Security & Investigations, American Express

Track Two

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

Proactive threat preparation significantly reduces disruptions to infrastructure and the broader community, bolstering resilience, safety and security. How can we effectively address these evolving physical and cyber threats to minimize outages and financial losses?

Physical Security of Critical Infrastructure from Terrorist Attacks - Daniel Golston, Associate Programme Officer, Organization for Security and Co-operation in Europe (OSCE)

Achieving effective, efficient, and faster post-disaster power restoration through resilience modeling - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory

Enhancing Cross-Border Risk Assessment for Critical Entity - Monica Cardarilli, Project Officer, European Commission Joint Research Centre (ECJRC)

Critical Entities Resilience Assessment to small-scale disasters - Martin Hromada, Vice-Dean for International Relations, Tomas Bata University in Zlín

Climate adaptation in critical infrastructure: A layered approach - Daniel Peregrina Gonzalez, PhD Candidate, Deltares

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

11:15am - 12:30pm - Session 7b: Case Study – Training Exercise of an incident at an electrical distribution facility

Following a technical training workshop, coordinated by Iberdrola Espana's distribution company, and personnel from the company's prevention service, in coordination with the Government sub-delegation in Valladolid, the Security Forces of Medina del Campo, the National Police, Civil Guard, Fire Brigade, Civil Protection and Local Police, we explore the outcomes of the exercise that looked at risks and prevention measures for the work that the organisations may have to carry out in the event of an emergency incident at an electrical distribution facility.

Moderated by Iberdrola

12:30pm - Delegate Networking Lunch

Thursday 14th November

2:00pm-3:30pm - Plenary Session 8:
WORKSHOP - What If: Exploring Critical Infrastructure Cascading Effects

Join us for an engaging and interactive session on the final day of CIPRE. Titled "What If," this session is designed to foster deep involvement from participants through dynamic, interactive tabletop exercises and thought-provoking scenarios.

Participants will dive into a series of hypothetical "what if" situations that challenge our preparedness and response strategies. A developing scenario that will encompass a wide range of threats including cyber and physical events, disruptions in the supply chain, hybrid threats, economic warfare, and the pressing need for climate change adaptation.

By exploring these multifaceted and interconnected threats, attendees will gain valuable insights into the complexities of protecting critical infrastructure. This session aims to enhance collaborative problem-solving skills, encourage innovative thinking, co-operation and prepare participants to better anticipate and mitigate future challenges.

Be prepared to think on your feet, work closely with fellow experts, and leave with a deeper understanding of the vulnerabilities and resilience strategies essential for safeguarding our critical infrastructure in an increasingly volatile world.

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

Monica Cardarilli, Project Officer, European Commission Joint Research Centre (ECJRC)

Frederic Petit, Project Officer, European Commission Joint Research Centre (ECJRC)

TBC

3.30pm - Conference Close

John Donlon QPM, FSI, Conference Chairman

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

Early Bird Deadline - 12th October 2024

Time	Session Title	Speakers/subject
09.00-09.30	**Registration & Welcome Coffee**	
09.30-09.45	Introductory Remarks	EU-CIP Coordinator: Emilia Gugliandolo (ENG)
09:45-10:20	Keynote Speech: ***Policy developments in the area of Critical Entities Resilience***	Sebastian Serwiak (DG HOME)
10:20-11:30	Roundtable discussion**: *Innovative Policies, Resilient Infrastructures: A Policy Dialogue*** *Moderator: Paolo Venturoni EOS*	Aljosa Pasic (SUNRISE Project) David Luengo (INDRA) Monica Cardarilli (JRC) Gerd Mueller (Secunet International) Brian Lee (ResilMesh) Luis Simon (VUB, Elcano University)
11:30-12:00	***Uptake of innovative results in the area of Infrastructure resilience***	Giannis Skiadaresis (DG HOME)
12:00-12:45	The EU-CIP-AMPLIFY Pillar: Training and Innovation Management Services	John Soldatos (INNOV)/Emilia Gugliandolo (ENG)
12:45-13:45	**Lunch Break**	
13:45-15-15	EU-CIP "Own Innovators' Pool"	Innovative solution providers EU-CIP Open Call Winners
15:15-15:45	Results of the survey & analysis of the EU Innovation Radar	Aleksandar Jovanovic (EU Vri)
15:45-16:15	**Coffee Break & Networking**	
16:15-17:00	Focus Group discussion***: Aligning Current Innovations with Practitioners' Needs in Critical Infrastructure"*** *Introduction: Rafa Company, Port of Valencia*	Breakout tables focused on various CI+ - **Transport** (Tim.Stelkens-Kobsch, DLR - **Energy** (Frederic Guyomard, EDF) - **Health Technologies** (Miguel Gaspar, ULS) - **ICT** (Cristian Patachia, Orange Romania) - **Finance (**Ramon Martín de Pozuelo, CXB) - **Resilience and safety of CI** (Gabriele Giunta, ENG)
17:00-17:30	**Conclusion presented by each table** *Moderator: Rafa Company, Port of Valencia*	ALL.
17:30-18:00	**Closing Remarks**	John Soldatos (INNOV)/Emilia Gugliandolo (ENG)
18:00-20:00	Networking reception	

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

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

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

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

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

Membership is currently FREE to qualifying individuals - see www.cip-association.org/join for more details.

International Association of
CIP Professionals

www.cip-association.org

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

The IACIPP initial overall objectives are:

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

The Association also aims to:

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

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

Networking Reception

Tuesday 12th November
5.30pm - 7:30pm

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

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

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

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

We look forward to welcoming you.

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

Event Hotel & Venue

Eurostars Madrid Congress
Parque Empresarial Omega
Avenida de la Transición Española, A-1, 22, salida 17
28108 Alcobendas
Madrid

www.eurostarshotels.co.uk/eurostars-madrid-congress.html

Located in Alcobendas, Madrid, Eurostars Madrid Congress stands out for its modern and functional spaces, endowed with excellent services to ensure the best stay for guests with the highest expectations. Very close to the Omega Business Park, The Eurostars Madrid Congress makes for the perfect hotel to host meetings and business events.

You'll find ample spaces in the hotel's rooms with sophisticated décor and plenty of details. You'll also enjoy incredible views and pleasant natural light from their imposing windows.

Accommodation

Critical Infrastructure Protection & Resilience Europe event HQ hotel for the 2024 event is the Eurostars Madrid Congress, the venue for CIPRE and CIP Week (including the EU-CIP conference).

The organisers of CIPRE have agreed a 15% discount off room rates for CIPRE and CIP Week delegates, which you can book directly with Promo Code 'CIPRE'.

Simply visit the Eurostars Madrid Congress Hotel booking link below and use Promo Code 'CIPRE' for your special room discount.

Booking link: www.eurostarshotels.co.uk/eurostars-madrid-congress.html
Apply Promo Code '**CIPRE**' for your special room discount

Registration and Participation Fees

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

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

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

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

GOVERNMENT, PUBLIC SECTOR AND MILITARY

Individual Full Delegate

Paid before 12th October 2024 .... €195
Paid on or after 12th October 2024 .... €295

OPERATORS OF CRITICAL NATIONAL INFRASTRUCTURE

Individual Full Delegate

Paid before 12th October 2024 .... €195
Paid on or after 12th October 2024 .... €295

COMMERCIAL ORGANIZATIONS

Individual Full Delegate

Paid before 12th October 2024 .... €495
Paid on or after 12th October 2024 .... €695

Sponsor/Exhibitor Full Delegate).

Paid before 12th October 2024 .... €245
Paid on or after 12th October 2024 .... €345

Student/University/Research Full Delegate

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

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

If you have registered for the EU-CIP programme only, you will not be allowed access to the CIPRE conference and will need to purchase an appropriate delegate pass.

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

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to CIP Week and Critical Infrastructure Protection & Resilience Europe 2024.

Co-Hosted by:

International Association of CIP Professionals

CIP Week Event Partner:

EU-CIP

Platinum Sponsor:

eset Digital Security Progress. Protected.

Silver Sponsor::

OTORIO

Bronze Sponsors:

EUSPA European Union Agency for the Space Programme

SALVADOR TECHNOLOGIES

Executive Sponsors:

PESI Plataforma Tecnológica Española de Seguridad Industrial

EE-ISAC

STIME

E.DSO

CCNE Crisis Communications Network Europe

ASD

Supporting Organisations:

CNPIC

CoESS

Help2Protect

NS&RC

ISIO

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Media Supporter:

Biometric Update.com

govCIO OUTLOOK

Cyber Security Review

Madrid, Spain

Spain, like many developed nations, prioritizes safeguarding its critical infrastructure (CI), the backbone of essential services like energy and communication and major players Iberdrola (energy) and Telefónica (telecoms), and the threats they face. The introduction of the CER Directive and NIS 2 Directive have been a challenge for many European nations and Spain is one of those leading their implementation in its CI protection policy and plans.

Spain's National Security Strategy (ENS) outlines the overarching framework for CI protection. It emphasizes risk assessment, prevention, preparedness, and response measures. The ENS is complemented by specific sectoral plans, like the National Plan for the Protection of Infrastructures (PNPIC), which details risk mitigation strategies for various CI sectors. Additionally, Spain actively participates in international CI protection initiatives.

The Ministry of Interior leads CI protection efforts, with its key agency CN-PIC working alongside sector-specific ministries like the Ministry for Ecological Transition and the Demographic Challenge (energy) and the Ministry of Economic Affairs and Digital Transformation (telecoms).

Operators like Iberdrola and Telefónica are responsible for implementing security measures within their infrastructure. They collaborate with the government in risk assessments, incident response planning, and information sharing.

Spain has a robust CI protection policy and plan, with government and private entities working together. However, the evolving threat landscape demands continuous adaptation. Critical infrastructure operators, play a crucial role in safeguarding Spain's essential services through robust cybersecurity measures, physical security investments, and disaster preparedness plans and an excellent location to host the 2024 Critical Infrastructure Protection Week and Critical Infrastructure Protection & Resilience conference.

We look forward to welcoming you to Madrid on 12th-14th November 2024, for the next annual gathering of the critical infrastructure and civil contingencies community at CIP Week in Europe.

Why participate and be involved?

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

Your participation will gain access to this key target audience:

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

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

How to Sponsor

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

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

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

Ray Beauchamp
(Americas)
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

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

Why participate and be involved?

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

Your participation will gain access to this key target audience:

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

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

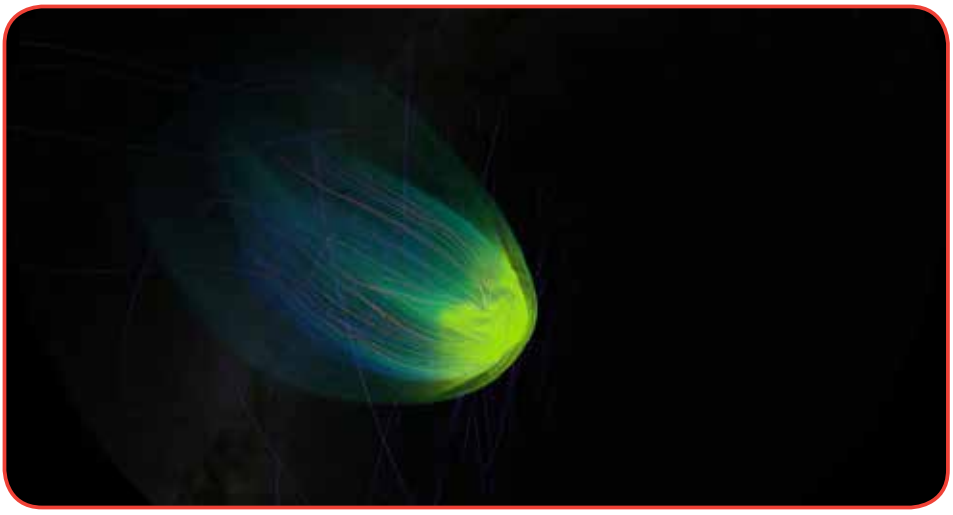
www.cipre-expo.com

Sponsorship Opportunities

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

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

Solar storms: Are we ready for another Carrington Event?



On 1 September 1859, the world experienced an improbable disruption.

British astronomer Robert Carrington first observed an intense white flare on the sun's surface, followed by a series of coronal mass ejections (CMEs), or massive bursts of solar wind and magnetic energy.

Here on Earth, the resulting geomagnetic storm produced polar-like auroras in the tropics. New Yorkers read their evening papers by the bright night sky, while gold miners in the Rockies made breakfast at 1 a.m., mistaking the Northern Lights for a cloudy morning.

Of course, the biggest impact was on electrical telegraph systems – the innovative tech of the time. Telegraphists reported sparks and even fires erupting, while transcontinental communication lines became inoperable.

To this day, it remains the largest solar storm ever recorded.

It happened five years before the International Telegraph Convention – the founding treaty for the International Telecommunication Union (ITU), whose 160th anniversary we are preparing to celebrate next year.

Yet it was just the kind of event that necessitates foresight and pre-emptive international coordination and action.

What if it happened again now?

If a solar storm of the same magnitude happened today, it could devastate our vastly more connected and increasingly digital world.

Nowadays, we depend on terrestrial telecom infrastructure, satellites, and the Internet, along with smart (digitally managed and operated) power grids, all vulnerable to geomagnetic disruptions.

A Carrington-like event today could cause high-voltage electrical transformers to overheat, leading to widespread blackouts. It might trigger long-term power outages, widespread communication failures, and crippling economic losses amounting to trillions of dollars worldwide.

Telecommunications satellites are also vulnerable to CMEs. Solar flare-ups can degrade solar panels, damage navigation systems, and alter orbital paths, potentially causing mass collisions, producing unprecedented debris, and kicking off the Kessler Syndrome you might remember from the 2013 film Gravity with Sandra Bullock and George Clooney.

British TV series COBRA, premiering in February 2020 – showed a fictional solar storm setting off massive social and political unrest.

And the COVID-19 pandemic, arriving concurrently, offered a grim reminder that disaster scenarios sometimes play out in real-life, too.

Near misses

In fact, our world has experienced its share of near misses.

A solar-induced radar blackout in 1967 set off military alerts of a nuclear attack.

Another solar storm, among the severest since Carrington, caused a nine-hour blackout in Quebec back in 1989 – before the Internet mattered so much beyond academia.

And this year's widely enjoyed Northern Lights – visible on 10-11 May from ITU's host city of Geneva, as well as further south – again reflected intense solar activity. Fortunately, digital networks escaped unscathed… this time.

Ongoing advances in technology, combined with deliberate preparedness, could mitigate the worst effects, with resilient power-grids blocking geomagnetic-induced currents and radiation-resistant satellites manoeuvring out of harm's way.

Space weather forecasting keeps improving, giving operators crucial hours or days to implement protective measures. Notably, ITU's recent World Radiocommunication Conference (WRC-23) secured future spectrum availability for such essential space and science services.

Expecting the improbable

Still, despite the known risks, preparing for a new Carrington-like event remains a challenge. Scientists estimate the likelihood of a similarly intense solar storm happening in the next hundred years at 12 per cent or less.

We cannot ignore the threat though.

Scientists also warn of rarer, yet more dangerous, superflares – massive solar eruptions that could release energy up to 1,000 times greater than the

Carrington Event. A superflare, though unlikely, could present an existential threat to humanity.

We must, in fact, brace for an array of risks.

Just a few weeks ago, the mass system failure of 19-22 July imprinted the "blue screen of death" into our collective consciousness, simply thanks to a faulty software update.

Submarine cables, which carry some 99 per cent of the world's Internet traffic, are often cut, usually by accident. Growing numbers of satellites enable advanced services for more people – but also bring new vulnerabilities. And hurricanes, typhoons, wildfires and other natural disasters, supercharged by the climate crisis, increasingly hit telecom towers, poles and other infrastructure that telecom services depend on.

Preparing together

It is essential for all of us to cooperate in building digital resilience.

ITU supports countries in developing national emergency telecom plans and strengthening their cybersecurity, including through cyber-drills.

During the recent WSIS+20 Forum, we gathered policy-makers and experts for a deep dive into submarine cable resilience, with further initiatives addressing subsea regulatory and infrastructure issues coming up soon.

ITU's first Space Sustainability Forum, taking place in Geneva on 10-11 September, will bring key stakeholders together to discuss how resilient satellite solutions could help bridge digital divide.

We must work together to protect the world's critical infrastructure. We must also agree on how to respond, fast, when incidents happen and make sure all countries are well prepared.

Ultimately, we need to act together – in solidarity – at the critical moment, safeguarding our common digital destiny and leaving no one behind.

[Source: ITU]

New Report on National Cybersecurity Governance: Ukraine

NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has published the country report on national cybersecurity governance in Ukraine as part of the National Cybersecurity Governance series.

The country report on Ukraine by Dr. Andrii Davydiuk and Prof. Oleksandr Potii comprehensively represents how legal frameworks shape national cybersecurity strategies. Examining the intersection of digital infrastructure and cybersecurity legislation highlights the crucial role of law in guiding government agencies, coordinating cyber incident responses and managing cyber crises. This study underscores the importance of robust legal structures in protecting against the evolving cyber threat landscape and ensuring national security in an increasingly digital world.

This publication is part of a series of national reports offering a comprehensive overview of cybersecurity governance by country. The aim is to improve awareness of cybersecurity management across varied national settings, supporting nations in enhancing their domestic cybersecurity governance, encouraging the spread of best practices, and contributing to the development of inter-agency and international cooperation.

Each country report outlines the division of cybersecurity roles and responsibilities between agencies, describes their respective mandate, tasks, and competences as well as any inter-agency coordination. In particular, it covers the mandates of political and strategic management; operational cybersecurity capabilities; cyber incident management; military cyber defence; and cyber aspects of crisis prevention. It offers an introduction to the broader digital ecosystem of the country and outlines national cybersecurity strategy objectives in order to clarify the context for the organisational approach in a particular nation.

Fortifying the frontline – why Zero Trust is key to national security

Cyberattacks have become the weapon of choice for adversaries operating on the national stage. A combination of agility, low cost, and the difficulty of reliable attribution makes cyber capabilities a powerful asset in any arsenal.

Unlike traditional warfare that requires getting personnel and materiel into position, cyberattacks can be launched from anywhere with little warning, making them an attractive option for nation-states and criminal groups alike. This is particularly true for nations with less developed physical military assets, as cyber warfare offers an asymmetric means to challenge more powerful adversaries.

Gary Barlet, Principal Solutions Architect, Public Sector, Illumio

Indeed, cyber capabilities hold many advantages over physical warfare, even for nations with well-developed military power. Intelligence reports assert that

Russia launched a large-scale cyberattack on Ukraine in concert with the start of its invasion.

In most cases, attribution is far muddier than overt physical action like a missile strike or a tank column rolling over the border. This means belligerents can push things much further without risk of escalation or reprisal - it's notable that we've never yet seen a cyberattack met with a physical response.

Cyber is also a much more agile proposition. High-end assets like ships and jets can take decades to go from development to deployment and take significant effort to employ, while a powerful digital weapon like a zero-day exploit may require mere days or weeks to employ with little effort.

This agility is also clear in the way the tactics of cyber adversaries are constantly evolving, with attackers employing increasingly sophisticated methods. The rise of artificial intelligence (AI) and deepfakes adds a new layer of complexity, enabling more convincing and deceptive attacks. Traditional trust-based security models are proving inadequate in this landscape, as they often fail to detect and mitigate these advanced threats.

The mounting threat to critical national infrastructure

The combination of agility, subtly and lower costs mean we have seen a surge of cyber threats on the national stage. It was recently revealed that the UK Ministry of Defence experienced a 400% increase in data breaches over the past five years. 550 incidents were reported across 2023.

Aside from the defence sector, Critical National Infrastructure (CNI) of all kinds is extremely vulnerable to cyber threats. Alongside known incidents coinciding with physical warfare as seen in Ukraine, we have witnessed a growing number of serious attacks on CNI around the world. Jeanette Hanna-Ruiz, former CISO of NASA, reported a 70% increase in incidents in recent years.

The energy sector is a particularly vulnerable target. Last year, Denmark suffered its largest cyberattack to date when 22 companies linked to its energy sector were attacked. While initially believed to be the work of notorious Russian advanced persistent threat (APT) group Sandworm, the perpetrators are currently unconfirmed.

The Colonial Pipeline attack remains one of the most prominent CNI cyber incidents, with widespread disruption to fuel supply across the US showing just how vulnerable the sector is to cyberattacks.

Similarly, the Royal Mail attack in the UK caused significant disruption to its overseas services. These incidents demonstrate how cyber adversaries can exploit vulnerabilities to cause widespread disruption and economic damage.

It's worth noting that larger military bases are typically structured like miniature cities, including their own CNI such as energy and water supplies. As such, many bases are also vulnerable to cyber threats targeting this infrastructure, posing an added threat to national security.

Still, most western nations have been lucky so far. Although these incidents were disruptive and costly, there have so far been very few truly catastrophic CNI attacks with widespread consequences. With international tensions continuing to run high, it may be only a matter of time until a serious attack devastates a country. That is, unless security is significantly improved.

The challenges of expansive and aging infrastructure

Maintaining cyber resilience in the defence and CNI sectors is fraught with challenges, with one of the most significant being the far-reaching presence of legacy technology. Both sectors are riddled with assets that were not designed with modern cybersecurity threats in mind. These outdated systems

are integral to many operations, yet their replacement is complex and costly, creating a persistent security gap that cyber adversaries can exploit.

When I served as Squadron Commander at an Air Force base, one of my greatest security concerns was the high level of interconnectedness between everything on a base's network.

You can count on critical assets like weapons systems to have a high degree of security defences in place. But supporting elements like power supply and temperature control might not be so well secured. And they all share the same network. The same is true in many CNI sectors which rely heavily on cyber-controlled physical systems.

The complexity of replacing outdated systems further compounds the issue. Defence infrastructure is particularly vast and interconnected, making the integration of new technologies without disrupting operations a formidable task.

The extensive use of third-party providers and supply chains also introduces additional risks. Many third-party vendors may not adhere to the stringent security standards required, creating weak links in the defence sector's cybersecurity framework.

Implementing modern security protocols around older systems can significantly enhance their security. This includes incorporating advanced encryption methods, secure authentication processes, and robust access controls. Strong network segmentation is particularly valuable here. Ring-fencing legacy tech works both ways, preventing it being used as a weak point to access the wider network, and stopping attackers reaching and disrupting critical systems. By surrounding legacy systems with modern security measures, organisations can mitigate the risks associated with these older technologies.

A thorough security assessment of third-party providers is also crucial. Conducting regular audits and continuous monitoring of these providers' systems ensures that they comply with the necessary security protocols, thereby minimising potential vulnerabilities.

The age of AI deception

As well as the need to drag aging infrastructure up to modern IT security standards, there is a significant risk from fast-moving new technology. In particular, AI has come to define the latest generation of digital threats.

The meteoric rise of AI is a double-edged sword when it comes to global security. While AI can act as a force multiplier, enhancing military capabilities and efficiency, it also poses significant risks when leveraged by adversaries. The defence sector is actively exploring ways to integrate AI into their systems, but they must simultaneously defend against AI-driven threats.

Deceptive AI is one of the most concerning risks here, especially when it comes to convincing audio and video deepfakes. Deepfake-powered fraud targeting consumers is a growing concern, and there have been more elaborate incidents involving high-level business decision makers.

But in a military context, this threat is even more dire. Imagine a scenario where troops receive a video call from what appears to be a commanding officer issuing critical movement orders that could bring them into harm's way. Or a missile emplacement receiving apparently genuine orders to fire on the wrong target; these are only some of the nightmarish outcomes.

The idea of adversaries manipulating our cyber capabilities and turning them against us was one of my greatest concerns during my military career, and the risk has grown significantly since then.

As the technology continues to evolve in leaps and bounds, the challenge of validating the

authenticity of such communications grows more daunting. How can personnel ensure they are truly speaking to their chain of command and not being deceived by sophisticated AI? Even if attempted deceptions are caught, their possibility will sow doubt in the legitimate chain of command.

Identity is key

From legacy tech and sprawling third-party supply chains, to the latest in AI doppelgangers, many of the cyber threats on the national stage come back to the same issue: identity.

Most cyberattacks are intrinsically linked to deception, regardless of whether it's an everyday breach involving stolen network credentials, or our nightmarish future scenario of deepfake battlefield orders. As such, the ability to quickly and accurately verify identity is key to defending against these attacks.

On the national stage, we're seeing a strong push towards the Zero Trust model as a way of achieving this identity security on the large scale needed. The Biden Administration in the US has been a leading force here, issuing an executive order in 2021 that included Zero Trust architecture among a raft of mandatory measures for federal government organisations. The NSA has been issuing on-going guidance to help organisations and governmental entities get to grips with the model.

The Zero Trust approach is a fundamental shift in cybersecurity, moving away from the traditional perimeter-based security approach to an adaptive strategy that is suitable for today's dynamic IT environment.

A central pillar of Zero Trust is Zero Trust Segmentation (ZTS), which divides the network environment up into sections with access governed by Zero Trust principles. This means every access request is explicitly verified, regardless of whether it originates from inside or outside the network. As a result, lateral movement is limited and prevents attackers from moving freely once they gain access.

At its core, Zero Trust operates on the principle of "never trust, always verify." This is a critical approach for both the CNI and defence sectors, which typically include complex and sprawling infrastructures that pose many opportunities for threat actors to hide and move unseen.

It also enhances the protection of interconnected assets, ensuring that critical infrastructure components remain secure even if other parts of the network are compromised. This comprehensive approach is essential for defending against sophisticated cyber threats targeting our defence and critical infrastructure.

Applying a 'least privilege' approach is fundamental to segmentation. It ensures that users and systems are granted only the minimum level of access necessary to perform their functions, thereby reducing the attack surface.

Zero Trust is also closely tied to the principle of assume breach, which acknowledges that no system is entirely secure, prompting continuous vigilance and preparedness for potential threats. This reframes the idea of a security breach from being a shocking worst case scenario, to an expected outcome. When it comes to matters of national security, being ready to tackle a breach immediately is a huge asset.

Getting moving with Zero Trust

A widespread Zero Trust implementation is a big undertaking and cannot be accomplished in a single stroke. Any organisation pursuing the model should anticipate going through several stages and gradually progressing through each step. Fortunately, this is now a well-mapped journey, with frameworks like CISA's Zero Trust Maturity Model providing useful guidance. It's also worth noting that each of the phases will themselves help to increase visibility and resilience against threats while the

implementation is under way.

The first step is mapping out the entire network to identify all assets, users, and data flows. This comprehensive understanding of the network's structure is crucial for effective monitoring and control. There must be a clear picture of where the biggest risks are, and the paths that could be used to reach them. Simply put, you can't defend what you can't see.

One of the biggest mistakes we see in organisations pursuing Zero Trust is to attempt a one-size-fits-all. This rarely works out for the average business and will absolutely fail for sectors as diverse as defence and CNI. Each branch of the military works very differently, with its own unique structure and priority. Likewise, while areas like energy and water treatment have similarities, they cannot be expected to follow the same plans. Each area must have its own bespoke strategy.

Next, network segmentation is another critical component, creating isolated environments within the network to contain potential breaches and limit the movement of attackers. By breaking the network into smaller, manageable segments, any intrusion can be quickly identified and contained, preventing widespread damage.

Strong access controls are essential, enforcing the principle of least privilege to reduce the attack surface. Implementing multi-factor authentication for sensitive systems adds an extra layer of security, making it significantly harder for attackers to gain unauthorised access.

Finally, advanced monitoring tools, powered by AI and machine learning, play a crucial role in detecting and responding to anomalies in real-time. These tools can identify unusual patterns and potential threats faster than traditional methods, enabling a swift and effective response.

The result will be a network environment that is far more resilient to initial intrusion. And even when attackers do get through, they will find it far more difficult to reach their goals and cause any real damage and disruption. This is especially valuable for fields like defence and CNI where attackers are counting on hitting fast and hard.

Cyber resilience will only grow more important

As cyber threats continue to evolve, national defence demands a proactive and comprehensive cybersecurity strategy. Implementing a Zero Trust approach is an essential part of enhancing cyber resilience, ensuring that critical national infrastructure can withstand and recover from attacks.

By continuously verifying identities, enforcing least privilege access, and employing advanced monitoring tools, organisations can significantly reduce their vulnerability to sophisticated threats.

Even with a strong Zero Trust strategy in place, the job isn't over yet – in fact it's never really over. Building security isn't the same as building a house – you can't get the walls and roof up and consider it done. Effective security requires a continual effort, which in this case means regularly auditing the Zero Trust implementation and looking for issues and areas to improve as the threat landscape shifts.

With both state-backed actors and opportunistic criminal gangs circling national infrastructure in search of weak points, continually improving resilience against cyber threats must be a top priority.

World Border Security Congress

25th-27th March 2025

Madrid, Spain

www.world-border-congress.com

Patrolling the Periphery - Developing Border Strategies Through Co-operation and Technology

Co-hosted and Supported by:

GOBIERNO DE ESPAÑA | MINISTERIO DEL INTERIOR

SAVE THE DATES

Spain's vast coastline and strategic location between Africa and Europe present unique challenges for the National Police and Guardia Civil.

Spain faces a constant influx of migrants seeking a better life in Europe. The Canary Islands and the enclaves of Ceuta and Melilla, bordering Morocco, are popular entry points. Patrolling these vast stretches, especially maritime borders, requires significant resources.

Spain is also a key entry point for hashish from Morocco and cocaine from South America destined for other European countries. The decentralized nature of trafficking groups makes it difficult to infiltrate and dismantle them.

The country, and region's, border security landscape is constantly evolving. By addressing these challenges through international collaboration, innovative technologies, and strategic resource allocation, the international border security community can strive towards a more secure future.

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 Madrid, Spain on 25th-27th March 2025 for the next gathering of international border security, protection and migration management professionals.

www.world-border-congress.com

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

Ray Beauchamp
Americas
E: rayb@torchmarketing.co.uk
T: +1 408-921-2932

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

for the international border management and security industry

Supported by:

European Association of Airport and Seaport Police | African Union | ISIO | International Association of CIP Professionals | HS&RC

Media Partners:

World Border Security Network | Border Security Report | World Security-Index.com

EU Space goes global

Demand for space-based applications is growing – and growing fast. In fact, over the course of the next decade, GNSS and Earth Observation combined global revenues are set to increase by nearly EUR 330 billion.

This is great news for the EU, whose economic recovery and resilience stands to benefit from the market uptake of EU Space technologies, and for the many citizens and businesses who rely on space-based data and services.

But why should these benefits be limited to the EU?

"While the technology may be European, the benefits of EU Space are clearly global," says EUSPA Executive Director Rodrigo da Costa. "That's why EUSPA is committed to bringing EU Space data and services to international markets."

At the centre of this commitment is Horizon Europe, the EU's funding programme for research and innovation.

"Through our Horizon Europe funded projects, EUSPA links the downstream space expertise of Europe with SMEs and universities around the world," adds da Costa. "In doing so, we not only foster further investments in EU Space, we also create new opportunities for EU space-based companies."

Copernicus at work in Chile and Colombia

One of those international projects is COMUNIDAD, which is dedicated to developing integrated solutions based on European GNSS and Copernicus for users in the Community of Latin American and Caribbean States (CELAC).

With a focus on Chile and Colombia, the Horizon Europe project is building regional capacity for processing Sentinel data and using Copernicus products and services to support the agriculture, forestry, and rural development sectors. For example, in Chile, a pilot will use Copernicus data to monitor snow cover changes in the country's Patagonia region.

"Variability in snow coverage has a direct impact on how water is allocated for drinking and agriculture, and the insights provided by this pilot will support local and national decision makers in implementing climate adaptation strategies," says Dr Gerard Olivar-Tost, a professor at Chile's University of Aysen, one of the project's partners.

A second pilot, set to take place in Colombia's Caldas region, will use Sentinel data to identify the distribution of coffee crops and other vegetation. This information will help decision makers both assess an area's suitability for cultivation and forecast harvest yields.

"The ultimate goal is to understand how extreme weather events impact the coffee production and, based on this understanding, implement effective adaptation and disaster risk management strategies for small Colombian coffee growers," explains Dr Juan Rodrigo Sanz Uribe, Head of Engineering and Senior Researcher at the Coffee Research Centre of Colombia, another of the project's partners.

The project also looks to establish an 'EU-CELAC Knowledge Area' by fostering research and innovation cooperation, promoting the use of new technologies, and facilitating technology transfer to support sustainable socio-economic development.

How about a little sugar with your space?

Another Horizon Europe project linking EU Space with Latin America is DINOSAR. The project is developing an operational diagnostic tool based on multi-sensor Copernicus data to consistently monitor sugarcane crops in Colombia.

"By helping farmers match fertiliser, pesticide and water use to a crop's actual needs, our solution will make sugarcane cultivation more sustainable and environmentally friendly," says Carlos Mosquera, CEO at C.I. AGROAP SAS, one of the project's partners.

While the actual work may be happening in the sugarcane fields of Colombia, DINOSAR's impact will have a global reach. After all, sugarcane is the world's largest crop by volume. "We aim to scale up our solutions so sugarcane farmers around Latin America – even the world – can use Copernicus data to make informed decisions about water, fertiliser and pesticide use," adds Corné van der Sande, Project Manager and Service Developer at eLEAF, the project's coordinating partner.

"Using European space solutions to support local sugarcane farmers in Colombia, the findings of which could benefit agricultural stakeholders here in Europe and around the world – that's just a taste of what we can achieve when EU Space goes global," concludes da Costa.

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

Are you sure your national infrastructure is secure?

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.

Invitation to Participate

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety.

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

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

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

As we come out or one of the most challenging times in recent history, off the back of a pandemic, it has stressed how important collaboration in protection of critical infrastructure is for a country's national security.

Join us in Houston, Texas, USA for the premier event for operators and government establishments tasked with managing the region's Critical Infrastructure Protection and Resilience.

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

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

To discuss exhibiting and sponsorship opportunities contact:

Ray Beauchamp
(Americas)
E: rayb@torchmarketing.co.uk
T: +1 408-921-2932

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

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

International Association of CIP Professionals

Help2Protect

ISIO - International Security Industry Organization

Flagship Media Partner:

critical infrastructure PROTECTION AND RESILIENCE NEWS

An Interview with E.DSO

Ben Lane, CIPRNA event manager, met Charles Esser, Secretary General at European Distribution System Operators (E.DSO)

E.DSO is the key interface between Europe's Distribution System Operators (DSOs) and the European institutions. E.DSO gathers 36 leading electricity DSOs in 19 countries, including 2 national associations, cooperating to ensure the reliability of Europe's electricity supply for consumers and enabling their active participation in our energy system.

Ben Lane (BL): I am the event manager of the Critical Infrastructure Protection & Resilience Europe (CIPRE) Conference. The next event is in Madrid in November (12-14). We are going to talk today about you and why you are here, and then, we're going to talk a little bit about E.DSO and some of the broad tasks that you have as an association in relation to your members and your wider work outside your members.

Charles Esser, Secretary General, European Distribution System Operators (E.DSO)

Charles Esser (CE): Certainly. I'm glad to be here and glad that E.DSO is involved in CIPRE.

BL: Tell us a little about yourself, Charles, just a short recap on your

career and how you've ended up in this position as Secretary General of E.DSO.

CE: I started at E.DSO as Secretary General at the end of last year, in December. Before that, I worked on the regulatory side. So, I worked for the Regulators Association in Europe, CEER. And there, I was Secretary General for four and a half years. And before that, I worked for that association on distribution system operators and on retail energy markets. So, I've been in the Brussels association area for about seven years.

I previously worked at the International Energy Agency and as a self-employed consultant. Before that, I worked for an NGO think tank, in energy analysis, but it was more on the political aspects of the sector. And so, here I am. For me, it is interesting to move from the regulatory side to working directly for an association of regulated utilities.

BL: So, there's a transition point in your career; you went from the regulatory side to the association side. Maybe that's a good place to start to introduce why you made that change and what your role now is, specifically at E.DSO.

CE: When I worked for the Regulators Association, previous to being Secretary General, I worked on DSOs. So instead of advocating for regulators' concerns, I change to advocating for regulated companies' concern. However, I think that both regulators and regulated companies agree that distribution system operators are working in the public interest, they are

natural monopolies, and so, they understand that they need to be regulated and that there are restrictions on things that they can do, compared to a purely competitive company.

Also, there are a lot of things to do running an effective Brussels-based association that are similar, no matter what the area. So, I think those are things that have been a naturally easy transition. And I think we're at a phase now where distribution system operators, or grids more generally, are seen as vital to the energy transition. I'm excited to have made the change and I feel like it's important to have a regulatory presence in Brussels and a presence of the regulated companies to get the kind of good policies that we all want from Brussels.

BL: Now, you are working as Secretary General for E.DSO. You've got some tasks. I'm sure there were some big tasks on your desk when you first arrived. Maybe explore some of those tasks and roles and responsibilities that you have as an association now and what you need to do to represent your members correctly. What is your day-to-day role?

CE: I manage a secretariat of about nine people. One of the things we do is advocacy. It's about making our voice heard in Brussels. It's about working with other associations that have similar views or even interacting with associations that may have different views and trying to persuade them or understand their point of view. I spend part of my time thinking and working with our policy and regulation committee to make sure we have solid defensible positions on different pieces of legislation. We are at a phase where our members will have to implement European legislation. Some of it may need to be transposed and, of course, that's a job for the legislature in the Member State.

It's also about looking for ways to cooperate and push forward our views or cooperate with other DSO associations or with associations representing other related industries in the energy sector.

We, as electricity-only DSOs,

strongly support electrification and continued electrification and working towards the targets that have been set in National Energy and Climate Plans (NECPs).

I think another vital part of E.DSO's work is European projects that we participate in, like the Horizon programme, but also sometimes from other programmes, like Erasmus. And so, we directly participate in consortia, and we usually have at least one or two of our members participate in the same consortium with us. In that way we can diffuse the knowledge from these projects to our members. We often have a dissemination role because we are an association, rather than just one DSO. But sometimes, we also carry out more technical tasks within consortium.

We have a committee that discusses and looks at those projects. We try to look ahead at projects that we might want to apply for. And we also play a role in knowledge sharing between our members. I should say that as distribution system operators are natural monopolies, our members don't compete among themselves. This allows for a great deal of knowledge sharing between our members on all kinds of topics.

And indeed, the topic perhaps of interest most to CIPRE is that we have a task force within our technology and knowledge sharing committee on cybersecurity, and they work on sharing knowledge on the latest developments in cybersecurity, best practices and thinking about the levels of investment needed. As regulated companies, of course investment levels are approved by the regulator, so this is part of the ongoing discussion.

BL: You touched on the point in terms of security and in terms of the CIPRE event, which is our topic here so what are the key items now, in terms of the transposition to NIS2 that maybe is keeping you awake at night?

CE: As the transposition continues, our members have looked at the topic and certainly thought about some issues that should be brought to the attention, in terms of transposition and what happens after transposition. And so, I would say there are a few things. One is, as we have implementation, we may need an ever more transverse kind of skillset in operators such as compliance experts, risk management.

We need more intense cooperation from different internal departments fostered by top management that defines compliance and with external regulators who attest to compliance. We also may have different views on what are operators of essential services. These may vary from member state to member state, and the threshold can be different or the criteria, so that's something to manage, and particularly there'll be some heterogeneity within Europe, and so, we'll need to adopt a very global approach. That means going beyond just the electricity sector and moving into other sectors.

We think NIS2 will have a very large perimeter; we've seen many thousands of entities concerned by the directive. We think another issue too is that there are other pieces of legislation that are related to NIS2 such as Network Code on Cybersecurity, the Critical Entity Resilience Directive, etc. that must be considered in implementation. Another essential question is, how will all levels of the supply chain cope with increased security standards? This is a concern. For DSOs, how do our members really function in this new landscape? That's an interesting point for us. Also, as regulated companies, the tariff does not define exactly how much spending there should be on cybersecurity, so how do we

communicate to the regulator exactly how much spending there should be on cybersecurity, how to defend that, how to make sure that the regulator understands everything that's involved with that? Perhaps we need some kind of cost model, but that's still to be discussed.

BL: Thank you. I think the last thing you wanted to talk about was your upcoming Cybersecurity Event.

CE: This year's E.DSO is co-organising the seventh edition of our Cybersecurity Forum. It is organized by us and the European Energy Information Sharing and Analysis Centre, EE-ISAC, the European Network for Cybersecurity, ENCS, and the European Union Agency for Cybersecurity, ENISA. This event will take place in Brussels on the 1st of October 2024. It will be in person only. We will be looking at questions such as, how can European regulations on cybersecurity be developed in a harmonized way? I talked a little bit about that just now. Also, under discussion is how we manage risks, avoid gaps, overlaps, and what's expected from different stakeholders in cybersecurity. How can resilience be assured? Resilience is a really important issue for us as DSOs, whether it's climate change or cybersecurity, and ensuring that kind of resilience is important. It's important to the grid, important to keep the lights on. It's important to competitiveness globally. So, we're excited to hold this forum on the 1st of October, and we cordially invite interested people to register to attend at: https://www.edsoforsmartgrids.eu/events/e-dso-ee-isac-encs-enisa-7th-cybersecurity-forum-from-theory-to-practice-how-do-we-get-it-right-how-do-we-get-it-right-in-time/

BL: That's a great roundup. See you in October at your event in Brussels, and CIPRE 2024 in Madrid.

Five Eyes cyber leaders provide threat briefing

Cyber security leaders from the Five Eyes intelligence alliance have made a rare joint appearance in public to provide a briefing on the evolving cyber threat landscape.

Felicity Oswald, CEO of the National Cyber Security Centre – a part of GCHQ – was joined by counterparts from Australia, Canada, New Zealand and the United States on a panel session at the Aspen Cyber Summit.

Speaking at the event in Washington DC, Ms Oswald outlined how partnerships with international allies, industry and academia are central to the UK's approach to driving up cyber resilience and countering the threat from online attackers.

She discussed how the global threat picture remains unpredictable due to the increasing range of actors using cyber capabilities and how working with partners is helping the UK to tackle common challenges at scale - from managing the quantum threat to cryptography to the cyber skills gap.

The need for critical infrastructure networks to have a strong security baseline was also highlighted, given the particularly sophisticated threats posed by nation state attackers, in addition to cyber criminal activities and state-aligned actors.

NCSC CEO Felicity Oswald said, "It is great to meet with counterparts from the Five Eyes intelligence alliance, which continues to deliver tangible benefits for our nations' cyber security.

"In cyberspace, where there are no borders, collaboration with likeminded partners and allies is essential for driving up our collective cyber resilience in an ever-changing world.

"We are committed to sharing insights into the cyber threats we face and working together to identify solutions to tackle common challenges."

Protecting electric grid health with drone-based power line inspection

By Oak Ridge National Laboratory

A sensor on the electric grid picks up a strange blip in current or voltage. What's happening, and will it cause an outage? Usually, a utility worker must travel in person to check. Researchers at the Department of Energy's Oak Ridge National Laboratory have developed a new automated drone inspection system that can respond rapidly to unusual electric grid behavior, especially in remote areas that are tough for a worker to reach.

ORNL demonstrated the new approach at a training facility for powerline workers owned by utility partner EPB of Chattanooga in Tennessee. A recording of popping sounds, like those made by an arc of superheated electricity, started the exercise. In moments, a drone lifted into the air, following GPS coordinates to check for problems.

Hovering near power lines, the drone filmed the equipment with a tiny camera and then called other drones carrying high-resolution acoustic sensors, radio frequency sensors or other specialized equipment. The drones livestreamed their inspection back to the EPB's command center and ORNL's linked Grid Operations and Analytics Laboratory in Knoxville. The drone-mounted sensors can collect enough information for the utility to decide whether to dispatch a bucket truck for urgent

maintenance to prevent a power outage.

The demonstration proved that humans don't have to be directly involved with this level of grid monitoring, said lead researcher Peter Fuhr, who also leads the Grid Sensing and Communications group at ORNL. Drone-based sensors could pinpoint problems faster.

EPB is interested in implementing the approach because accurate, early recognition of electric line malfunctions can prevent outages and save money. "The biggest opportunity is identifying imminent equipment failure," said Jim Glass, assistant vice president of Smart Grid Operations for EPB. "Just as with your health, if you catch problems early, you can correct them with less expense and difficulty. Proactively addressing problems before customers experience outages provides tremendous benefit."

The automated drone inspection and its technology are part of a collaborative project called Autonomous Intelligent Measurement Sensors and systems, or AIMS, funded by DOE's Office of Electricity. ORNL researchers developed the system for using machine-to-machine communications to automatically sense problems, generate work orders and coordinate multi-stage drone inspection of electrical transmission equipment. The project also supports processing the drone data and images so they are useful in rapid decision making.

AIMS customizes off-the-shelf drones, sensors and software

along with new technology, algorithms and automated protocols developed by ORNL. Using commercial technology when possible makes the approach practical and affordable for electricity providers.

"This is completely novel to the utility world," Fuhr said. "No one has put this together as a holistic system before. We're taking these components and operating them in a very different way, tailoring the math, hardware and software to the needs of utilities."

In the cases when commercially available products were not affordable for use across a utility system, the ORNL team designed new technology. For example, ultraviolet cameras for the drones were priced at $25,000 and weighed 10 pounds. ORNL researchers invented a combination visual/ultraviolet/invisible light sensor that's less than 1 percent of the cost and weighs less than a pound, Fuhr said.

Here's how the inspection process works: Sensors mounted on power lines and transformers throughout the grid trigger the process when they collect information. The utility's centralized management system can automatically compare these readings of current and voltage with waveforms in the Grid Event Signature Library, a vast DOE repository of grid data maintained by ORNL. When irregular activity is identified, a ground control unit can be automatically directed to send a scout drone from an electrical substation. The system can decide which drone is the closest with the appropriate range and battery charge.

The scout drone uses global positioning coordinates to locate and check the area with a radio frequency sensor, visual and infrared cameras and a simple sound detector. The drone can monitor its own battery, dodge obstacles such as trees and power lines, record readings and convey them in real time using wireless or cellular networks – or in the case of the demonstration, via EPB's fiber optic network.

Based on information collected by the scout drone, the ground control system can send other drones equipped with more

specialized inspection capabilities. Fuhr compares the scout drone to an emergency room triage nurse. "You show up at the ER intake, where a person evaluates your condition and decides if you need a specialist," he said. "This works the same. The scout decides what type of measurement is needed based on whether there is electrical arcing, a cracked fuse or a branch on a power line."

Sensor data from the drones, as well as their location and operating status, could be relayed to the central control system in real time. Researchers are working on ways for this processing to occur near the drone, such as at a substation, reducing drain on the battery as well as the risk of interrupted communications. Quantum-based communication will generate random keys that encrypt access to the sensor data and protect drone controls, Fuhr added.

Although this inspection approach is designed to operate independently of human intervention, a built-in override function allows a person to immediately land the drones or send them back to their chargers.

ORNL researcher Elizabeth Piersall adapted the sensor components and developed control software for thedrone and cameras. She also created algorithms to recognize dangers to power equipment that are visible in the video feed. "We want to understand how to use these sensors to accurately identify active arcing, even when dealing with potentially poor resolution and motor vibration from affordable sensors and drones," she said. To train these models, Piersall has been able to use a vast trove of drone video taken during routine power line inspections through an earlier EPB partnership with the University of Tennessee at Chattanooga.

Fuhr envisions a fleet of drones, each equipped with a different sensing capability, on standby at wireless chargers in substations. EPB has about 100 substations covering 600 square miles of service area, but Glass said he envisions equipping the 20 largest substations first and then adding more as needed. Outfitting substations with the affordable drones ORNL identified would be much more economical than the cost of sending trained line workers in a bucket truck to check far-flung electric lines and equipment.

Glass said EPB has an equal interest in using drones for both routine and emergency line inspection after storms. "The first step in restoration efforts after a major weather event is to assess where the most severe damage is, and drones could be a huge advantage in that."

Piersall noted that although utilities have thousands of stationary sensors on the grid, those don't offer an easy way to see elevated equipment close up while it's operating. "This provides a perspective on the information that utility specialists may not have otherwise," she said. "We are not just finding a better way to do something that can be done already: We are providing a new capability."

ORNL researchers Gary Hahn, Ali Ekti, Bill Monday, Jason K. Richards, and Ozgur Alaca and University of Tennessee students Emma Foley and Stephanie Tomasik also contributed to the research, which is funded by DOE's Office of Electricity.

UT-Battelle manages ORNL for the Department of Energy's Office of Science, the single largest supporter of basic research in the physical sciences in the United States. The Office of Science is working to address some of the most pressing challenges of our time.

CISA Releases Plan to Align Operational Cybersecurity Priorities for Federal Agencies

The Cybersecurity and Infrastructure Security Agency (CISA) has published the Federal Civilian Executive Branch (FCEB) Operational Cybersecurity Alignment (FOCAL) Plan. As the operational lead for federal cybersecurity, CISA uses this plan to guide coordinated support and services to agencies, drive progress on a targeted set of priorities, and align collective operational defense capabilities. The end result is reducing the risk to more than 100 FCEB agencies.

Each FCEB agency has a unique mission, and thus have independent networks and system architectures to advance their critical work. This independence means that agencies have different cyber risk tolerance and strategies. However, a collective approach to cybersecurity reduces risk across the interagency generally and at each agency specifically, and the FOCAL Plan outlines this will occur. CISA developed this plan in collaboration with FCEB agencies to provide standard, essential components of enterprise operational cybersecurity and align collective operational defense capabilities across the federal enterprise.

"Federal government data and systems interconnect and are always a target for our adversaries. FCEB agencies need to confront this threat in a unified manner and reduce risk proactively," said CISA Executive Assistant Director for Cybersecurity, Jeff Greene. "The actions in the FOCAL plan orient and guide FCEB agencies toward effective and collaborative operational cybersecurity and will build resilience. In collaboration with our partner agencies, CISA is modernizing federal agency cybersecurity."

The FOCAL plan is organized into five priority areas that align with agencies' metrics and reporting requirements. Each priority has goals ranging from addressing universal cybersecurity challenges such as managing the attack surface of internet-accessible assets and bolstering cloud security to long-rage efforts including building a defensible architecture that is resilient in the face of evolving security incidents. The priority areas for FCEB agencies are:

- **Asset Management** – fully understand the cyber environment, including the operational terrain and interconnected assets.

- **Vulnerability Management** – proactively protect enterprise attack surface and assess defensive capabilities.

- **Defensible Architecture** – design cyber infrastructure with an understanding that security incidents will happen, and that resilience is essential.

- **Cyber Supply Chain Risk Management (C-SCRM)** - quickly identify and mitigate risks, including from third parties, posed to federal IT environments.

- **Incident Detection and Response** - improve the ability of Security Operations Centers (SOCs) to detect, respond to, and limit the impact of security incidents.

The FOCAL Plan was developed for FCEB agencies, but public and private sector organizations should find it useful as a roadmap to establish their own plan to bolster coordination of their enterprise security capabilities.

The Plan is not intended to provide a comprehensive or exhaustive list that an agency or CISA must accomplish. Rather, it is designed to focus resources on actions that substantively advance operational cybersecurity improvements and alignment goals.

EPA Urgently Needs a Strategy to Address Cybersecurity Risks to Water and Wastewater Systems

The water sector faces increasing cybersecurity-related risk. While national reporting requirements for cyber incidents are being developed, known incidents have disrupted water sector operations. Nations (including Iran and China), cybercriminals, and others have targeted water systems. For example, foreign hackers targeted multiple water systems in late 2023. Cyberattacks threaten public health, the environment, and other critical infrastructure sectors.

A cyberattack on U.S. drinking and wastewater systems could, for example, produce drinking water with unsafe levels of bacteria or chemicals. Nations, cybercriminals, and others have targeted some of the nearly 170,000 U.S. water systems, which are increasingly automated.

EPA leads water cybersecurity efforts. It has worked with the water sector to improve cybersecurity. However, EPA hasn't identified and prioritized the greatest risks sector-wide. It also relies on water systems to voluntarily agree to improve cybersecurity.

Water and Wastewater Systems' Vulnerability to Cyberattacks

Federal agencies and other entities have acted to improve water sector cybersecurity, but reported

challenges such as workforce skills gaps and older technologies that are difficult to update with cybersecurity protections. Further, the sector has made limited investments in cybersecurity protections because water systems prioritize funding to meet regulatory requirements for clean and safe water, while improving cybersecurity is voluntary. In a May 2024 alert, the Environmental Protection Agency (EPA) said it planned to increase enforcement activities to ensure drinking water systems address cybersecurity threats.

EPA has assessed aspects of cybersecurity risk but has not conducted a comprehensive sector-wide risk assessment or developed and used a risk-informed strategy to guide its actions. EPA is required by law, as well as National Security Memorandum 22 (NSM-22), to identify, assess, and prioritize water sector risk. EPA official said they have assessed threats, vulnerabilities, and consequences, but have not integrated this work in a comprehensive assessment. Without a risk assessment and strategy to guide its efforts, EPA has limited assurance its efforts address the highest risks.

EPA has faced challenges using its existing legal authority and voluntary approaches to manage cybersecurity risks but has not fully evaluated either approach. In March 2023, EPA interpreted existing legal requirements to include cybersecurity assessments at drinking water systems but withdrew the requirement 7 months later after facing legal challenges. Previous requirements and NSM-22 direct EPA to identify the authorities it needs to compel the sector to address risks. In July 2024, EPA officials said they had evaluated their authorities and would release the evaluation in 2025 with their risk assessment and strategy. Doing so and seeking additional authority as necessary can help EPA ensure the water sector is better prepared for any future cyberattacks.

Why GAO Did This Study

Recent cyber incidents highlight the vulnerability of the 170,000 water and wastewater systems in the U.S. water sector. EPA is responsible for leading, coordinating, and supporting activities to reduce cybersecurity risk to the water sector. The agency works in partnership with the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA) and other federal, state, and local entities.

GAO was asked to review cybersecurity threats facing the water sector and the federal government's efforts to address these threats. This report (1) describes cybersecurity risks and incidents; (2) examines actions by selected federal and nonfederal entities to improve cybersecurity; and (3) evaluates EPA's actions to address known risks.

Recommendations

GAO is making four recommendations, including that EPA assess sector risk; develop and implement a national cybersecurity strategy; and evaluate the sufficiency of its legal authorities to carry out its cybersecurity responsibilities and seek additional authority as necessary. EPA concurred with the recommendations and said it is taking action to complete them.

CISA Launches New Portal to Improve Cyber Reporting

The Cybersecurity and Infrastructure Security Agency (CISA) announced its cyber incident reporting form moved to the new CISA Services Portal as part of its ongoing effort to improve cyber incident reporting.

The Portal is a secure platform with enhanced functionality for cyber incident reporting, including integration with login.gov credentials. The portal's enhanced functionality includes the ability to save and update reports, share submitted reports with colleagues or clients for third-party reporting, and search and filter reports. A new collaboration feature allows users to engage in informal discussions with CISA.

"Any organization experiencing a cyber attack or incident should report it – for its own benefit, and to help the broader community. CISA and our government partners have unique resources and tools to aid with response and recovery, but we can't help if we don't know about an incident," said CISA Executive Assistant Director for Cybersecurity Jeff Greene. "Sharing information allows us to work with our full breadth of partners so that the attackers can't use the same techniques on other victims, and can provide insight into the scale of an adversary's campaign. CISA is excited to make available our new portal with improved functionality and features for cyber reporting."

To guide incident reporters through the reporting process, CISA also released a voluntary cyber incident reporting resource. It helps entities understand "who" should report an incident, "why and when" they should report, as well as "what and how to report." Several resources to reduce cyber risk are also available.

NCSC and partners issue warning over North Korean state-sponsored cyber campaign to steal military and nuclear secrets

Critical infrastructure organisations are strongly encouraged to stay vigilant to DPRK-sponsored cyber operations.

The UK and international allies have exposed a global cyber espionage campaign carried out by attackers sponsored by the Democratic People's Republic of Korea (DPRK) to further the regime's military and nuclear ambitions.

The National Cyber Security Centre – a part of GCHQ – has issued a new advisory today (Thursday) alongside partners in the United States and the Republic of Korea which reveals how a cyber threat group known as Andariel has been compromising organisations around the world to steal sensitive and classified technical information and intellectual property data.

The NCSC assesses that Andariel is a part of DPRK's Reconnaissance General Bureau (RGB) 3rd Bureau and that the group's malicious cyber activities pose an ongoing threat to critical infrastructure organisations globally.

The cyber actors have primarily targeted defence, aerospace, nuclear and engineering entities, and organisations in the medical and energy sectors to a lesser extent, in order to obtain information such as contract specification, design drawings and project details.

As part of its operations, Andariel has also launched ransomware attacks against US healthcare organisations in order to extort payments and fund further espionage activity.

This advisory shares technical details and mitigation advice to help defend against the actors who have been seen exploiting known vulnerabilities to access victims' systems before deploying malware and other tools to maintain persistence, evade detection and exfiltrate data.

The advisory outlines how Andariel has evolved its operations from conducting destructive attacks targeting US and South Korea organisations to conducting specialised cyber espionage and ransomware attacks.

Europol coordinates global action against criminal abuse of Cobalt Strike

Law enforcement has teamed up with the private sector to fight against the abuse of a legitimate security tool by criminals who were using it to infiltrate victims' IT systems. Older, unlicensed versions of the Cobalt Strike red teaming tool were targeted during a week of action.

Throughout the week, law enforcement flagged known IP addresses associated with criminal activity, along with a range of domain names used by criminal groups, for online service providers to disable unlicensed versions of the tool. A total of 690 IP addresses were flagged to online service providers in 27 countries. By the end of the week, 593 of these addresses had been taken down.

Known as Operation MORPHEUS, this investigation was led by the UK National Crime Agency and involved law enforcement authorities from Australia, Canada, Germany, the Netherlands, Poland and the United States. Europol coordinated the international activity, and liaised with the private partners. This disruptive action marks the culmination of a complex investigation initiated in 2021.

Cobalt Strike is a popular commercial tool provided by the cybersecurity software company Fortra. It is designed to help legitimate IT security experts perform attack simulations that identify weaknesses in security operations and incident responses. In the wrong hands, however, unlicensed copies of Cobalt Strike can provide a malicious actor with a wide range of attack capabilities.

Fortra has taken significant steps to prevent the abuse of its software and has partnered with law enforcement throughout this investigation to protect the legitimate use of its tools. However, in rare circumstances, criminals have stolen older versions of Cobalt Strike, creating cracked copies to gain backdoor access to machines and deploy malware. Such unlicensed versions of the tool have been connected to multiple malware and ransomware investigations, including those into RYUK, Trickbot and Conti.

Cooperation with the private sector was instrumental in the success of this disruptive action. A number of private industry partners supported the action, including BAE Systems Digital Intelligence, Trellix, Spamhaus, abuse.ch and The Shadowserver Foundation. These partners deployed enhanced scanning, telemetry and analytical capabilities to help identify malicious activities and use by cybercriminals.

This novel approach is possible thanks to Europol's amended Regulation which has strengthened the Agency's capacity to better support EU Member States, including by collaborating with the private sector. Through this novel approach, Europol can gain access to real-time threat intelligence and a broader perspective on cybercriminal tactics. This partnership enables a more coordinated and comprehensive response, ultimately enhancing the overall resilience of the digital ecosystem across Europe.

Police recover over USD 40 million from international email scam

A global stop-payment mechanism developed by INTERPOL has helped Singapore authorities make their largest ever recovery of funds defrauded in a business email compromise scam.

A commodity firm based in Singapore filed a police report stating that they had fallen victim to a business email compromise scam, in which a scammer obtains access to or impersonates a business email account to deceive employees into transferring money to their bank account.

Tthe firm had received an email from a supplier requesting that a pending payment be sent to a new bank account based in Timor Leste. The email, however, came from a fraudulent account spelled slightly different to the supplier's official email address.

Unaware, the firm transferred USD 42.3 million to the fake supplier, only discovering the crime four days later when the genuine supplier said it had not been paid.

On receipt of the police report, the Singapore Police Force (SPF) swiftly requested assistance from authorities in Timor Leste through INTERPOL's Global Rapid Intervention of Payments (I-GRIP) mechanism.

I-GRIP uses the global police organization's 196-country police network to speed up requests for assistance in financial crime cases.

The SPF's Anti-Scam Centre received confirmation that USD 39 million was detected and withheld from the fake supplier's bank account in Timor Leste.

Moreover, Timor Leste authorities arrested a total of seven suspects in relation to the scam through follow-up investigations, leading to the further recovery of more than USD 2 million. Steps are being taken for the return of the stolen funds to the victim in Singapore.

Isaac Oginni, Director of INTERPOL's Financial Crime and Anti-Corruption Centre (IFCACC), said, "Speed is crucial to successfully intercepting the proceeds of online scams, with police, financial intelligence units and banks cooperating across multiple jurisdictions in a race against time.

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

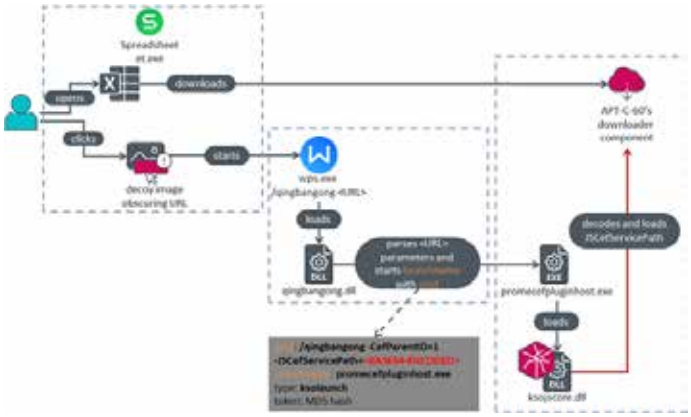
SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE

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

ESET Research: Spy group exploits WPS Office zero day; analysis uncovers a second vulnerability

ESET researchers discovered a remote code execution vulnerability in WPS Office for Windows (CVE-2024-7262). It was being exploited by APT-C-60, a South Korea-aligned cyberespionage group, to target East Asian countries.



When examining the root cause, ESET discovered another way to exploit the faulty code (CVE-2924-7263). Following a coordinated disclosure process, both vulnerabilities are now patched. The final payload in the APT-C-60 attack is a custom backdoor with cyberespionage capabilities that ESET Research internally named SpyGlace.

"While investigating APT-C-60 activities, we found a strange spreadsheet document referencing one of the group's many downloader components. The WPS Office software has over 500 million active users worldwide, which makes it a good target to reach a substantial number of individuals, particularly in the East Asia region," says ESET researcher Romain Dumont, who analysed the vulnerabilities.

During the coordinated vulnerability disclosure process between ESET and the vendor, DBAPPSecurity independently published an analysis of the weaponised vulnerability and confirmed that APT-C-60 has exploited the vulnerability to deliver malware to users in China.

The malicious document comes as an MHTML export of the commonly used XLS spreadsheet format. However, it contains a specially crafted and hidden hyperlink designed to trigger the execution of an arbitrary library if clicked when using the WPS Spreadsheet application. The rather unconventional MHTML file format allows a file to be downloaded as soon as the document is opened; therefore, leveraging this technique while exploiting the vulnerability provides for remote code execution.

Salvador Technologies' platform enables rapid recovery for clients during CrowdStrike outage

Salvador Technologies' critical infrastructure and industrial clients swiftly recovered from a CrowdStrike outage in minutes, using the company's advanced cyber-incident recovery platform.

This platform ensured that customers maintained complete operational continuity without relying on standard IT protocols, as the company's technology and platform enabled its customers to maintain operation continuity during the recent CrowdStrike outage.

Salvador Technologies reports that its critical infrastructure and industrial customers using the company's cyber-incident recovery platform for automating their recovery processes and securing their systems were able to return to full and normal operations within minutes of understanding that their systems and machines were down due to the CrowdStrike outage. In most instances, customers were able to execute their recovery even before their main IT servers were available.

"The CIO of a leading medical center customer told us last week that the CrowdStrike outage initially suspended the operations of thousands of workstations throughout its main facility. Manually restarting and fixing these workstations would have required several days of nonstop work, putting the lives of patients at risk, while costing the hospital millions of dollars in labor costs and operational downtime," explained Alex Yevtushenko, co-founder and CEO of Salvador Technologies. Salvador Technologies' air-gapped cyber-incident recovery platform consists of hardware connected to the HMI (human machine interface) or SCADA (supervisory control and data acquisition), an agent software, and a monitoring system, enabling full visibility of the operations.

Fidesmo Partners with LEGIC to Enhance Contactless Access Control Solutions

LEGIC is excited to announce a partnership with Stockholm-based Fidesmo, a leading Trusted Service Manager (TSM) platform provider to some of the world's largest consumer and financial service brands.

Fidesmo's technology-agnostic platform enables makers of contactless products and services to create secure smartphone- and transponder-based products and solutions.

The partnership marks LEGIC and Fidesmo's cooperation towards the expansion of the company's connected devices platform portfolio based on LEGIC's leading, end-to-end credential management software and secure semiconductors. This will enable end-customers and partners to strengthen their offering and increase customer satisfaction through enhanced security and a broader range of connected devices, particularly in the access management markets.

LEGIC's General Manager Christoph Beckenbauer said, "We are excited to enable Fidesmo to enhance their offering for secure contactless transactions, particularly in the access management markets. By integrating LEGIC's established, end-to-end credentialing technology, we are in a strong position to help Fidesmo establish a leadership position among providers of access management products, particularly among our vast global network of over 300 solution provider partners."

CEO of Fidesmo, Anders Malmström, said, "This partnership with LEGIC is a major step forward for Fidesmo. It allows us to work with yet another industry leader and showcase the flexibility and scale of our platform while also broadening our impact in the access control industry. We're committed to advancing our role as a TSM for both access control providers and devices, and this collaboration positions us perfectly to do so."

Wavefront Announces Shipment of First Batch of Vigilant FLS 600

Wavefront, a leader in innovative sonar technology, is thrilled to announce the shipment of the first batch of its highly anticipated Vigilant FLS® 600.

This latest addition to the Vigilant family of forward looking sonars will see the first units installed in a range of applications including surface and subsurface, crewed and uncrewed platforms.

Vigilant FLS 600 is a compact navigation and obstacle avoidance sonar creating – with unrivalled resolution and detail – a real-time, easy to interpret 3D terrain map of the seabed with automated alarms warning of objects in the water column ahead.

Vigilant has two principal operating modes: 3D and Sonar mode, both of which offer a class leading 120 degrees field of view on all range scales. Vigilant's unique patented technology allows our 3D mode to provide stunning 3D depth imagery, further ahead of the platform than any competing system, at ranges in excess of 20 times the prevailing water depth up to a maximum 600 m range and down to 100 m depth. Sonar mode processes the intensity of the acoustic data to extract long-range positional data of objects up to ranges of 600 m. Data from both modes are used to automatically generate alerts for the operator or supervising system to warn of the presence of a navigationally relevant obstacle.

With its history mapping capability, a comprehensive picture of the underwater environment surrounding the vessel is built up. This provides crews and autonomous systems with maximum situational awareness for collision or ground avoidance, tight manoeuvres or backing out of confined areas.

Speaking about this milestone for the Vigilant FLS 600, Paul Badger, Wavefront Managing Director, said 'Vigilant FLS 600 bridges the gap from UUV, AUV and ASV applications all the way through to mega yachts and cruise ships to deliver high resolution navigational imaging and long range obstacle avoidance'.

Baiduri Bank Streamlines Security and Authentication Journey Across Consumer and Corporate Banking with HID

HID®, a worldwide leader in trusted identity solutions, announced that Baiduri Bank, a member of Baiduri Bank Group and the largest conventional bank in Brunei Darussalam, has implemented HID Approve™ powered by the HID Authentication Platform across its consumer and corporate banking platforms, offering a single trusted authentication source for customer identity.

Baiduri Bank realized an opportunity to undertake a digital transformation to help ensure the delivery of a smooth customer experience, which entailed updating its digital banking software to build upon a cloud-based authentication infrastructure.

Baiduri Bank integrated HID Approve powered by the Authentication Platform across its consumer and corporate banking platforms. Offering a single trusted authentication source for customer identity, HID Approve helps to reduce complexity with standards-based, scalable solutions covering the entire authentication journey.

HID Approve provides mobile authentication and transaction signing with robust security protocols, hardened through standards-based cryptography. Featuring customizable security policies to protect communication channels, HID Approve is backed by rigorous third-party security testing and independent audits. HID Approve helps to deliver more seamless user experience, simplified compliance, flexible deployment and lower cost of ownership compared to traditional solutions.

ICEYE and Aon expand collaboration with flood and wildfire data agreement to enhance event response

ICEYE, a global leader in satellite-powered disaster management solutions, has announced that Aon, a leading global professional services firm, has expanded its data licensing agreement to include ICEYE's Flood Insights data globally and Wildfire Insights data for the US.

Under the agreement, Aon will incorporate ICEYE's near real-time flood and wildfire data into its event response capabilities for Reinsurance clients, to facilitate the loss analysis of catastrophic events. The high-resolution Insights data from ICEYE allows Aon to provide clients with detailed location-level analysis on flood and wildfire insights into damage of properties.

ICEYE's large constellation of NewSpace satellites provides access to a new level of persistent monitoring for any location on Earth, with synthetic aperture radar (SAR) technology delivering uninterrupted visibility, day and night, in any weather conditions and through smoke. Hazard and damage data is made available within hours of an event occurring with updated analysis provided at regular intervals as the flood or wildfire develops.

Stephen Lathrope, Senior Vice President for Solutions, ICEYE, added: "ICEYE is delighted to be expanding its data agreement with Aon and building on the success of the solutions we have supported. In an increasingly volatile natural catastrophe environment characterized by increasing frequency, severity, and complexity, rapid access to damage and hazard data will be critical. At ICEYE, we continue to expand our constellations and enhance our technology as we help shape the future of satellite-powered, data-driven disaster response."

ADVERTISING SALES

Ray Beauchamp -
Americas
E: rayb@torchmarketing.co.uk
T: +1-408-921-2932

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

INVITATION TO ATTEND

Securing the Inter-Connected Society

The premier event for the critical infrastructure protection and resilience community.

EARLY BIRD RATES CURRENTLY APPLY

Register today and save with the Early Bird discount - deadline 12th October.

The first 'Critical Infrastructure Protection Week' will take place in Madrid Spain and will see IACIPP host the 'Critical Infrastructure Protection & Resilience Europe' conference and exhibition and 'EU-CIP Horizon Project' conference as the first events as part of this initiative.

Critical Infrastructure Protection and Resilience Europe (CIPRE) brings together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Europe.

The conference will look at the developing themes and challenges facing the industry, including the importance of the implementation of the **NIS2 Directive and Directive on the Resilience of Critical Entities** and the obligations of CI owner/operators and agencies, as well as create a better understanding of the issues and the threats, helping to facilitate the work to develop frameworks, good risk management and strategic planning.

Join us in Madrid, Spain for the the 9th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure, part of CIP Week in Europe.

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

Leading the debate for securing Europe's critical infrastructure

Speakers include:

- **Jose Luis Perez Pajuelo**, Director General, National Center for Critical Infrastructure Protection, MOI
- **Dr. Enrique Belda Esplugues**, Director General, Port of Valencia
- **Luca Tagliaretti**, Executive Director European Cybersecurity Competence Center (ECCC)
- **Daniel Golston**, Associate Programme Officer Organization for Security and Co-operation in Europe
- **Dr Monica Cardarilli**, Project Officer European Commission Joint Research Centre, Italy
- **Rodrigo Brito**, Global Head of Cybersecurity Portfolio Nokia, Portugal
- **Frederic Petit**, Project Officer European Commission Joint Research Centre, Italy
- **Peter Nilsson**, Police Commissioner Head of Airpol, Europe
- **John Laene**, Managing Director RAILPOL
- **Dr Victor Vevera**, General Director ICI Bucharest, Romania
- **Alessandro Lazari**, Fellow in Critical Infrastructure Protection and Resilience University of Salento, Italy & International Association of CIP Professionals

For full speaker line up visit www.cipre-expo.com/speakers-2024

Supporting Organisations:

Platinum Sponsor:

Digital Security Progress. Protected.

Flagship Media Partner: