critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

WINTER 2024/25
www.cip-association.org

FEATURE:
Reducing disaster risks to deliver a resilient future

FEATURE:
New report: Terrorists exploiting global tensions

FEATURE:
Improving Red Teaming for Critical Infrastructure Protection: A Comprehensive Approach

ARE WE GETTING THE DESERVED RETURN-ON-INVESTMENT FROM THE EU RESEARCH ON CRITICAL INFRASTRUCTURE RESILIENCE?

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.

Co-Hosted by:

Invitation to Attend

Register online today

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 recent 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 previous Administration, designated 16 critical infrastructure sectors that will be subject to additional oversight through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

Trump's official platform, 'Agenda 47', highlights the need to protect critical infrastructure from cyber threats.

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.

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 and to register visit **www.ciprna-expo.com**

Speakers include:

- Steve Harris, Deputy Executive Assistant Director for Infrastructure Security, CISA
- Senator Bob Hall, State Senator, Texas Senate District 2, Texas State Senate
- John Miri, President, Electric Grid Cybersecurity Alliance
- Marshal Wilson, Co-Director, Southwest Border Food Protection and Emergency Preparedness Center
- Robert Russell, Regional Director (A) for Region 6, Cybersecurity and Infrastructure Security Agency
- Sunil Madhugiri, Chief Technology Officer, Office of the Assistant Commissioner, U.S. Customs and Border Protection
- Clint Ladd, Critical Infrastructure Protection Coordinator, Texas Department of Public Safety / Texas Office of Homeland Security
- Waqas Ahmed, Sr. Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency
- Marco Ayala, President, Houston InfraGard Members Alliance
- Lt. Col. Tommy Waller, USMC Ret., President & CEO, Center for Security Policy, USA
- Nelson Silva, Senior Product Manager, Nokia

For full speaker line up visit www.ciprna-expo.com/speakers2025

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

Executive Sponsors:

Flagship Media Partner:

Platinum Sponsor:

Gold Sponsors:

Silver Sponsor:

WHAT DOES THE FUTURE HOLD IN A CHANGING WORLD?

'We live in interesting times' has been an overused phrase of late, but seems to be more apt than ever.

The recent election of President Trump into the White House certainly stirred the world, and since his inauguration has created a whirlwind of change - change in attitudes, change in views and change in policies. This appear to be far reaching, with no department looking to be safe from change. So what could it mean to security, national and international?

Well, we are yet to see in full, but have started to see the strengthening of the Southern and Northern borders, the rescinding of Executive Order 14110 on AI, the declaration of a national energy emergency, assessment of the Federal Emergency Management Agency and notably EO14161 Protecting the United States From Foreign Terrorists and Other National Security and Public Safety Threats, as well as 'Agenda 47' highlighting the need to protect critical infrastructure from cyber threats - one of the core missions for the Cybersecurity & Infrastructure Security Agency (CISA).

All this will pan out over the coming months as to what it means policy-wise, but doesn't stop the immediate challenges and imminent threats faced by critical infrastructures, as these can also come from natural disasters or accidents - something that cannot be legislated for.

As the new Government settles into position, it is important the industry stays focussed. Information sharing, collaboration and cooperation become the rock of success for any sector.

We are delighted to see Critical Infrastructure Protection & Resilience North America being held in Houston, TX on 11th-13th March, co-hosted by Infragard Houston. This provides a great opportunity to network and understand the latest threats, challenges and opportunities for the industry, and we hope to see you there.

We also hope you enjoy reading this issue, and 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.

TORCH

Are we getting the deserved return-on-investment from the EU research on critical infrastructure resilience?

By October 17, 2024, the EU member states were supposed to notify the European Commission that the transposition of the Critical Entities Resilience (CER) Directive into respective national laws had been accomplished. Only two (out of 27) member states managed to meet that deadline.

Could the EU research projects in the area of critical infrastructure/entities (CI/CE) resilience have helped more to mitigate this delay? Could that mitigation be part of a more optimal return on investment (RoI)? Was the investment in recent years (e.g., over 4.5 b€ in digital transformation initiatives, or 450 M€ for cybersecurity projects and civil security) not adequate? Could it have produced more convincing answers to claims like "Europe's critical infrastructure is becoming dangerously vulnerable" ? Especially in the context of new and evolving challenges or the "European CIs under continuous attacks" ?

There is a general agreement about the need to reach better RoI or, in the same context, Return on Research Investment (RoRI). But the agreement about how to do it practically is still to be achieved. Leaving the extreme positions aside, like "the only real RoI is the commercially measurable use of project results", on one side, and "any use of project results represents RoI", on the other side, one can opt for the middle ground and assume that "an evident use leading to tangible benefits represents an RoI". For the CI/CE-related research, that can include, e.g., resilience standards, broadly adopted guidelines or evidence provided as inputs for the new EU and national policies. Applying such a definition, however, when searching for RoI-relevant results in the repositories of the EU project results such as CORDIS, Innovation Radar, or Dealflow, yields hardly any convincing evidence. The reported RoI-relevant results are often only vaguely described, not quantified, often out of date, and almost regularly lacking examples of real use or quantified benefits. As an example, the search for the results mentioning the CER Directive in the EU Dealflow tool provides no entries (January 2025). Similarly, the search for "resilience and infrastructure" among approx. 14,000 entries in the EU Innovation Radar, yields only 44 matches.

The reasons for the above can be numerous. E.g., the difficulty in aligning the needs and interests of industrial security and openness required by public research. Or, the lack of full-scale industry involvement (e.g., not participating with departments directly involved in production or marketing). Or, in the area of standardization, the rules and timing of standardization bodies being incompatible with the rules and timing of the EU projects. Or, the project results are simply not reported in the tools. Or, the main motivation of the researchers in the projects being to get new, follow-up projects, not necessarily to exploit the results of the finished ones. Many of these reasons are mentioned and explained in the recommendations of the evaluation reports made during the transition from one EU Framework Programme (FP) to another , but less often implemented afterward. The fact that EU projects legally

and practically do not exist after their final date, certainly also does not contribute to the sustainability of accessibility to project results and achieving good RoI.

In addition, imposing a too broad spectrum of (sometimes contradictory) goals, or the need to balance between breakthrough technology research and market success, on one side, and political constraints on the other side, can be very challenging for a good RoI. The latter is especially true and applicable to the area of CI/CE resilience, nowadays at the very top of the EU priorities . Their final results in many cases "never cross the chasm to the market, even if they achieved technological goals set in the project proposal" (exceptions available, of course). Even worse, on the researchers' side, the difficulties of meeting too many different or too highly set goals can lead to unrealistic or deceiving reporting, nowadays potentially worsened by the possible indiscriminate and unreported use of AI. On the EU side, limiting resources for monitoring the achievement of multiple goals, lower the threshold to clientelism.

How could the situation be improved? Generic, top-down, solutions suggested so far are generally well-aligned and present in the recommendations: strengthening and leveraging existing platforms (ERNCIP, Hubs, Radars…), better integration of research with industry and standardization, introducing mechanisms that support project continuity beyond formal completion, strong involvement of industry stakeholders, rewarding genuine success and penalizing exploitative practices, promoting monitoring and accountability, to mention just some of them. But, looking at the past decades of EU research, it seems that many suggested solutions have not been implemented as recommended.

Hence, the bottom-up solutions should be tried. Among them, establishing measurable indicators of success and robust evaluation systems is certainly at the top of the priority list. The data collection for the indicators such as those in the EUR 27314 EN should become mandatory and the indicators better known and understood, possibly including also the non-self-declared indicators

of successful exploitation (which could be used for monitoring and stress-testing, too – e.g., in combination with standards like DIN 91461). The key research-to-market transfer RoI indicators, quantifying effectiveness, efficiency, and transformation are generally available, but not used because data are missing, and the mandates and obligations are not well defined, especially not at the EU level. The prerequisite for such a system is a joint EU strategy, e.g., similar to the recent US strategy documents specifying both the overall framework and the need to "prioritize measurement". A future extension of the CER Directive?

To conclude, the EU research on critical infrastructure resilience and researchers should be further encouraged and incentivized to deliver more tangible RoI, including results directly usable and useful for the application of the CER Directive and the overall EU resilience, thus helping in meeting both the deadlines like the "October 17, 2024" one and the top level goals like the ones declared by the EU7. The push should include also the readiness and courage to openly name and address the real issues, avoid the "newspeak", and undertake efficiently the actions needed.

A. Jovanovi, Steinbeis European Risk & Resilience Institute, Germany

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

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

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

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

Increasing Cybersecurity Attacks

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

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

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

Resource Challenges

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

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

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

Skills and Retention Trends

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

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

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

A complimentary copy of ISACA's 2024 State of Cybersecurity survey report can be accessed at www.isaca.org/state-of-cybersecurity-2024.

Reducing disaster risks to deliver a resilient future

The Pact for the Future – adopted by world leaders at the September 2024 Summit of the Future – is the most comprehensive international agreement in decades, covering entirely new areas while also addressing issues that have long stalled consensus. It aims to equip international institutions to navigate a rapidly changing world. It is a pressing call to strengthen global cooperation and address the multifaceted challenges of our era-from sustainable development and digital governance to peace and security.

he Pact offers multiple entry points for advancing disaster risk reduction (DRR) and resilience-building efforts to accelerate implementation of the 2030 Agenda for Sustainable Development alongside the Sendai Framework, and framing global development beyond 2030.

The Pact for the Future makes a clear global commitment to promote a disaster risk-informed approach to sustainable development at the local, national, regional and global levels, and to accelerate progress on integrating disaster risk reduction into policies, programmes and investments at all levels. The representation of DRR in the Pact also ensures that future development initiatives are sustainable and inclusive, safeguard communities and foster long-term resilience.

Numerous actions and commitments are aligned with the recommendations and calls to action reflected in the Midterm Review of the Sendai Framework. They reinforce and build on the commitments from the 2023 SDG Summit Political Declaration to reduce disaster risk, promote resilience, and promote a disaster risk-informed approach to sustainable development.

Protecting the interests of future generations

Declaration on Future Generations

18. Prioritize urgent action to address critical environmental challenges and implement measures to reduce disaster risk and build resilience, reverse the degradation of ecosystems and ensure a clean, healthy and sustainable environment; and reaffirm the importance of accelerating action to address climate change and its adverse impacts, based on the principle of common but differentiated responsibilities and respective capabilities in the light of different national circumstances, noting the importance for some of the concept of "climate justice".

The Declaration on Future Generations sets out steps to make sure that today's decisions protect the interests of future generations. It is a call to safeguard the future through responsible, inclusive policies.

At the heart of the Declaration is the recognition that the actions-and inactions-of present generations have profound implications for those who will come after us. It is a reminder that leaders today have a responsibility to act with the needs and interests of future generations in mind.

Emphasizing critical areas such as sustainable development, climate action, digital cooperation, and youth inclusion, the Declaration aims to create an equitable, sustainable world that prioritizes peace, security, and human rights for future generations. One important proposal is the appointment an Envoy for Future Generations - someone who would ensure that long-term thinking is embedded in global policies.

The DRR agenda is closely aligned with this approach, focusing on reducing vulnerabilities for future generations by addressing new, emerging and future risks. A future-oriented approach demands the development of policies promoting long-term resilience planning, considering future risks such as climate-induced disasters, and embedding DRR into forward-looking multilateral frameworks - as were proposed in UNDRR's 2022 Global Assessment Report.

Intersections between the Pact and disaster risk reduction

The Pact specifically calls for action around several core DRR priorities:

- Addressing the drivers and root cases of vulnerability
- Strengthening efforts to prevent, anticipate, and mitigate the impact of humanitarian emergencies
- Promoting synergies between climate adaptation, DRR, environmental protection, and nature conservation
- Implementing the Early Warnings for All initiative
- Reforming the international financial architecture, including addressing the specific vulnerabilities of developing countries
- Adopting a holistic approach to development including strengthening institutional capacities, improvement of infrastructure, and the enhancement of community resilience.

An unambiguous appeal for a risk-informed approach

Action 6. We will invest in people to end poverty and strengthen trust and social cohesion…

(g) Promote a disaster risk-informed approach to sustainable development that integrates disaster risk reduction into policies, programmes and investments at all levels.

Within the Pact, DRR has been given specific focus to ensure

it remains a central pillar of sustainable development efforts, and a core principle for safeguarding development gains for future generations:

- Investing in people: Poverty and social inequality are underlying factors that exacerbate disaster vulnerability. The Pact urges investment in people, to strengthen social cohesion and build trust. This involves adopting policies that are informed by disaster risk to ensure that development efforts truly enhance community resilience. Resilience must be integrated into development to ensure that any gains are safeguarded for future generations.

- Synergies with adaptation and environmental action: DRR must go hand-in-hand with climate adaptation and wide-ranging sustainability efforts. By aligning DRR strategies with climate adaptation and efforts to restore, protect, conserve and sustainably use the environment, the Pact fosters a unified approach to resilience. This involves incorporating nature-based solutions into disaster planning to tackle structural vulnerabilities, address biodiversity loss, and strengthen resilience against systemic risks.

- Strengthening community resilience: The Pact advocates for holistic development approaches that strengthen both institutional and community resilience. This includes building resilient infrastructure, supporting inclusive community planning, and ensuring that resources reach the most vulnerable populations, enhancing resilience across society.

- Preparedness and Prevention for future disasters: The Pact's emphasis on strategic foresight, climate adaptation, resilient infrastructure, and the prevention of systemic risks provides essential guidance for shaping UNDRR's priorities and strategic focus areas moving forward. This also opens the opportunity to signal a clear narrative on the cost of not investing in prevention and resilience across all areas.

Data and technology at front and centre

Global Digital Compact 45. We commit by 2030 to…

(c) Develop open and accessible data systems to support effective disaster early-warning, early action and crisis response (SDG 3 &11).

Technology and data can be game changers for disaster risk reduction, improving our understanding of hazards, vulnerability and exposure; allowing more precise and proactive planning; and facilitating effective and timely early warning systems.

Leveraging effective data governance frameworks and AI will allow for unprecedented forecasting capabilities, giving communities a better understanding of future risks. Predictive analytics can identify high-risk areas and populations, allowing for targeted interventions that reduce loss of lives and livelihoods.

The "Early Warnings for All" initiative is a central element in the Pact, offering improved early actions in response to natural hazards. Early-warning systems rely on robust data to track weather patterns and hazard indicators, giving communities the lead time needed to evacuate, prepare resources, and minimize disaster impacts.

Resilience at the centre, across the UN system

The Pact calls for stronger coordination across the UN system to address global challenges. System-wide coherence will require a common understanding of the full scope of current and emerging risks, and the governance models required to address them, with DRR playing a central role in safeguarding lives, livelihoods and development gains.

UNDRR's strategic framework aligns closely with the Pact's focus on strategic foresight and long-term resilience. By embedding disaster resilience into the SDGs, we can ensure a comprehensive DRR approach leading up to 2030 and beyond.

As part of this drive, UNDRR can help ensure systematic disaster risk reduction efforts globally, through greater coordination across UN agencies. This system-wide DRR strategy promotes coherence in how the UN addresses DRR, ensuring that efforts are unified and comprehensive.

Financing a resilient future

The case for investment in prevention is unequivocal. Financial strategies must adopt a long-term perspective to effectively address pressing global challenges.

- Target those at risk: Those most vulnerable to disasters – such as LDCs, LLDCs, and SIDS – are often neglected by current financial structures. International financial architecture must be reformed to make it more responsive and fit for purpose.

- Reshape resource mobilization: The 4th Financing for Development (FfD4) Conference in June 2025 will be a key moment to shape resource mobilization for disaster risk reduction (DRR) through 2030 and beyond. Since the Addis Ababa Action Agenda (2015) emphasized DRR financing for "natural disasters", the risk landscape has evolved, requiring a broader, more integrated approach.

- Financial architecture for today and tomorrow: Advances in financing mechanisms, highlighted by UNDRR and the Midterm Review of the Sendai Framework, provide an opportunity to establish a resilient financial architecture that meets today's challenges and future needs, including through innovative and anticipatory financing mechanisms. DRR is a prerequisite for sustainable development and has been proven to be a sound economic decision. Preventing the creation of new risk, reducing existing risk, and increasing preparedness and risk transfer solutions where they cannot be avoided is a key pillar for this architecture. Act now for the Pact of the Future

Extending the reach of resilience

The Pact offers immediate opportunities for broadening the reach of disaster resilience efforts:

- Unpacking and contextualizing the Pact: UNDRR can lead efforts to educate and engage stakeholders – within and beyond the UN system – on the Pact's DRR dimensions. By building awareness and fostering partnerships, UNDRR can maximize the Pact's impact, engaging a global lineup of disaster risk stakeholders and partners in follow-up activities and initiatives.

- Alignment with intergovernmental processes: The Pact for the Future is aligned with upcoming global processes including the Fourth International Conference on Financing for Development, the Second World Summit for Social Development, the 2025 UN Ocean Conference, the Conferences of the Rio Conventions, the Urban Agenda, as well as the 2025 Peacebuilding Architecture Review. This opens opportunities for DRR in various contexts —including sustainable finance, climate action, and resilience-building agendas – reinforcing its role in the 2030 Agenda.

- Better coordination: The Pact calls for stronger coordination across the UN system to address global challenges: with its wide-ranging mandate, UNDRR is well positioned to coordinate well-integrated disaster risk management across sectors.

- Long-term foresight: UNDRR will play a critical role in leveraging science, data, and strategic foresight to advance long-term disaster risk reduction and resilience building.

FS-ISAC Releases Timely Data Governance and Generative AI Guidance

To help financial firms understand and mitigate the risks posed by implementing Generative Artificial Intelligence (GenAI), FS-ISAC, the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, has published step-by-step guidance titled More Opportunity, Less Risk: 8 Steps to Manage Financial Services Data with GenAI.

"GenAI presents enormous opportunities for financial firms to improve business operations, provide better customer service, and even improve their cybersecurity posture," said Michael Silverman, Chief Strategy & Innovation Officer at FS-ISAC. "However, just like any new technological development, GenAI increases security risks when it's not leveraged in a safe and compliant manner. This guidance allows financial institutions to experience the positive offerings of GenAI by outlining the risks and corresponding steps to mitigate the threats."

Developed by FS-ISAC's Artificial Intelligence Working Group, the guideline outlines eight foundational steps to developing an effective data governance approach that harnesses the benefits of GenAI while remaining compliant with security standards.

- Consider Your Risks: Many of the risks associated with traditional data governance can be exacerbated by GenAI. Developing policies, technical controls, clear roles and responsibilities, and accountability metrics, among other steps, can shed light on risks, gaps, and opportunities.

- Data Selection Criteria: Using datasets requires an accountable, cautious approach with constant oversight. Develop a clear path for data selection, then conduct periodic risk testing to make sure the controls to protect the datasets are working as intended.

- Create and Maintain a Data Lineage Inventory: Strong access controls, data sanitization practices, and accurate data classifications are necessary to counteract concerns around data lineage and traceability.

- Be Disciplined with Data Access and Authorization: GenAI training data should be segregated and access restricted to ensure models are training on the correct data. Establish a regular review cadence of datasets and their access.

- Obsessively Protect Your Customers' Data: Security techniques including differential privacy, encryption in transit and at rest, data sanitization, and sandboxing should be leveraged to maintain the confidentiality, integrity, and availability of sensitive information.

- Use Best Practices When Building Effective Test Plans: Generate baselines for model testing and leverage cross-sector data sharing to ensure adequate coverage across a domain. Understanding the reliability and completeness of underlying data allows for stronger model testing with fewer limitations.

- Keep Current on Model Vulnerabilities: Fundamental data governance security practices combined with basic cybersecurity hygiene can alleviate vulnerabilities created by the growing threat landscape.

- Require Your Vendors' Transparency on Your Data Storage: Establish transparent communication with all vendors to ensure activities are compliant with regional and international requirements, as well as the firm's internal security standards.

GenAI use cases and risks are still evolving, and while GenAI offers great potential for financial services processes, the sector has many concerns about data security, usage, privacy, and compliance. This report is designed to help financial institutions assess their needs and determine a secure and effective approach to using GenAI in data governance.

New report: Terrorists exploiting global tensions

Terrorists continue to adapt their methods and narratives to exploit global events, digital technology, and societal vulnerabilities. The EU Terrorism Situation and Trend Report (EU TE-SAT) 2024, published today by Europol, provides a detailed overview of the evolving terrorism landscape in the European Union.

Geopolitical tensions amplifying terrorist narratives

The 7 October 2023 Hamas attack on Israel and the subsequent military response in Gaza have triggered global reactions. Hamas widely shared propaganda from the initial attack to mobilise jihadist groups globally. Terrorist groups used the high number of civilian casualties to develop propaganda, radicalise individuals and intensify calls for violence. Hamas utilised the crisis to secure funding via money transfers, cryptocurrencies, and Hawala networks. Some of these transfers potentially came from the EU.

The conflict and the propaganda stemming from it has unified extremist narratives across jihadist, right-wing, left-wing, and anarchist groups, sparking online incitement to violence, particularly targeting Jewish and Israeli interests worldwide. This has amplified anti-Semitic and anti-Muslim tensions within the EU. Regionally, Hezbollah's confrontations with Israel raise EU security concerns.

Leveraging today's youth and technology

The involvement of young people in terrorism-related activities is growing. Terrorist groups increasingly exploit online platforms and gaming environments to reach younger audiences. Disseminating content like videos, music and memes, these groups radicalise individuals and mobilise them for propaganda production, recruitment, and even attacks. Furthermore, the radicalisation has sped up; the time between initial exposure to extremist content and violent action has significantly decreased.

Increased anti-Semitic and anti-Muslim rhetoric has heightened societal tensions, resulting in strong polarisation of certain groups. Meanwhile, both jihadist and right-wing extremists have used the Israel-Hamas conflict to promote their narratives and inspire action.

The dual nature of technology emerges when it is exploited by terrorist groups, which are capitalising on advancements in AI and encrypted communication technologies to further their operations. AI-generated deepfakes are being used for propaganda and disinformation, while encrypted messaging apps provide secure communication channels for planning and recruitment. Innovation has been used for weaponry, with 3D-printed firearms becoming more popular, particularly among right-wing extremists.

EU TE-SAT 2023 key figures:

- 120 terrorist incidents across seven EU Member States, including 98 completed attacks, 9 failed attempts, and 13 foiled plots, marking a significant rise from 2022.
- 6 fatalities and 12 injuries resulted from jihadist attacks, the deadliest form of terrorism in the EU.
- 426 arrests for terrorism-related offences were made across 22 Member States, with jihadist offences accounting for 78 % of the total.

Jihadist terrorism: a continuous and lethal threat

Jihadist terrorism remains the most significant threat to EU security. In 2023, 5 of the 14 attempted jihadist attacks were completed. All these were carried out by lone actors, highlighting the challenges of preventing attacks by isolated individuals. Furthermore, these so-called lone actors are well connected via online communities. Most attacks used weapons such as knives and firearms, with perpetrators often radicalised online. Jihadist propaganda continued to exploit divisions in society and geopolitical events, such as the October 2023 Hamas attack on Israel, to recruit and radicalise individuals.

Terrorist groups are also leveraging encrypted communications and social media to evade detection while continuing to disseminate propaganda targeted at vulnerable individuals. Young people are increasingly involved in producing and disseminating propaganda on online networks. 334 individuals were arrested for jihadist-related offences, with young people making up a growing proportion of the total arrests. Detention facilities remain hotspots for radicalisation, with some inmates attempting to recruit others. Released prisoners continue to pose a potential security risk.

Right-wing terrorism: exploiting digital tools

While only two right-wing terrorist attacks took place in 2023, and both were foiled, the ideological and operational threat posed remains significant. Right-wing extremists, particularly younger individuals, are increasingly active in online communities, producing propaganda, inciting violence, and experimenting with technologies such as 3D printing to create weapons.

Online platforms are used for spreading propaganda, recruiting others, and sharing weapon-making instructions, with significant interest in 3D-printed firearms. Arrests included young individuals who were radicalised online and involved in incitement and planning attacks. Narratives like eco-fascism and anti-system rhetoric gained prominence, combining environmental concerns with extremist ideology.

Left-wing and separatist terrorism: persistent activities

Left-wing and anarchist terrorism accounted for 32 attacks in 2023, mostly targeting property and critical infrastructure. Separatist groups were responsible for the majority of completed attacks. These left-wing and anarchist terrorist groups often align their activities with socio-political grievances, such as anti-capitalist and environmental movements.

Left-wing actors targeted government buildings, financial institutions, and businesses. Support for imprisoned anarchists remained a catalyst for violent acts, as did broader anti-state sentiments. Ethno-nationalist groups remained active, often focusing on regional independence.

The future of risk communications is community engagement

Risk communication is about empowering people and communities to build resilience and take lifesaving actions. From yellow traffic lights to tornado sirens, we encounter risk messages every day; however, when it comes to urging community preparedness for threats, we must move away from a "one size fits all" messaging approach to affect meaningful changes.

Hazards, such as heavy rain and wind, only become disasters when they meet unprepared and vulnerable communities. We must urgently address the barriers that limit individual and community preparedness and lead to disasters, such as language barriers, the inability to identify and question rumors, and lack of resources needed to build preparedness. Strategic risk communications can bridge the gap between threat awareness and action. When culturally competent messaging is paired with robust and purposeful community engagement, they become powerful tools to inspire resilience building.

Our communities can only take steps to prepare and recovery quicky from disasters if they feel empowered in their decision making. That begins with information presented in the right way, at the right time, and through trusted channels. Engagement with communities begins by asking questions and listening through two-way communication. Through active listening we learn about a communities' culture and history, we can tailor methods and messaging that helps communities make informed decisions.

True strategic risk communication reaches the whole community, ensuring that everyone, including the most vulnerable populations, are equipped with the knowledge and resources needed to respond effectively. Developing targeted communications for specific populations means creating messages that are delivered in the right languages, reflective of the historical context of the place and the people, and aligned to the unique risks of the community.

For communities with language barriers, access to simple, clear, and accessible information is imperative for building understanding. Word-for-word translations are insufficient because words can have multiple or different meanings across dialects. By engaging a community, communicators can learn which languages are needed and identify partners to support translation and message sharing. This is work that FEMA is doing to meet people where they are and is an approach that UNDRR advocates.

The messenger is just as important as the message in determining whether community members are willing to trust and act upon the information. Effective community engagement involves building partnerships with community organizations to amplify messages. Through these

partnerships, communicators can identify community leaders, including business professionals, religious leaders, and teachers. Identifying those critical trusted messengers coupled with finding trusted sources of information can reduce misconceptions and build messaging coalitions.

For the last several years, FEMA's National Preparedness Month campaigns have enlisted community partners to help amplify preparedness messaging—including Howard University, a historically-black university, to help develop and deliver preparedness messaging to Black and African American communities; the Rosalynn Carter Institute for Caregivers, to reach older adult communities—specifically those with limited resources, disabilities, living in rural areas; and, most recently, signed an Memorandum of Understanding with the National Council on Asian Pacific Americans to advance preparedness messaging in Asian American, Native Hawaiian and Pacific Islander communities. FEMA even maintains a valuable partnership with the National Football League to get preparedness messaging into the hands of sports fans.

Finding and leveraging community networks to gather and convey information can develop credibility and trust before disasters strike. Communicators can build on these to express empathy, expertise, and honesty to address people's desire for clarity in uncertain times and meet the moment with trusted information.

For those moments when we move from preparedness into imminent hazard warning—where we must reach a lot of people all at once—the United Nation's Early Warnings for All (EW4All) initiative uses multiple tools to support early warning systems that are inclusive, effective and accessible to children so that no one is left behind. These systems provide safety alerts and actions directly to people. Messages as simple as "get to high ground" can save lives during a tsunami. Ideally, the combination of technology and existing relationships will get lifesaving information to people in the moments they truly need to know what to do end to end.

In today's busy news environment,

with more and more channels and platforms for information, it can be difficult to help communities tune out the noise and zero in on the right information. As we have seen during the most recent federal responses to Hurricanes Helene and Milton, we are facing a more contentious information environment during disasters.

False and misleading information is being generated at historic levels to sow distrust, making positive and collaborative community relationships essential to overcome the falsehoods. Communicators are increasingly finding allies in local news outlets, community social media, and nonprofit partners. Even in schools, partnerships are critical in promoting a culture of disaster prevention and preparedness from a young age.

Local journalists play a crucial role in risk communication, as they are uniquely positioned to understand and reflect the concerns of their communities. Their deep connections allow them to rapidly disseminate critical information during crises, ensuring that messages are timely, accurate, culturally relevant and help combat information that is wrong and being used to hurt people. All disasters start and end at the local-level, and all communicators need to remember that and shift strategies accordingly. A recent Pew Research report finds 85% of U.S. adults say local news outlets are important to the well-being of their communities, and 70% of Americans rank local journalists as being in touch with their communities.

At the end of the day, risk communication is about meeting people where they are, as FEMA Administrator Deanne Criswell has said since the very first day she ran the agency.

There is a renewed urgency to know our communities, and a need to leverage community partners and build a trusted messenger network. With climate-driven disasters becoming more frequent and severe, there is no time to waste.

The time is now to invest in relationship building, and for communicators, community leaders, and local news outlets to join forces and save lives. By forging stronger bonds today, we lay the foundation for a more resilient tomorrow.

Saskia Carusi is Deputy Chief of the United Nations Office for Disaster Risk Reduction (UNDRR) – Regional Office for the Americas and the Caribbean.

Navigating cybersecurity investments in the time of NIS 2

The latest report of the European Union Agency for Cybersecurity (ENISA) aims to support policy makers in assessing the impact of the current EU cybersecurity framework, and particularly the NIS 2 Directive, on cybersecurity investments and the overall maturity of organisations in scope.

The fifth iteration of the NIS Investments report provides key insights into how organisations in scope of the NIS 2 Directive allocate their cybersecurity budgets, build their capabilities, and mature in line with the Directive's provisions, while also exploring global cybersecurity trends, workforce challenges, and the impact of AI.

The report further provides insights into the readiness of entities to comply with new requirements introduced by key horizontal (e.g. CRA) and sectorial (e.g. DORA, NCCS) legislation, while also exploring the challenges they face.

The EU Agency for Cybersecurity Executive Director, Juhan Lepassaar, highlighted: "The NIS 2 Directive signifies a turning point in Europe's approach to cybersecurity. Within a fast evolving and complex threat landscape, the proper implementation of the NIS 2 requires adequate investments and especially into the new sectors which fall under the scope of the updated Directive. The ENISA NIS Investments report provides evidence-based feedback to policymakers and stakeholders regarding NIS-driven investments. These insights are essential for informed decision-making and addressing potential hurdles and gaps in cybersecurity policy implementation."

The 2024 edition features a significant enhancement compared to previous versions, as it extends the survey sample to include sectors and entities that are in scope of NIS 2. Through this approach, this report provides a pre-implementation snapshot of relevant metrics for the new sectors and entities under NIS 2, laying a foundation for future assessments of the impact of NIS 2. Additionally, it includes a sectorial deep dive in the Digital infrastructure and Space sectors.

Data were collected from 1350 organisations from all EU Member States covering all NIS2 sectors of high criticality, as well as the manufacturing sector.

Key findings

- Information security now represents 9% of EU IT investments, a significant increase of 1.9 percentage points from 2022, marking the second consecutive year of growth in cybersecurity investment post-pandemic.

- In 2023, median IT spending for organisations rose to EUR 15 million, with information security spending doubling from EUR 0.7 million to EUR 1.4 million.

- For the fourth consecutive year, the percentage of IT Full Time Equivalents (FTEs) dedicated to information security has declined, from 11.9% to 11.1%. This decrease may reflect recruitment challenges, with 32% of organisations—and 59% of SMEs—struggling to fill cybersecurity roles, particularly those requiring technical expertise. This trend is especially notable given that 89% of organisations expect to need additional cybersecurity staff to comply with NIS2.

- New NIS2 sectors are comparable in cybersecurity spending to existing NIS Directive entities, with their investments largely focused on developing and maintaining baseline cybersecurity capabilities. Emerging

areas, such as post-quantum cryptography, receive limited attention with only 4% of surveyed entities investing and 14% planning future investments.

- The majority of organisations anticipate a one-off or permanent increase in their cybersecurity budgets for compliance with NIS 2. Notably, a substantial number of entities will not be able to ask for the required additional budget, a percentage that is especially high for SMEs (34%).

- 90% of entities expect an increase in cyberattacks next year, in terms of volume, costliness or both. Despite that, 74% focus their cybersecurity preparedness efforts internally, with much lower participation in national or EU-level initiatives. This gap underscores a critical area for improvement, as effective cross-border cooperation in managing large-scale incidents can only be achieved at these higher levels.

- Overall awareness among in-scope entities is encouraging, with 92% being aware of the general scope or specific provisions of the NIS 2 Directive. However, a notable percentage of entities in certain new NIS 2 sectors remain unaware of the Directive, suggesting a potential need for increased awareness campaigns by the national competent authorities.

- Entities in sectors already covered by NIS outperform those newly included under NIS 2 across various cybersecurity governance, risk, and compliance metrics. Similarly, entities in new NIS 2 sectors show lower engagement and higher non-participation rates in cybersecurity preparedness activities. This highlights the positive impact the NIS Directive has had on the sectors already in scope; and creates anticipation for the impact NIS 2 will have on the new sectors.

Through the years, the series of the NIS Investments report provide a rich historical dataset which, building on this year's foundation, will allow us to gain insights into the effect of NIS 2 on new entities within its scope.

Maritime Cargo Security: Additional Efforts Needed to Assess the Effectiveness of DHS's Approach

The U.S. economy depends on the efficient flow of millions of tons of cargo each day throughout the global supply chain, most arriving by ship. However, U.S.-bound vessels and maritime cargo shipments are vulnerable to criminal activity or terrorist attacks that could disrupt operations and limit global economic growth and productivity.

The Coast Guard and U.S. Customs and Border Protection monitor these vessels for potential national security risks, like smuggling.

At the 8 ports the GAO reviewed, the agencies generally followed selected leading collaboration practices such as "leveraging resources"—like helping each other with vessel boardings during staff shortages.

The Coast Guard has worked with others to develop a strategic goal for maritime security. We recommended that the Coast Guard better measure progress toward this goal.

The Department of Homeland Security (DHS) uses a layered maritime security approach to identify potentially high-risk, U.S.-bound vessels and cargo shipments. Within DHS, the U.S. Coast Guard and U.S. Customs and Border Protection (CBP) are the lead agencies that manage programs that screen, target, and examine these vessels and shipments. Both agencies conduct these activities before vessels and cargo depart foreign seaports, in transit, and upon their arrival at U.S. seaports. For example, both agencies have intelligence programs to screen and target these vessels and cargo across the supply chain.

The James M. Inhofe National Defense Authorization Act for Fiscal Year 2023 includes a provision for GAO to assess federal efforts to secure U.S.-bound vessels and maritime cargo from national security-related risks. This report addresses (1) how DHS secures these vessels and cargo from supply chain risks, (2) the extent that DHS used selected leading collaboration practices, and (3) the extent that DHS assessed its approach.

GAO reviewed agency policies, procedures, and collaboration efforts and government-wide strategy documents, and assessed DHS collaboration efforts against five relevant leading practices identified in prior GAO work. GAO also interviewed Coast Guard and CBP officials from 16 field locations at a non-generalizable sample of eight U.S. seaports selected for varying volumes of cargo and diversity of geographic regions.

GAO recommended that the Coast Guard, with sector partners, develop objective, measurable, and quantifiable performance goals and measures and use this performance information to assess progress towards the goals and effectiveness of the layered approach to securing vessels and maritime cargo on an ongoing basis. DHS concurred with its recommendations.

- The Commandant of the Coast Guard, in coordination with Transportation Systems Sector partners, should develop objective, measurable, and quantifiable performance goals and associated performance measures.

- The Commandant of the Coast Guard, in coordination with Transportation Systems Sector partners, should use the performance information collected to assess progress toward strategic and performance goals and the overall effectiveness of the layered approach to securing vessels and maritime cargo on an ongoing basis.

Launch of international advisory body to support resilience of submarine telecom cables

The International Telecommunication Union (ITU), the United Nations Agency for Digital Technologies, and the International Cable Protection Committee (ICPC), the leading industry organisation promoting submarine cable protection, have formed the International Advisory Body for Submarine Cable Resilience to strengthen the resilience of this vital telecommunication infrastructure.

Submarine telecommunication cables form the backbone of global communications, carrying most of the world's Internet traffic and enabling critical services across the globe, including commerce, financial transactions, government activities, digital health and education.

The Advisory Body will address ways to improve cable resilience by promoting best practices for governments and industry players to ensure the timely deployment and repair of submarine cables, reduce the risks of damage, and enhance the continuity of communications over the cables.

"Submarine cables carry over 99 per cent of international data exchanges, making their resilience a global imperative," said ITU Secretary-General Doreen Bogdan-Martin. "The Advisory Body will mobilize expertise from around the world to ensure this vital digital infrastructure remains resilient in the face of disasters, accidents, and other risks."

Recognizing the vital role of subsea infrastructure

Damage to submarine cables is not uncommon, with an average of 150

to 200 faults occurring globally each year and requiring about three cable repairs per week, according to the ICPC.

The primary causes of damage include accidental human activity, such as fishing and anchoring, alongside natural hazards, abrasion and equipment failure.

"The formation of this International Advisory Body with ITU marks another step toward safeguarding our global digital infrastructure," said ICPC Chair, Graham Evans. "By working together, we can promote best practices, foster international collaboration, and create a consistent approach to protect the vital submarine cable networks that underpin global connectivity."

Supporting digital resilience globally

The Advisory Body's 40 members include Ministers, Heads of Regulatory Authorities, industry executives, and senior experts on the operations of telecommunication cables.

Members come from all world regions, ensuring diversity and inclusion from countries ranging from small island states to major economies. The membership captures the perspectives of those whose livelihoods and digital futures depend on the operation of submarine telecommunication cables, as well as those who work to deploy, maintain and protect this vital infrastructure.

The Advisory Body is co-chaired by H.E. Minister Bosun Tijani, Minister of Communications, Innovation and Digital Economy of the Federal Republic of Nigeria, and Prof. Sandra Maximiano, Chair of the Board of Directors of the National Communications Authority of the Republic of Portugal (ANACOM).

"Submarine cables are essential to the functioning of our connected world, but they face risks that require coordinated, proactive action," said Tijani. "Therefore, we are happy to host the inaugural Submarine Cable Resilience Summit to be held in Nigeria in early 2025."

"This initiative underscores the global community's commitment to strengthening these networks and advancing international cooperation for digital resilience," said Maximiano.

The Advisory Body will meet at least two times a year. It will consult with experts on telecommunications, digital resilience infrastructure development, infrastructure investment and international policy to provide strategic guidance and encourage sector-wide collaboration.

Improving Red Teaming for Critical Infrastructure Protection: A Comprehensive Approach

In the world of cybersecurity, the term "Red Team" traditionally refers to simulated adversaries tasked with testing a system's defenses. However, as the threat landscape becomes increasingly sophisticated and multifaceted, the approach to Red Team operations must evolve. Protecting critical infrastructure is no longer just about technological defenses; it requires a holistic approach that encompasses both technical and human aspects.

By Aurora García, a journalist and consultant specializing in security and cybersecurity.

A true Red Team operation must go beyond conventional penetration tests and vulnerability assessments. It needs to integrate every aspect of an organization's security posture, involving not only IT departments but also human, operational, and strategic layers of the organization. Cybersecurity is not only about firewalls, encryption, and penetration tests. It's about understanding the vulnerabilities that extend to organizational processes, behaviors, and decision-making. When it comes to critical infrastructure, these vulnerabilities can have far-reaching consequences beyond the digital realm.

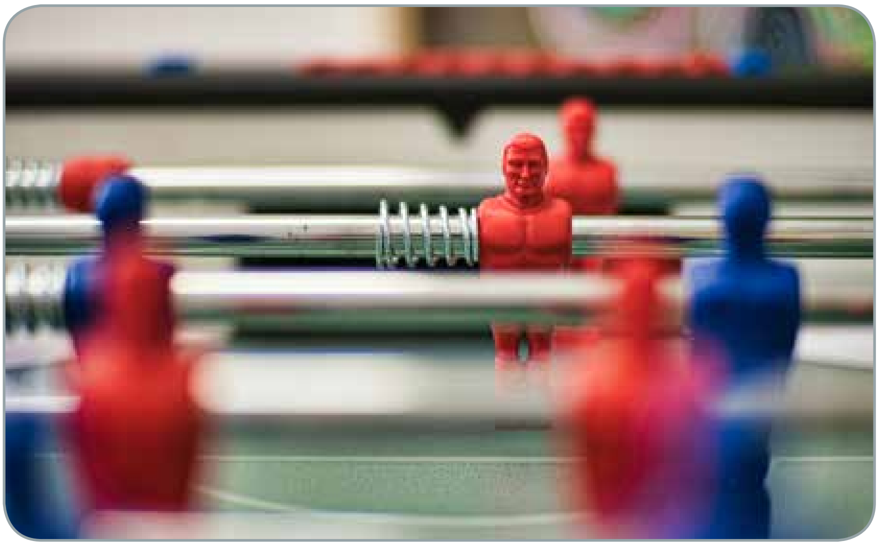
Understanding the Full Scope of Red Teaming

When executed correctly, Red Team missions simulate real-world threats by evaluating not only the technology but also the behaviors, processes, and policies that could be exploited by adversaries.
We live in an era where social engineering, misinformation, and internal threats are increasingly common tactics used by attackers. The human factor, whether intentional or not, remains the most significant vulnerability in any cybersecurity strategy. From spear-phishing to poorly implemented security protocols, organizations are often their own worst enemies.

In the context of critical infrastructure, where the stakes are particularly high, Red Team engagements must go beyond identifying technical flaws. Effective Red Teams must operate with the understanding that human vulnerabilities, communication breakdowns, and organizational inertia can be just as dangerous as any exploited firewall or malware. For this reason, a successful Red Team mission should include training and simulations at all levels of the organization, ensuring that the response to cyber threats is unified and well-coordinated.

Example of Planets: An Integrated Model for Critical Infrastructure

To illustrate how a comprehensive approach can be effectively applied, we can refer to the



Planets system, which I developed specifically for protecting critical infrastructure in a bank. Planets is a system based on the TIBER-EU framework, designed to overcome the limitations of conventional Red Team missions.

The model consists of several "planets" that work in coordination, covering all aspects of protection. Épsilon, the first planet, is made up of a multidisciplinary team that conducts a thorough risk assessment of the bank, considering not only technological threats but also criminal trends and operational characteristics of the client. The next step is the Gamma planet, which prepares the infrastructure for Alpha to identify vulnerabilities before the real attack takes place. Finally, Omega executes the simulated attack in its final phase, while Delta focuses on threat prospecting, anticipating potential criminal products and developing strategies to stay one step ahead of attackers.

This integrated approach allows Red Team teams to not only assess threats but also act proactively, incorporating both human and technological elements into a much more realistic simulation.

Beyond the Screen: Incorporating Human Elements into Red Team Missions

When designing Red Team missions, it's essential to think of them as real-world scenarios. Cyberattacks rarely occur in isolation; they are often part of a broader strategy designed to exploit both technology and human systems. A Red Team should consider how an attacker might use social engineering tactics, internal threats, and even the media to manipulate situations to their advantage. The key to success is not just understanding how to penetrate a network, but anticipating how an adversary might exploit a weak link within the organization's human framework.

At its core, Red Teaming is about creating the most accurate and complete model possible of the adversary's potential behavior. By integrating human intelligence into the process, Red Teams can simulate more realistic threats that go beyond traditional technical penetration tests. The result is not only identifying vulnerabilities but

better preparing the organization for a coordinated and multifaceted attack.

Adapting Red Teaming to the Evolving Threat Landscape

The global cybersecurity environment is rapidly changing, and the protection of critical infrastructure is no longer a passive activity. Organizations must anticipate and stay ahead of evolving threats. By leveraging intelligence-driven Red Team operations, companies can design security strategies that are adaptive and proactive.

The next step in the evolution of Red Teaming is not simply improving technical capabilities but developing a deeper understanding of how adversaries operate on all fronts. Red Team members should come from diverse fields, not just cybersecurity professionals, but also behavioral analysts, communication experts, and even crisis management specialists. Only through a multidisciplinary approach can Red Team missions provide the most realistic and insightful assessments of critical infrastructure defenses.

In the face of increasingly complex threats, Red Teams must embrace both the technical and human aspects of cybersecurity. The goal is not merely to simulate attacks but to understand how vulnerabilities can be exploited across a wide spectrum of organizational activities.

By focusing on the integration of both technical and human elements, Red Teams can help organizations transition from a reactive security posture to a proactive one, ensuring that critical infrastructures remain secure and resilient in the face of evolving threats.

Tackling cybercrime: common challenges and legislative solutions identified by Europol and Eurojust

The latest joint report by Europol and Eurojust, Common Challenges in Cybercrime, explores the persistent and emerging issues that hinder cybercrime investigations.

The report highlights several pressing challenges faced by law enforcement, including the overwhelming volume of digital data, the risk of data loss, and the persistent barriers to accessing critical information due to legal and technical constraints. The increasing use of anonymisation services has further complicated efforts to track criminal activities online.

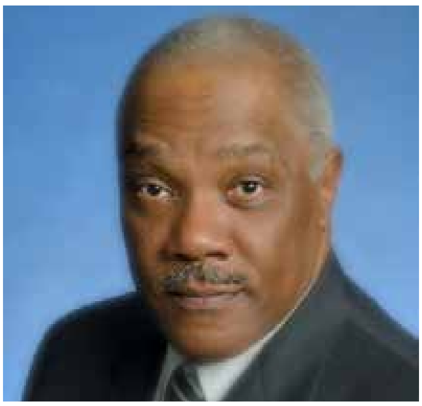
To help mitigate these challenges, the report explores the impact of new EU legislative tools, such as the e-Evidence Package, the Digital Services Act, and the EU AI Act. These instruments aim to facilitate data access, improve cross-border cooperation, and enhance investigative capabilities. However, their effectiveness will largely depend on how they are implemented and integrated into existing operational strategies.

The report also underscores the value of the strategic cooperation between Europol and Eurojust, highlighting initiatives such as the SIRIUS Project, which has strengthened collaboration in cybercrime investigations. These efforts continue to play a crucial role in helping law enforcement agencies navigate an increasingly complex digital landscape.

While challenges remain, the report emphasises the potential of these new legislative measures to strengthen the fight against cybercrime. Equipping law enforcement with the right tools and ensuring their effective use in investigations will be key to staying ahead of evolving cyber threats.

Artificial Intelligence Perspective: The Changing of the Guard

In the United States, a newly elected president causes turmoil during his administration's initial days and weeks. This occurs in every new administration. Many of the government's web links change or disappear. Additionally, the new president revokes executive orders of his predecessor and issues amended or new directives. One such action of the president is an Executive Order (EO). An EO is a directive issued by the President of the United States to manage the



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

federal government's operations. When rooted in statutory or constitutional authority, these orders have the force of law. The basis is found in Article II of the U.S. Constitution. The scope and impact of an EO is binding for Federal Agencies and employees. However, these orders are not directly binding for private individuals and organizations. Another federal government organization that enforces presidential directives is the Office of Management and Budget (OMB). OMB issues memorandums to provide guidance, instructions, or updates to federal agencies on budget, management, and regulatory policies. These memorandums play a key role in ensuring that federal agencies operate in compliance with executive priorities, legislative requirements, and administrative standards. The legal basis for OMB authority is found in the United States Code. Understanding the source of orders and directives to guide my thoughts is essential.

On January 20, 2025, President Trump revoked Executive Order 14110: The Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. On January 23, 2025, President Trump issued an EO directing his office to review with all agencies the aspects of EO 14110 for relevance to their AI initiatives. The directive's section 5 States:

"Sec. 5. Implementation of Order Revocation. (a) The APST, the Special Advisor for AI and Crypto, and the APNSA shall immediately review, in coordination with the heads of all agencies as they deem relevant, all policies, directives, regulations, orders, and other actions taken pursuant to the revoked Executive Order 14110 of October 30, 2023 (Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)."

NOTE: APST is the Assistant to the President for Science and Technology and APNSA is the Assistant to the President for National Security Affairs.

President Trump, in his first term, issued two Executive Orders related to AI. The first was EO 13859, titled Executive Order on Maintaining American Leadership in Artificial Intelligence. This

order was issued on February 11, 2019, and it outlines the policy and principles for promoting AI research and development (R&D), ensuring economic and national security, and fostering public trust in AI technologies. The order emphasizes the need for sustained investment in AI, the development of technical standards, workforce training, and international collaboration. It assigns roles and responsibilities to various federal agencies and sets objectives for enhancing data access, computing resources, and regulatory guidance. Furthermore, the order includes provisions for protecting U.S. AI technologies from foreign adversaries and for promoting AI-related education and workforce development.

The second was EO 13960, titled "Executive Order on Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government." This order was issued on December 3, 2020, and it highlights the potential of AI to enhance government operations, reduce costs, improve services, and support decision-making. Additionally, it aligns with a prior executive order aimed at maintaining American leadership in AI. The order also includes a table listing key figures in the Trump administration, along with various White House offices and councils.

A detailed review of President Trump's earlier Executive Orders aligns with former President Biden's EO 14110. We in the critical infrastructure community need to monitor the results of the APST and APNSA reviews with U.S. federal agencies to determine how future AI governance will impact our operations.

Shaping the Future of AI in Security: CoESS Launches Ethical and Responsible AI Charter

A Milestone for the Private Security Sector and Critical Infrastructure Protection

In an era where artificial intelligence (AI) is likely to reshape the security landscape, the Confederation of European Security Services (CoESS) has taken a decisive step to promote the ethical and responsible deployment of AI in security services. The launch of the CoESS Charter for the Ethical and Responsible Use of AI in European Security Services marks a crucial milestone for any type of object protected by Private Security Companies, including critical infrastructure.

Published in October 2024, this landmark document provides a much-needed ethical and operational guideline for AI adoption across the private security sector, providing an overview of AI use cases in the industry as well as recommendations for AI governance in the context of the EU AI Act. As AI-driven surveillance, threat detection, and predictive analytics become more prevalent, the need for clear ethical and compliance guidelines has never been more pressing.

Why This Charter Matters for Critical Infrastructure Protection

The increasing integration on AI in security presents both opportunities and risks. While AI enhances situational awareness, speeds up threat detection, and strengthens security operations, its use can raise concerns about privacy, bias, and accountability. For critical infrastructure sectors—ranging from energy and transport to telecommunications and finance—the responsible implementation of AI is paramount.

Recognizing these challenges, the CoESS Charter provides ten recommendations to guide AI deployment in security operations, based on values such as:

1. Compliance with Laws and Respect of Fundamental Rights

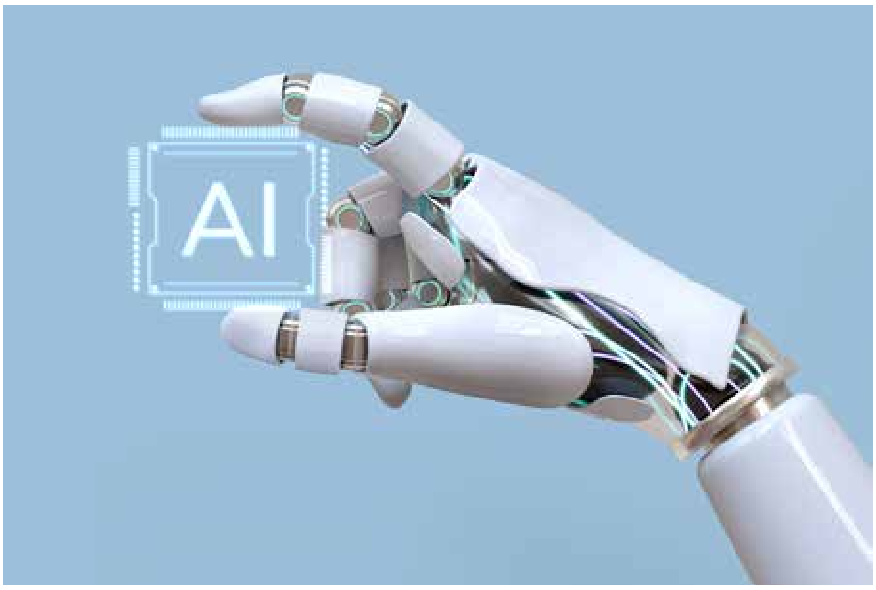
AI applications must adhere to European and national laws, including GDPR, and uphold human rights, ensuring AI-driven security measures do not infringe on privacy or fundamental freedoms. The use of AI shall further promote diversity, equality, inclusion and non-discrimination.

2. Human Oversight and Accountability

AI should assist, not replace, human decision-making in security operations. A clear chain of accountability and adequate training of staff must be maintained, ensuring that security professionals remain in control and are empowered to make informed decisions based on new insights and information.

3. Transparency and Explainability

AI-driven security measures must be transparent, and their decision-making processes should be explainable to regulators, clients, data subjects and the public.



4. Data privacy

Data governance along the deployment's value chain shall ensure the protection of European citizens' data privacy rights enshrined in the EU Charter of Fundamental rights and GDPR.

5. Robustness and Cybersecurity

AI systems and their use in security services shall be safe, resilient and secure against both physical and cyber manipulation or sabotage. They must be able to prevent, withstand and overcome incidents.

6. Proportionality and Sustainability

AI tools should be deployed only when necessary, ensuring they are proportionate to the specific use-case and the risks they mitigate. The deployment of AI shall holistically contribute to the United Nations' Sustainable Development Goals, promoting inclusive growth, (ecologically) sustainable development and well-being.

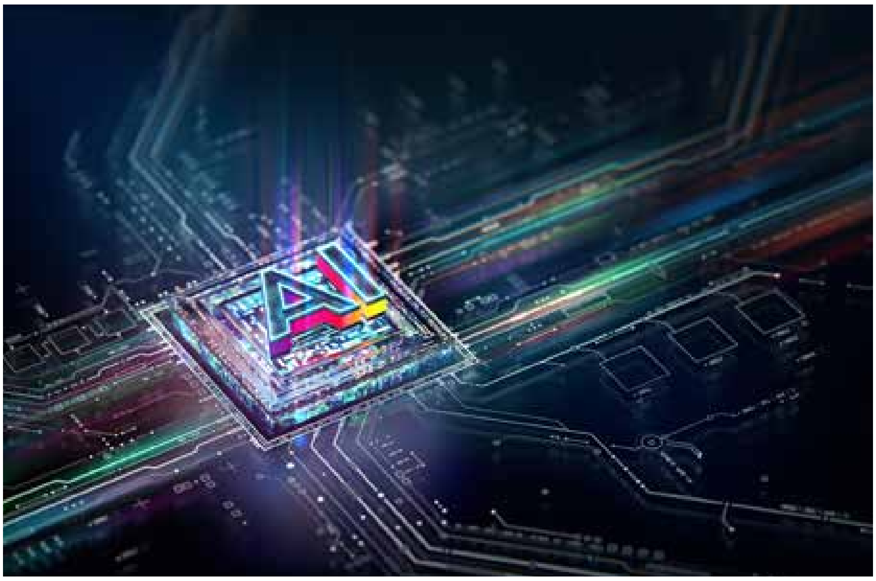
These principles can guide CI operators when deploying AI-empowered security solutions at their premises. By setting a high ethical standard, CoESS aims to promote trust in AI-driven security solutions, ensuring they are both effective and ethically sound.

Navigating the EU Regulatory Landscape

The CoESS Charter arrives at a pivotal moment, as the European Union has adopted its AI Act—the world's first comprehensive legislation on AI, with its first legal obligations applying as soon as 02 February 2025. The AI Act introduces a risk-based classification system for AI applications, with some security-related AI use cases likely falling under high-risk categories, requiring stringent compliance measures.

By proactively aligning its ethical framework with EU law, CoESS positions the private security industry as a responsible and forward-thinking stakeholder in AI governance. This not only benefits security providers but also reassures critical infrastructure operators and the public that AI in security will be developed and deployed responsibly.

The Road Ahead: Implementation and Industry Adoption



The launch of the CoESS Charter is just the beginning. Its success depends on industry-wide adoption and the integration of these principles into operational standards, procurement policies, and training programs for security professionals.

CoESS calls upon security service providers, technology developers, and critical infrastructure stakeholders to endorse and implement the Charter's principles. Through collaboration and adherence to these guidelines, the security industry can maximize the benefits of AI while mitigating its risks.

Conclusion: A Call for Ethical AI in Security

AI has the potential to revolutionize security operations, particularly in the protection of critical infrastructure. However, without ethical safeguards, AI-driven security could lead to unintended consequences, including bias, over-surveillance, and accountability gaps.

By launching the Charter for the Ethical and Responsible Use of AI in European Security Services, CoESS takes a leadership role in shaping the future of AI in security—balancing technological progress with ethical responsibility and human-centered deployment.

As AI adoption accelerates across security applications, now is the time for industry leaders, policymakers, and critical infrastructure operators to commit to ethical AI practices and high levels of compliance. CoESS has laid the foundation; it is up to the security industry to build upon it.

About the author:

Alexander Frank, CoESS Deputy Director General, Coordinator and Co-Author of the AI Charter.

Using satellite sea level tracking to anticipate storms and protect coastal areas

The ongoing 2024 Atlantic hurricane season is leaving a lasting footprint due to the resulting fatalities and infrastructure damage in coastal zones. Timely forecasts of extreme sea levels are crucial to mitigate the imminent risk that challenges the capacity of emergency response systems.

To help counter this increasing risk, scientists from the Joint Research Centre, CEDEFOP, LEGOS (France), and USC (USA) developed a global model to improve predictions of sea levels. The model incorporates satellite measurements with local atmospheric conditions.

There is an increasing consensus that human-caused global warming has intensified recent hurricanes, driving more frequent and more energetic episodic sea level along the global coastal zone.

For example, Hurricane Beryl, on which Copernicus prepared emergency maps, made history as the earliest Category 5 Atlantic hurricane on record. Category 4 Hurricanes Helene and Kirk along with Category 5 Hurricane Milton resulted in an aftermath totalling over 264 fatalities and costing $172 billion in damage.

As a result, forecasting where and when natural disasters are likely to occur is critical, and satellite measurements, with their global ocean coverage, can be key to making these forecasts more accurate.

Satellites can provide information about the sea level across the world's oceans, despite their temporal scarcity due to the long and variable revisit times of each satellite mission.

The analysis led to a continuous in-time description of the open ocean sea level for a period of 63 years, revealing both the areas of the general circulation ocean currents and the areas exposed to intense tropical cyclone activity.

Commission reports show faster progress is needed across Europe to protect waters and better manage flood risks

The European Commission is publishing its latest reports on the state of water in the European Union.

Covering the implementation of the Water Framework Directive, the Floods Directive, and the Marine Strategy Framework Directive, the reports highlight the progress made to improve the state of EU water bodies over the past six years. They also identify key areas where further efforts are needed.

The reports offer valuable insights into the condition of EU freshwater and marine waters and the actions taken to improve it, as well as measures to reduce flood risks. They also provide country-specific information and tailored recommendations to support continued progress and sustainable water management across Europe.

Information provided by the reports will play a crucial role in shaping the upcoming Water Resilience Strategy, which aims to address the most pressing water-related challenges in Europe.

More work needed to ensure water resilience

Water Framework Directive Implementation Report

The report on the implementation of the Water Framework Directive identified several positive trends. Member States have generally improved knowledge and monitoring of surface and ground water bodies, increased spending, and improved application of EU water-related legislation, though there are considerable regional differences. Most groundwater bodies also continue to achieve good quantitative and chemical status.

However, significant work is needed to meet EU targets on freshwater quality and quantity. The average health of EU surface water bodies is critical, with only 39.5% achieving good ecological status, and only 26.8% achieving good chemical status. This is mainly due to widespread contamination by mercury and other toxic pollutants.

Water scarcity and drought are also growing concerns across most of the EU.

The EU has made key recommendations to Member States to improve water management by 2027, including:

- Increase compliance with EU water laws by adhering to pollution limits, particularly nutrient pollution from agriculture, and ensuring that wastewater discharge is dealt with properly to protect the environment and human health;
- Ensure sufficient financing to address funding gaps and guarantee effective implementation of water management measures;
- Implement additional measures to address persistent environmental challenges, such as chemical pollution;
- Promote water reuse and increase efficiency and circularity to prevent aquifer overexploitation, combat illegal abstractions, and mitigate droughts.

Floods Directive Report

The assessment of the implementation of the Floods Directive shows notable improvements in flood risk management, better alignment of objectives and measures, and consideration of challenges posed by climate change.

Nevertheless, most plans failed to include quantitative targets, making it difficult to draw conclusions as to the effectiveness of flood risk management. With more frequent and severe floods in Europe, Member States need to expand their planning and administrative capacity, and adequately invest in flood prevention. To achieve this, ecosystem restoration and nature-based solutions, as well as preparedness measures like early warning systems and awareness raising, are key.

Marine Strategy Framework Directive Programmes of Measures Report

According to the report on the Marine Strategy Framework Directive, some limited progress has been made towards introducing and implementing measures to reach the Directive's objectives, particularly relating to marine litter.

Member States are encouraged to do more to achieve good environmental status of all EU marine waters, and to sustainably protect the resource base upon which marine-related economic and social activities depend.

Some key EU recommendations to achieve this include:

- Enhancing the design and implementation of measures to protect and restore marine biodiversity, and to reduce nutrient, chemical and underwater noise pollution;
- Introduction of new and improved financing and governance measures to ensure effective implementation of ambitious and coherent measures across the EU's marine environments.

Background

The report complements the European Environment Agency's State of Europe's water 2024 report.

The EU's water resources face significant pressure due to unsustainable land use, hydro-morphological changes, pollution, climate change, increased demand for water, urbanization, and growing populations.

When asked about the main threats linked to water issues in their country, the majority of Europeans mention pollution, followed by overconsumption and wasting water.

The EU's Water Framework Directive requires Member States to ensure that all surface water (lakes, rivers, transitional and coastal waters) and groundwaters achieve good quality status by 2015. This deadline can be postponed to 2027 under certain conditions.

The Floods Directive requires Member States to identify and map areas prone to flooding and develop plans to minimise risk and potential damage through Flood Risk Management Plans. Today, the Commission publishes its assessment of these for the period 2021 to 2027.

River Basin Management and Flood Risk Management Plans are developed for six-year periods. Today, the Commission publishes its assessment of these for the period 2021 to 2027.

The Marine Strategy Framework Directive (MSFD) requires Member States to assess, monitor and take measures to protect and improve the state of their seas to achieve good environmental status. The programmes of measures assessed are those submitted for the period 2021-2027. The Commission's assessment focuses on the measures that Member States developed for their respective marine strategies. These programmes are an update of the first programmes of measures reported in 2016.

GEARING UP FOR CRITICAL INFRASTRUCTURE PROTECTION & RESILIENCE NORTH AMERICA (CIPRNA)

11th-13th March 2025, Houston, TX

The 2025 Critical Infrastructure Protection and Resilience North America (CIPRNA) conference takes place in Houston, Texas in March. This will be our 6th annual conference in the United States and follows on from our very successful European event – CIPRE - which took place in Madrid in November 2024.

The event has an exciting line up of both topics and international speakers, seeking to explore the complexities and innovations in place around the protection and resilience of our Critical National Infrastructure and Information.

CIPRNA seeks to bring together leading stakeholders from industry, operators, agencies, academia and government to provide detailed insights into current policy and practices and to collaborate on the efforts required to continually address the range and complexity of challenges faced across our critical sectors.

In this era of technological advancements and dynamic global volatility, the security and resilience of our critical infrastructure are of paramount importance.

Geopolitical and technological shifts are posing as big a test as we've ever faced and when we consider all this alongside the dramatic impact of climate change, we start to understand the enormity of the challenges before us.

There can be little doubt that climate change is making natural disasters more frequent, ferocious and costly. Extreme weather events are becoming more common place. 2024 was the hottest year since records began with a year-on-year increase over the past decade and the first time it has reached 1.6 degrees higher than the pre industrial average.

We only need look at the recent wildfires in Los Angeles, the devastating floods caused by exceptionally heavy rainfall in Spain in October 2024 and the historic drought in the Amazon Basin last year, which reduced water levels to a 120 year low, as examples of real concern.

The global risk landscape is constantly changing. The safety and security of a nation depends on the ability of critical infrastructure owners and operators to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions.

The need to build resilience into preparedness planning is something that is high on the agenda for many countries and none more so than the United States. It was recently referenced by Dr. David Mussington the former Executive Assistant Director of the Cybersecurity and Infrastructure Security Agency (CISA) who stated, "It's a whole of community responsibility to prepare and secure the nation's critical infrastructure and protect the vital services it provides, so when something does happen, we are better able to respond to and recover from any impacts."

Over the course of the last four years, CISA has played a critical and evolving role in the nation's policy and strategy on cybersecurity, infrastructure security, and resilience and

they continue to do so. Their vision is for secure and resilient infrastructure for the American people and their mission is to lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

On 30th April last year, the White House released the National Security Memorandum-22 (NSM) on Critical Infrastructure Security and Resilience which updates national policy on how the U.S. government protects and secures critical infrastructure from cyber and all-hazard threats.

NSM-22 recognizes the changed risk landscape over the past decade and leverages the authorities of federal departments and agencies to implement a new risk management cycle that prioritizes collaborating with partners to identify and mitigate sector, cross-sector, and nationally significant risk.

The culmination of this cycle is the creation of the 2025 National Infrastructure Risk Management Plan (National Plan)—updating and replacing the 2013 National Infrastructure Protection Plan and will guide efforts to secure and protect critical infrastructure over the coming years.

The need to continually review, develop and update policies, practices, procedures and technologies to meet growing and changing demands is absolutely essential so it will be interesting to monitor the impact and progress of that new National Plan. That will, without doubt, be subject of considerable discussion at the conference. As will the fact that there is a new President in position whose campaign leaned heavily on the themes of economy and national security and what that may mean for the future of the protection and resilience of infrastructure and information in the United States.

As we all know, our world is constantly changing as wars, geopolitics, technology and climate change are adding further complexity in the security and resilience of our nations. As the pace of that change continues to accelerate so to must our efforts to deal with the range of challenges across the Physical, Cyber and Natural Disaster spectrums.

In seeking to address these issues there is a fantastic agenda lined up with the CIPRNA event in Houston. There are some excellent speakers covering a wide range of important topics and presenting their considered views on the way forward in protecting, securing and developing the resilience of our infrastructure and information internationally.

The conference is specifically designed to stimulate debate and as we have found at all of the events across North America and Europe, the active participation of all involved across the sessions adds real value in the development of new thinking.

The exhibition taking place alongside the conference will be showcasing some of the latest technologies that are currently being utilised internationally within both the physical and cybersecurity environments across a range of infrastructure sectors.

This will be a most rewarding and enjoyable event and I hope to see you in Houston.

John Donlon QPM FSyL
Conference Chairman
Chairman, IACIPP

critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 11th-13th, 2025
Marriott at South Hobby Airport
HOUSTON, TEXAS, USA
www.ciprna-expo.com

Securing the Inter-Connected Society

For Securing Critical Infrastructure and Safer Cities

Co-Hosted & Supported by::

International Association of CIP Professionals
INFRAGARD MEMBERS ALLIANCE HOUSTON

REGISTER TODAY
Early Bird Discount deadline February 11th,2025

SPECIAL RATES FOR GOVERNMENT AND OWNER/OPERATORS
Register by February 11th
see inside for details

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.

Preliminary Conference Programme

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

Register online at www.ciprna-expo.com

Platinum Sponsor:
3B PROTECTION

Gold Sponsors:
SIMSPACE
Deloitte.

Silver Sponsor:
JCI | Security Products

Leading the debate for securing America's critical infrastructure

Executive Sponsors:
INSTITUTE FOR HOMELAND SECURITY
AUTO-ISAC
TIA Telecommunications Industry Association
ASSOCIATION OF AMERICAN RAILROADS

Supporting Organisations:
INFRAGARD MEMBERS ALLIANCE LOUISIANA
IACI
ISIO
NSORG
STIME

Media Partner:
critical infrastructure PROTECTION AND RESILIENCE NEWS

Welcome to the 7th Critical Infrastructure Protection and Resilience North America

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).

Pursuant to CIRCIA, entities operating in critical infrastructure sectors will be obligated to report “covered cyber incidents” within 72 hours of the entity developing a reasonable belief that a cyber incident occurred. In addition, critical infrastructure entities must report ransom payments within 24 hours after a payment is made. CIRCIA delegated rulemaking authority to the Cybersecurity and Infrastructure Security Agency (CISA). We wrote about CISA’s proposed rule containing cyber incident reporting requirements in a recent article.

We must be prepared!

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

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

NSM-22 directs federal agencies to set “minimum requirements and effective accountability mechanisms for the security and resilience of critical infrastructure, including through aligned and effective regulatory frameworks.” NSM-22 goes on to direct federal agencies and departments to “utilize regulation, drawing on existing voluntary consensus standards as appropriate” to establish the minimum requirements and accountability mechanisms applicable to critical infrastructure entities. In addition, NSM-22 states that “accountability mechanisms should continuously evolve to keep pace with the Nation’s risk environment.”

NSM-22 highlights a potential “accountability mechanism” through the adoption of new requirements in the federal procurement process. For example, NSM-22 encourages federal agencies and departments to utilize “grants, loans, and procurement processes, to require or encourage owners and operators to meet or exceed minimum security and resilience requirements.” In addition, NSM-22 specifically directs the General Services Administration with ensuring that government-wide contracts for critical infrastructure assets and systems contain “appropriate audit rights for the security and resilience of critical infrastructure.”

NSM-22 also directs U.S. intelligence agencies and critical infrastructure entities to strengthen collaboration and engagement. For example, NSM-22 recommends owners and operators of critical infrastructure entities be afforded the opportunity to identify sector intelligence needs and priorities that support specific security and resilience efforts.

One of the most notable modifications contained in NSM-22 is the elevation of CISA as the national coordinator for Critical Infrastructure cybersecurity efforts across the federal government and private sector. For example, NSM-22 directs CISA to specifically identify and categorize certain critical infrastructure entities as Systemically Important Entities (SIEs).

Critical Infrastructure Protection and Resilience Americas will bring together leading stakeholders from industry, operators, agencies and governments to collaborate on securing North America.

Please register online at www.ciprna-expo.com.

We look forward to welcoming you to Critical Infrastructure Protection & Resilience North America and the Marriott Hotel at South Hobby Airport, Houston on March 11th-13th, 2025.

Register online at www.ciprna-expo.com.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Welcome from the Conference Chairman

Dear Friends and Colleagues,

Collaborating and Cooperating for Greater Security

It gives me great pleasure to invite you to join us at the Critical Infrastructure Protection and Resilience North America (CIPRNA) conference in Houston, Texas for what will be 3 days of exciting and informative presentations and discussions on securing North America's critical infrastructure and information.

This is our 6th annual conference here in the United States and follows on from our very successful European event which took place in Madrid in November 2024. This year we are delighted to have the support of a number of organisations, which include InfraGard Houston, the Telecommunications Industry Association (TIA), The International Emergency Management Society (TIEMS), the International Association of Certified ISAOs (IACI) and The International Trade Organization (ISIO)

There is an exciting line up of topics and speakers, as you will see from the very packed agenda, where we will seek to explore the complexities and innovations in place around the protection and resilience of our Critical National Infrastructure and Information.

CIPRNA seeks to bring together leading stakeholders from industry, operators, agencies, academia and government to provide detailed insights into current policy and practices and to collaborate on the efforts required to continually address the range of challenges faced across our critical sectors.

The last few years has seen the world immersed in a period with significant challenges and a great deal of uncertainty. The war between Russia and Ukraine continues unabated and we continue to see rising tension in the Middle East where on 1st October 2024, Israel invaded Southern Lebanon in an escalation of the ongoing Israel–Hezbollah conflict, a spillover of the Israel–Hamas war.

The loss of life and the utter devastation that has been caused is deeply concerning as is the obvious impact that both wars have on the position of Global Peace and Security.

The protection and resilience of our infrastructure and information systems against malicious attacks and natural disasters are crucial issues for all society. We have seen new highs in temperatures being recorded throughout 2024 and through this we have seen devastating wildfires, flooding and earthquakes and not a day goes by without there being some reference to the potential of a cyber-attack significantly affecting the very core of our critical infrastructure.

There is, therefore, a continual need to review, develop and update policies, practices, procedures and technologies to meet those growing and changing demands.

In seeking to address these issues we have a fantastic agenda lined up with some excellent speakers covering a wide range of important topics and presenting their considered views on the way forward in protecting, securing and developing the resilience of our infrastructure and information internationally.

The conference is specifically designed to stimulate debate and your active participation across the sessions will add real value in the development of new thinking.

I know you will find this a most rewarding and enjoyable event and I look forward to seeing you in Houston.

John Donlon QPM FSyI
Conference Chair

Follow us:

Critical Infrastructure Protection & Resilience

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Why Attend?

Your attendance to Critical Infrastructure Protection and Resilience North America will ensure you are up-to-date on the lastest issues, policies and challenges facing the security of America's critical national infrastructure (CNI).

You will also gain an insight in to what the future holds for North America, the collaboration and support between neighbours 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 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.ciprna-expo.com

For conference or registration queries please contact:
Ben Lane
Event Director
E: benl@torchmarketing.co.uk

Who Should Attend

Critical Infrastructure Protection and Resilience North America is for:

- Police and Security Agencies
- DHS, CISA, FEMA, TSA, DISA, GAO, NSA, NCTC, FBI and related emergency management, response and preparedness agencies
- Emergency Services
- National government agencies responsible for national security and emergency/contingency planning
- Local Government
- CEO/President/COO/VP of Operators of national infrastructure
- Security Directors/Managers of Operators of national infrastructure
- CISO of Operators of national infrastructure
- Facilities Managers – Nuclear, Power, Oil and Gas, Chemicals, Telecommunications, Banking and Financial, ISP's, water supply
- Information Managers
- Port Security Managers
- Airport Security Managers
- Transport Security Managers
- Event Security Managers
- Architects
- Civil Engineers
- NATO
- Military
- Border Officials/Coast Guard

Join us in Houston, Texas for Critical Infrastructure Protection and Resilience North America and join the great debate on securing America's critical infrastructure.

"Disruption to infrastructures providing key services could harm the security and economy of North America as well as the well-being of its citizens."

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Exhibition Opening Hours		On-Site Registration Hours	
Tuesday March 11th	1.00pm to 7.30pm	Tuesday March 11th	8.00am to 6.00pm
Wednesday March 12th	9.00am to 5.30pm	Wednesday March 12th	8.30am to 5.00pm
Thursday March 13th	9.00am to 4.30pm	Thursday March 13th	8.30am to 4.00pm

REGISTER ONLINE AT WWW.CIPRNA-EXPO.COM

Register Online Today at www.ciprna-expo.com/register

REGISTRATION

The Critical Infrastructure Protection & Resilience North America is open and ideal for members of federal government, emergency management agencies, emergency response and law enforcement or inter-governmental agencies, DHS, CISA, FEMA, TSA, DISA, GAO, NSA, NCTC, FBI, Fire, Police, INTERPOL, AMERIPOL and associated Agencies and members (public and official) involved in the management and protection of critical national infrastructure.

The Conference is a must attend for direct employees, CSO, CISO's and security, fire and safety personnel of critical infratructure owner/operators.

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

EARLY BIRD DISCOUNT - deadline February 11th, 2025

Register yourself and your colleagues as conference delegates by February 11th, 2025 and save with the Early Bird Discount. Registration details can be found at www.ciprna-expo.com/register.

REGISTER ONLINE TODAY AT WWW.CIPRNA-EXPO.COM/REGISTER

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 North America, then you can benefit from a special discount on standard rates:

- INFRAGARD Houston and INFRAGARD Louisiana
- The International Emergency Management Society (TIEMS)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- International Security Industry Organization (ISIO)
- International Association of Certified ISAOs (IACI)

Check the Registration Information at www.ciprna-expo.com/registration-fees

Schedule of Events

Tuesday March 11th, 2025

8.30am - 12.30pm - Site Visit (for delegates registered for the site visit)

1:00pm - Exhibition Opens

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

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

4.00pm-5:30pm - Session 1: NSM22 Strategies to All Hazards, One Response: Navigating Cyber, Natural, and Man-Made Threatss

5:30pm - Networking Reception in Exhibition Hall

Wednesday March 12th, 2025

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: Power & Energy Sector (Grid Resilience) Symposium

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

4:15pm - 5:30pm - Session 5a: Food & Agriculture Sector Symposium

Track Two

9:00am-10:30am - Session 2b: Cybersecurity and AI - Best Practice and Minimum Standards

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

11:15am - 12:30pm - Session 3b: Maritime and Port Security Sector Symposium

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

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

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

4:15pm - 5:30pm - Session 5b: Oil & Gas Sector Symposium

Thursday March 13th, 2025

9:00am-10:30am - Session 6a: IT OT Threats

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

11:15am - 12:30pm - Session 7a: Modeling and Methodology Around Incident Mitigation & Emergency Management

9:00am-10:30am - Session 6b: Strategic Resilience Planning & Risk Mitigation

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

11:15am - 12:30pm - Session 7b: Technologies to Detect and Protect

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

2pm-3:30pm - Session 8: Collaboration, Information Sharing and Enhancing PPPs

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

4.30pm - Expo Close

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

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Tuesday March 11th

Conference Programme

2:00pm-3:30pm - OPENING KEYNOTE

Chair: John Donlon QPM, FSI

International adviser on security intelligence

Steven Harris, Deputy Executive Assistant Director for Infrastructure Security, Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA)

Nim Kidd, Chief of the Texas Division of Emergency Management (TDEM)*

Mayor of Houston*

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

4:00pm-5:30pm - Session 1: NSM22 Strategies to All Hazards, One Response: Navigating Cyber, Natural, and Man-Made Threats

All Hazards, One Response highlights the interconnectedness of cyber, natural, and man-made threats. It emphasizes the need for a comprehensive approach to risk management, resilience, and emergency response. In the context of the new NSM 22 and critical infrastructure, this means developing strategies that address a wide range of threats, fostering collaboration among stakeholders, and implementing robust security measures to protect vital assets.

Chair: **Paul Titus, Director, Critical Infrastructure Security and Resilience, INL**

Derek Padden, President, Blue Glacier Management Group

Robert Russell, Regional Director (A) for Region 6, Cybersecurity and Infrastructure Security Agency (CISA)

Andy Bochman, Senior Grid Strategist, INL

Marco Ayala, President, Infragard Houston

5:30pm-7:30pm - Networking Reception in Exhibit Hall

---

*invited

Wednesday March 12th

Track One

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

This session reviews the dynamic landscape of threats against CI, which include climate, terrorism, insider threats, and cyberattacks including the emerging challenges asserted by AI, which necessitate a proactive approach to security. To effectively address these emerging challenges, it is crucial to identify, monitor, and assess their potential impact. By continuously reviewing and updating policies, practices, and technologies, organizations can enhance their resilience and mitigate risks.

Janna White, Special Agenct for Houston Infragard, FBI*

Cyber Threats to the US Critical Infrastructure in an Era of Geopolitical Tensions - Chris Essid, Senior Advisor, Public Safety Information Technology, Cybersecurity and Infrastructure Security Agency (CISA)

Sunil Madhugiri, Chief Architect and Chief Technology Officer (CTO) for Office of Information and Technology, US Customs & Border Protection

Managing Unmanned Aircraft System (UAS) Risks to Critical Infrastructure - Michael Hill, Program Specialist, CISA

Dominic Dillon, Founder & CEO, 3B Protection

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

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

Communications is key to any community and its infrastructure assets has become increasingly threatened. Without communications, business will be lost, and any emergency coordination would be a disaster. The internet has become a vital part of communications for all. Protection of communication assets and their resilience is vital for businesses, government and all sectors of CI.

CISA Priority Telecommunications Services - Enhance Your Emergency Communications Capability - Colleen Wright, Outreach/Acquisitions Specialist, CISA

Research Supporting Security Testing Capabilities Relating to Telecommunications Equipment - Eileen Rubin, Program Manager, Department of Homeland Security, Science and Technology

Mike Regan, VP, Business Performance, Telecomms Industry Association (TIA)

Securing critical telecom networks against cyber threats - Nelson Silva, Senior Product Line Manager - Nokia Cybersecurity

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

Track Two

9:00am-10:30am - Session 2b: Cybersecurity and AI - Best Practice and Minimum Standards

The threat of cyber-attacks by state actors and hacktivists, such as criminals and malicious rogue players, grows ever higher to cause disruption to our infrastructures, how do we assess and prioritise these risks and threats to better build cyber resilience? What role can AI play, and as a potential threat in itself, how do we regulate AI to build trust in its development and use? How can we report incidents for the benefit of everyone to better understand these threats?

An Approach to Artificial Intelligence (AI) Informational Activities - Ron Martin, Capitol Technology University

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

UAS Cybersecurity: Building Cyber-Resilient Unmanned Aircraft Systems (UAS) Fleets for Critical Infrastructure - Michael Lees, Program Specialist, Infrastructure Security, CISA

Simulating Tomorrow's Security: The Critical Role of OT in Disaster Recovery Preparedness - Graham Westbrook - VP of Sales Engineering, SimSpace

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

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

The Maritime and Port Security Sector is a critical component of national infrastructure. Ports serve as gateways for trade and commerce, while maritime routes facilitate global transportation. To protect this vital sector, robust security measures are essential, including surveillance, law enforcement, and international cooperation. This session will explore the current security threats, as well as risk mitigation through planning, preparation and best practices.

Lester Millet, Head of Security, Port of Louisiana & President, Infragard LA

Better Preparation for Long-Term Maritime Transportation System (MTS) Emergencies and DoD National Security Campaigns - Kelly Wilson, Idaho National Laboratory

Ed Landgraf, Chairman, Coastal And Marine Operators

The Path to Total Resiliency for Safe Harbors - Joe Morgan, Segment Development Manager – Critical Infrastructure, Axis Communications

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

Wednesday March 12th

Track One

2:00pm-3:30pm - Session 4a: Power & Energy Sector (Grid Resilience) Symposium

The energy sector has become the most critical of sectors. Without power, driven by oil, gas and renewable energies, all other CI stops. Recent cyber attacks on the energy sector, as well as natural hazards, from hurricanes in the Gulf to fires in California, gives much room for thought on how we best protect our most vital assets, including IT/OT and SCADA systems. How can we mitigate the impact of an attack or outage on the wider community and society, and build greater grid resilience?

Chair: Tommy Waller, President and CEO, Center for Security Policy

Physical security solutions for the grid - Rob Velasco, CIP Global Ventures

Cybersecurity from the utility perspective - John Miri, President, Electric Grid Cybersecurity Alliance

EMP protection from a utility perspective - Eric Easton, Ph.D., P.E., Vice President, Grid Transformation and Investment Strategy, Centerpoint Energy

Protecting the Grid from Solar Weather & HEMP's Ground Induced Currents - David Anderson

COO, VP, EMPRIMUS, USA

Grid protection & the role of state legislators - Senator Bob Hall, State Senator, Texas Senate District 2, Texas State Senate

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

4:15pm-5:30pm - Session 5a: Food & Agriculture Sector Symposium

The Food & Agriculture Sector faces a myriad of threats and risks. Climate change, natural disasters, criminals, and geopolitical tensions can disrupt food production and distribution; having cascading effects on economies. Additionally, cyberattacks and supply chain vulnerabilities pose significant challenges to food and national security. To mitigate these risks, robust measures are essential, including: sustainable farming practices, resilient supply chains, critical infrastructure protection initiatives, and effective risk management strategies.

Chair: Holli Tietjen, Director of Emergency Management, Texas Animal Health Commission

"AgroGuard" and Engaging Producers, Supply Chain Intro - Marshal Willson, State of New Mexico's Co-Director of the Southwest Border Food Protection and Emergency Preparedness Center

Interconnected Infrastructure Sectors and Information Sharing - Dan Frazen, State of Colorado's Agriculture Emergency Coordinator and Lead for the Rocky Mtn AgSecure Working Group

Technologies to protect agriculture and proactive work of academia - Robert Crane, Program Executive – Public Sector, Energy Security and PNT, Institute for Homeland Security, Sam Houston State University

Track Two

2:00pm-3:30pm - Session 4b: 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.

Chris Engelbrecht CSP, Safety and Emergency Management Director, Missouri Department of Transportation

Senior Representative, Transport Security Administration (TSA)

Faye Francy, Executive Director, Automotive Information Sharing and Analysis Center (Auto-ISAC)

Janet St. John, Director of Cybersecurity, Association of American Railroads

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

4:15pm-5:30pm - Session 5b: Oil & Gas Sector Symposium

The oil and gas sector faces significant threats and challenges from cyberattacks, physical sabotage, natural disasters, and geopolitical tensions, which pose a constant risk to the industry's operations and supply chain. Aging infrastructure, lack of cybersecurity expertise, and regulatory complexities further exacerbate these challenges. Protecting CI in this sector requires a comprehensive approach that addresses both physical and cyber threats, investing in resilient infrastructure, and fostering industry collaboration.

Chair: Marco Ayala, Infrgard Houston

Research Supporting the Cybersecurity of Industrial Control Systems (ICS) - Eileen Rubin, Program Manager, Department of Homeland Security, Science and Technology

California's Emergency Fuel Planning for Catastrophic Events - Stacie Neal, Senior Critical Infrastructure Analyst, Idaho National Lab

TBC

Thursday March 13th

Track One

9:00am-10:30am - Session 6a: IT OT Threats

IT-OT convergence in critical infrastructure has increased the risk of cyberattacks. Malicious actors can exploit vulnerabilities in IT systems to compromise operational technology (OT), leading to disruptions, damage, and even safety hazards. To mitigate these threats, organizations must implement robust cybersecurity measures, including network segmentation, access controls, and incident response plans. Fostering collaboration between IT and OT teams is essential for effective risk management.

Data and Analysis Imperatives across Information and Operational Technology Environments - David Carroll, Engineering, Cybersecurity, CISA

The OSS Maze: Understanding the Cybersecurity Risks - Norman Speicher, Program Manager, OSS, Department of Homeland Security

Industry/Government Collaboration on Hunting for Living-of-the-Land Techniques in OT Environments - Matthew Kress-Weitenhagen, Control Systems Cybersecurity Analyst , Dept. of Energy CESER – Energy Threat Analysis Center

Critical Infrastructure adoption of Zero-Trust Protection - Ron Martin, Professor of Practice, Cap Tech Uni / Dr Jayne Suess / Leighton Johnson

Securing Unmanned Infrastructure - Guerry Bruner, Program Manager, ITS & Unmanned Infrastructure, ASSA ABLOY Opening Solutions

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

11:15am-12:30pm - Session 7a: Modeling and Methodology Around Incident Mitigation & Emergency Management

Predicting how threats can impact business continuity of critical assets can be of major benefit for planning resiliency or emergency response. This affects both financial and resource planning. So what are the latest roles and assessments in modeling and methodology? What role can machine learning and AI play in building more accurate predictions and what measures can be put in place to mitigate risk?.

Chemlock - Douglas Frey, Supervisory Chemical Security Inspector, CISA

Positioning, Navigation and Timing (PNT) Capabilities - Michael Wilbur, Program Manager, PNT, Department of Homeland Security, Science and Technology

Modeling Cyber Supply Chain Incidents with Multilayered Graph Motifs - Gabriel Weaver, Senior Critical Infrastructure Analyst, Idaho National Laboratory

The Security of Crowded Places - Sarah Jane Prew, Arup UK

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

Track Two

9:00am-10:30am - Session 6b: Strategic Resilience Planning & Risk Mitigation

Being prepared for the changing threat environment can benefit greatly in mitigating its impact on infrastructure and the broader community, ensuring resilience, safety and security. How to we develop and plan the best resilience strategies within our CI community? Through discpline in information sharing and making infrastructure preparedness personal, we can help to build resilience into our infrastructures that benefit the whole community.

Securing Your Chemicals Against Everchanging Threats - Chris McNeely, Management and Program Analyst, Office of Chemical Security, Cybersecurity and Infrastructure Security Agency (CISA)

Developments in Bombing Prevention Security and Resilience - Douglas DeLancey, Office for Bombing Prevention, CISA

Enhancing ICT Critical Infrastructure Resilience: Exploring AI and Software Assurance - Laura Hershon, Program Analyst, National Risk Management Center, CISA

Addressing Consequence within Operational Risk: Why threats and security are just not that important! - Ollie Gagnon, Chief Homeland Security Advisor, Idaho National Laboratory

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

11:15am-12:30pm - Session 7b: 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.

Securing the Gatekeepers: Protecting Access Control Systems in Critical Infrastructure - Joey Yanire, LEGIC Identsystems Ltd

How to Manage and Unify Disparate Physical Security Systems - Thomasina Martin, Key Account Manager, Genetec Inc

Extending Perimeters to the Sky: Drone Incursion Stories & Solutions - David Lewin, Regional Sales Manager East, Echodyne

Dominic Dillon, Founder & CEO, 3B Protection

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

Thursday March 13th

2pm-3:30pm - Session 8: Collaboration, Information Sharing and Enhancing PPPs

Information sharing and cooperation is crucial for effective risk management and resilience planning. By fostering collaboration among government, operators, and communities, we can enhance the protection of critical infrastructure. However, barriers to information sharing persist. To overcome these challenges, we must build trust and create a supportive environment that encourages open communication and knowledge exchange.

Moderator: John Donlon QPM FSI

Clint Ladd, Texas Critical Infrastructure Protection Coordinator, Texas Department of Public Safety

Public Private Partnerships to Increase Community Preparedness- how the CAER group trains and exercises with local emergency management and hazmat teams - Josie Ross, Emergency Management Officer, City of Henderson

Central Texas Public Safety Commission Infrastructure and Public Safety Partnerships - Robert Clark, Executive Director, CTPSC

Gary Scheibe, Chairman, Houston Ship Channel Security District (HSCSD)

Enhancing critical infrastructure security through advanced technologies and multi-agency collaboration - Christopher Blake Carver, MPA, ENP, CPSL, Director of Market Development, Hexagon

---

Questions, Discussion, Round Up and Conference Close by John Donlon QPM, FSI, Conference Chairman

---

Networking Reception

Tuesday March 11th
5.30pm - 7:30pm
Exhibition Floor

We invite you to joins us at the end of the opening day for the Critical Infrastructure Protection & Resilience North America Networking Reception, which will see the CNI security industry management professionals gather for a more informal reception, in a Covid compliant environment.

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.

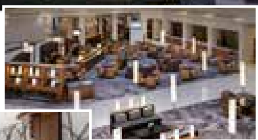
The Networking Reception is free to attend and open to industry professionals.

We look forward to welcoming you.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

The Venue and Accommodation

Houston Marriott South at Hobby Airport
9100 Gulf Fwy
Houston
TX 77017



Enjoy new heights of comfort at Houston Marriott South at Hobby Airport. Begin your stay with a complimentary shuttle to and from William P. Hobby Airport. Stay a short drive from prominent local attractions at our Houston hotel near Hobby Airport, like the University of Houston and NRG Park. Indulge in a savory steak or a signature cocktail from Latitude 29, our on-site restaurant, where we serve classic American favorites in a chic atmosphere. For your next conference or special event, shake things up with the help of our 12 event venues, custom catering and event planners. Wake up to a delicious breakfast and fuel up with Starbucks coffee. After a busy day or a long flight, relax in upscale guest rooms and suites boasting pillowtop mattresses and room service all available at our Houston, Texas, hotel near Hobby Airport. No matter the reason, Houston Marriott South at Hobby Airport offers an elevated experience for a good time in Houston.

For more details on the hotel and online booking visit **www.ciprna-expo.com/accommodation**

Booking Your Accommodation

Special Room Rate for CIPRNA Delegates – $150 prpn (excl taxes)

Promo Code: **CIPRNA**

Book your hotel accommodation at the **Houston Marriott South at Hobby Airport** at **www.ciprna-expo.com/hotel-booking**

Delegates/attendees can make reservations in the following way:

- Online: Reservations can be made online at www.ciprna-expo.com/hotel-booking

Click on the link, complete your information and quote Promo Code CIPRNA to get your CIPRNA group booking rate.

Special Group Rate ends 17th February

We look forward to welcoming you to Houston, TX.

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Why participate and be involved?

Critical Infrastructure Protection and Resilience North America provides a unique opportunity to meet, discuss and communicate with some of the most influential critical infrastructure protection, safer cities 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 North America gives you a great opportunity to meet key decision makers and influencers.

www.ciprna-expo.com

How to Exhibit

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

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

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

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

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 here.

- Platinum Sponsor - $14,950
- Gold Sponsor - $10,500
- SIlver Sponsor - $8,950
- Bronze Sponsor - $6,950
- Conference Proceedings Sponsor - $4,950
- Site Visit Sponsor - $4,500
- Delegate Folder Sponsor - $4,500
- Networking Reception Sponsor - $3,500
- Coffee Break Sponsor - $3,500
- Lanyard Sponsor - $3,500
- Badge Sponsor - $3,500

Packages can be designed and tailored to meet your budget requirements and objectives.
Please enquire for further details.

Exhibiting Investment

The cost of exhibiting at the Critical Infrastructure Protection & Resilience North America conference is:

Table Top Exhibit 5’x7’ - $3,000
Table Top Exhibit 10’x10’ - $4,950
Raw space with 1 x table and 2 x chairs, pipe and drape, electrical socket, wi-fi, 1 Exhibitor Delegate pass with full conference access, lunch and coffee breaks included, listing in the official event guide and website.

Exhibitors also benefit from a 50% discount on Conference Delegate Fees.

ASK ABOUT OUR BOOKING BUNDLES FOR EXTRA EXPOSURE

ALL PRICES SUBJECT TO 8.25% HOUSTON/TEXAS SALES TAX

A Homeland Security Event For Securing Critical Infrastructure and Safer Cities

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience North America 2025.

Platinum Sponsor:

3B PROTECTION — BALLISTIC / BLAST / BREAK-IN

Supported & Co-Hosted by:

International Association of CIP Professionals

INFRAGARD Members Alliance Houston

Gold Sponsors:

SIMSPACE

Deloitte.

Bronze Sponsors:

Genetec

ECHODYNE

Silver Sponsors:

JCI | Security Products

Coffee Break Sponsor:

AXIS Communications

Lanyard Sponsor:

CAPITOL Technology University

Executive Sponsors:

Institute for Homeland Security

AUTO-ISAC

TIA Telecommunications Industry Association

Association of American Railroads

Bag Sponsor:

Hanwha

Supporting Organisations:

INFRAGARD Members Alliance Louisiana

IACI

STIME

ISIO

Help2Protect

Flagship Media Partner:

critical infrastructure Protection and Resilience News

Media Supporters:

govCIO Outlook

BIOMETRIC UPDATE.COM

World Security-index.com

BORDER SECURITY REPORT

CIO Review Europe

Cyber Security Review

Owned & Organised by:

TORCH

DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS

Book your delegate place by 11th February 2025 and save with the Early Bird rate

REGISTRATION IS SIMPLE

1. Register online at www.ciprna-expo.com/register
2. Complete this form and email to: ciprna@torchmarketing.co.uk
3. Complete this form and mail to: CIPRNA 2025, Torch Marketing, 200 Ware Road, Hoddesdon, Herts EN11 9EY, UK.

DELEGATE DETAILS

(Please print details clearly in English. One delegate per form, please photocopy for additional delegates.)

Title: ________ First Name: ________________________

Surname: ____

Job Title: ____

Company: ____

E-mail: ____

Address: ____

Street: ____

Town/City: ____

County/State: ____

Post/Zip Code: ____

Country: ____

Direct Tel: (+) ____

Mobile: (+) ____

Direct Fax: (+) ____

Signature : ________________________ Date: ___________

(I agree to the Terms and Conditions of Booking)

CONFERENCE FEES

GOVERNMENT, MILITARY AND PUBLIC SECTOR/AGENCY
Individual Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and 2 lunches)

- ☐ Paid before 12th February 2025 .... $195
- ☐ Paid on or after 12th February 2025 .... $295

OPERATORS/OWNERS OF INFRASTRUCTURE
Individual Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and 2 lunches)

- ☐ Paid before 12th February 2025 .... $195
- ☐ Paid on or after 12th February 2025 .... $295

COMMERCIAL ORGANISATIONS
Individual Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)

- ☐ Paid before 12th February 2025 .... $595
- ☐ Paid on or after 12th February 2025 .... $895

Exhibitor Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch)

- ☐ Paid before 12th February 2025 .... $295
- ☐ Paid on or after 12th February 2025 .... $450

Student Full Conference
(includes 3 day conference, conference proceedings, keynote, exhibition, networking reception, coffee breaks and lunch) - Student ID required

- ☐ Paid before 12th February 2025 .... $195
- ☐ Paid on or after 12th February 2025 .... $195

☐ **Conference Proceedings only** $495

☐ **EXHIBITION ONLY** (on-site registration $50) $10
(includes access to exhibition floor only)

Terms and Conditions of Booking

Payment: Payments must be made with the order. Entry to the conference will not be permitted unless payment has been made in full prior to 11th March 2025.
Substitutions/Name Changes: You can amend/change a delegate prior to the even start by notifying us in writing. Two or more delegates may not 'share' a place at an event. Please ensure separate bookings for each delegate. Torch Marketing Co. Ltd. reserve the right to refuse entry.
Cancellation: If you wish to cancel your attendance to the event and you are unable to send a substitute, then we will refund/credit 50% of the due fee less a $100 administration charge, providing that cancellation is made in writing and received before 12th February 2025. Regretfully cancellation after this time cannot be accepted. If we have to cancel the event for any reason, then we will make a full refund immediately, but disclaim any further liability.
Alterations: It may become necessary for us to make alterations to the content, speakers or timing of the event compared to the advertised programme.
Data Protection: Torch Marketing Co. Ltd. gathers personal data in accordance with the UK Data Protection Act 1998 and we may use this to contact you by telephone, fax, post or email to tell you about other products and services.
Please tick if you do not wish to be contacted in future by:

☐ Email ☐ Post ☐ Phone ☐ Fax

PAYMENT DETAILS

(METHOD OF PAYMENT - 8.25% SALES TAX WILL BE ADDED TO FEES.)

☐ Wire Transfer (Wire information will be provided on invoice)

☐ Credit Card
Invoice will be supplied for your records on receipt of the order/payment.

Please fill in your credit card details below:
☐ Visa ☐ MasterCard

All credit card payments will be subject to standard credit card charges.

Card No: ____

Valid From ____ / ____ Expiry Date ____ / ____

CVV Number ______ (3 digit security on reverse of card)

Cardholder's Name: ________________________________

Signature: ______________________________ Date: __________
I agree to the Terms and Conditions of Booking.

Complete this form and email to ciprna@torchmarketing.co.uk

Infragard Building Cross-sector Collaboration for Enhancing Resilience

The recent InfraGard Congress and Awards in Orlando underscored the critical importance of collaboration between the FBI and the private sector in protecting our nation's infrastructure. The outgoing FBI Director's keynote speech celebrated InfraGard's achievements, highlighting how this partnership has revolutionized national security through real-time information exchange, educational initiatives, and cooperation across various sectors. He emphasized the program's ongoing significance in an ever-changing threat environment, where cyber and physical threats are increasingly linked. With the introduction of the new Director, there's a renewed hope for even stronger alliances and more robust protection strategies. The new Director will enable collaboration to enhance infrastructure security, pledging to leverage cutting-edge technologies and foster deeper public-private partnerships for a safer, more resilient America.

The Value of InfraGard

InfraGard serves as a vital link between private sector leaders, critical infrastructure operators, and the FBI. It has grown into a fundamental part of our national security framework. Its membership, which includes business leaders, IT specialists, security professionals, military personnel, and law enforcement officers, forms a diverse group all dedicated to safeguarding our critical infrastructure.

What makes InfraGard unique is its role in knitting together different industries, creating a space where actionable intelligence and new threats can be shared efficiently among all parties involved. With its offerings of workshops, educational programs, and networking opportunities, InfraGard equips its members to predict and neutralize risks preemptively, making it an indispensable asset in bolstering our nation's resilience against threats.

Cross-Sector Collaboration: A Unique Strength

InfraGard's strength lies in its focus on cross-sector collaboration. The Houston InfraGard Members Alliance (HIMA) Chapter program has established numerous Cross-Sector Councils (CSCs), each designed to address the specific challenges faced by critical infrastructure sectors. These councils serve as a forum for sharing best practices, discussing emerging threats, and developing strategies to enhance security. InfraGard's CSCs include:

- Artificial Intelligence Cross-Sector Council
- Banking and Financial Services Cross-Sector Council
- Bryan/College Station Cross-Sector Council
- Coastal Bend Cross-Sector Council

- Countering Human Trafficking Cross-Sector Council
- Defense Industrial Base Cross-Sector Council
- Education Cross-Sector Council
- Energy Cross-Sector Council
- Healthcare Cross-Sector Council
- Legal Cross-Sector Council
- Maritime Domain Cross-Sector Council
- Public Venues Cross-Sector Council
- Security Executives Cross-Sector Council
- Southeast Texas Cross-Sector Council
- Technology Cross-Sector Council
- Telecommunications Cross-Sector Council
- Transportation Cross-Sector Council

These councils empower members to engage in meaningful dialogue and collaborate on sector-specific challenges while aligning with broader national security goals. By focusing on areas such as artificial intelligence, maritime security, and telecommunications, InfraGard ensures that every facet of critical infrastructure receives the attention and expertise it requires.

Houston InfraGard Members Alliance: Leading the Charge

The Houston InfraGard Members Alliance (HIMA) has established itself as one of the most dynamic and impactful chapters in the InfraGard network. Nestled in the heart of a region that's a hub for energy, maritime trade, healthcare, and technology, HIMA's work is indispensable for securing assets that are pivotal not only to Houston but also to the nation's overall resilience.

HIMA is renowned for its ability to forge strong partnerships between an eclectic mix of stakeholders—from executives in the energy sector to public safety officials. The chapter's dedication to providing high-quality education and training ensures that its members are well-prepared to confront the unique challenges faced by Houston's critical infrastructure. HIMA's engagement with the Energy Cross-Sector Council and the Maritime Domain Cross-Sector Council underlines the region's crucial role in global energy production and international trade.

The events hosted by HIMA are

often looked upon as a model for how InfraGard chapters can address local issues while contributing to the broader goals of national security. By nurturing collaboration among industries, government agencies, and law enforcement, HIMA not only protects Houston but also strengthens the interdependent infrastructure that keeps the entire country running. These events are not just about networking; they're about building a community of practice where the sharing of knowledge and resources directly translates into enhanced security measures.

The Value of Events Like CIPRNA

In addition to its local efforts, InfraGard recognizes the importance of national and international events like the Critical Infrastructure Protection and Resilience North America (CIPRNA) conference. Events like CIPRNA provide a global platform for addressing the evolving challenges faced by critical infrastructure sectors.

CIPRNA focuses on securing critical infrastructure through innovation, collaboration, and proactive risk management. By bringing together experts from diverse fields, it fosters an environment where new technologies, strategies, and policies can be explored and refined. Key topics often include risk mitigation, incident response, and the integration of emerging technologies like artificial intelligence and blockchain into infrastructure security.

The relevance of such events cannot be overstated. They provide attendees with actionable insights and foster relationships that transcend regional and national boundaries. For HIMA members, events like CIPRNA offer a valuable opportunity to showcase the chapter's leadership in infrastructure protection while gaining insights that can be applied locally.

HIMA in Action: Case Studies and Initiatives

To illustrate HIMA's impact, consider the case of a recent cybersecurity threat that targeted the energy sector in Houston. HIMA's swift response, coordinated through its network, involved sharing real-time threat intelligence with members, thereby preventing widespread disruption. This incident highlighted how HIMA's local knowledge, combined with the broader insights from InfraGard, can effectively counter even the most sophisticated threats.

Moreover, HIMA has been instrumental in initiating programs aimed at enhancing physical security in the port areas, understanding the unique vulnerabilities that arise from Houston's role as a major maritime gateway. Through these initiatives, HIMA has not only fortified individual sites but also contributed to broader safety policies and practices that benefit the entire maritime community.

Community Engagement and Education

Education is another pillar of HIMA's strategy. Regular workshops, seminars, and training sessions are held to keep the community informed about the latest security threats and resilience strategies. These educational efforts extend beyond just the members; they reach out to schools, universities, and even the general public to raise awareness about cybersecurity and infrastructure protection.

HIMA's community outreach also includes partnering with local emergency services for drills and simulations, ensuring that in the event of a real crisis, the response would be as coordinated and effective as possible. These exercises have proven invaluable, providing practical experience that prepares everyone from first responders to corporate security teams for real-world scenarios.

Looking Forward: The Role of InfraGard in a Changing World

As we look towards the future, the role of InfraGard, and specifically chapters like HIMA, becomes increasingly vital. The landscape of threats is ever-evolving, with new technologies bringing both opportunities and vulnerabilities. The integration of IoT devices, the rise of smart cities, and the increasing reliance on digital infrastructure mean that the threats are not just more numerous but also more complex.

In this context, InfraGard's mission is more crucial than ever. The organization must continue to adapt, ensuring that its members are at the forefront of both understanding and mitigating these risks. Events like the InfraGard Congress and CIPRNA are essential for this adaptation, providing platforms for learning, collaboration, and innovation.

Horizon

InfraGard's mission of protecting the nation's critical infrastructure has never been more vital. From the program's overarching framework of collaboration to the local efforts of chapters like the Houston InfraGard Members Alliance, the impact of InfraGard is far-reaching and profound. Events like the InfraGard Congress and CIPRNA further amplify this impact, providing platforms for learning, collaboration, and innovation.

As threats continue to evolve, the importance of programs like InfraGard and events like CIPRNA will only grow. Together, they ensure that the United States remains resilient, adaptive, and prepared to meet the challenges of an increasingly complex world.

Join the Patriots Circle https://www.infragardnational.org/infragard-patriots-circle

Marco (Marc) Ayala, President, Houston InfraGard Members Alliance

Counter-Drone Technology for Critical Infrastructure: Your Layered Security Stack is the Sum of Its Parts

The rapid and emerging proliferation of drones, or unmanned aerial vehicles (UAVs), is two-fold: drones for good and drones for bad. On the positive side, drone technology is transforming industries, from delivering goods, to capturing aerial imagery for search and rescue missions, aiding in disaster response, and beyond. However, much like any technology, bad actors having the same accessibility to drones poses clear and present dangers, particularly to the Nation's critical infrastructure.

Take for example the sheer increase in drone activity around airports. A recent report from the U.S. Government Accountability Office (GAO) revealed that, since 2021, the Transportation Security Administration (TSA) has documented over 2,000 drone sightings near U.S. airports, with major airports experiencing incidents almost daily. Between 2021 and 2022, 63 of these incidents forced pilots to take evasive maneuvers, including four cases involving commercial airplanes.

Similar unnerving events are taking place around energy utilities, with a mix of unauthorized sightings and downright concerted efforts to wreak havoc. Perhaps the most alarming example of late was the recent attempt of a drone operator to launch a UAV armed with explosives at an electric substation in Nashville.

Further complicating the scene are the limitations on what exactly can be done when a drone enters the airspace at a critical infrastructure site. Under current U.S. federal laws, security teams and law enforcement are strictly prohibited from stopping a drone in flight, even if it poses a clear and immediate threat and is flying where it's not supposed to. This is because these small aircraft hold the same protections as any other aircraft operating in the National Airspace System (NAS). That is, they can't be tampered with, shot down, or mitigated against, unless by the Departments of Justice (DOJ), Homeland Security (DHS), Energy (DOE), or Defense (DOD).

From nuclear, gas, and electric facilities, bridges, dams, communication networks and other assets, these vital sites face escalating threats from unauthorized drone activity and the current limitations to how security teams can handle incursions. Whether used for surveillance, smuggling, or potential sabotage, drones demand sophisticated countermeasures.

To protect critical infrastructure effectively, a multi-layered security stack—centered on radar, optical, and radio frequency (RF) sensors—provides the robust, integrated solution that security teams need to protect critical infrastructure. At the heart of

this system is early detection, which provides security teams the opportunity to assess drone threats to the nearby airspace, and when necessary, respond to drone threats, including facilitating a law enforcement response to minimize the drone threat.

Making the Case for a Multi-Layered Security System

Due to the multiple ways in which drones can navigate through the airspace, a multi-layered drone detection system is required to provide comprehensive airspace awareness around critical infrastructure facilities. A layered security system functions as a precisely tuned orchestra, where each component works in harmony to deliver a comprehensive security strategy.

Singular technologies, while effective in isolated tasks, often leave critical gaps that can be exploited. For this reason, experts in the counter-drone industry often say that "no sensor can act alone". Instead, a great security system is the sum of its parts.

The true essence of a layered system lies in its adaptability and discernment. High-end systems allow for customizable settings, optimizing detection by either prioritizing sensitivity—alarming when any sensor is triggered—or reducing false positives by requiring multiple sensors to confirm an alert. This flexibility not only enhances the likelihood of identifying stealth or uncommon drones, but also minimizes unnecessary disruptions, tailoring system performance to specific operational needs.

Such integration improves situational awareness, giving security teams the critical time and accurate data needed to respond effectively. In a landscape where split-second decisions can dictate outcomes, a layered security system is no longer an optional enhancement—it is an indispensable necessity in countering the drone threat.

The Kinds of Sensors You Need in Your Counter-Drone Security Stack

When figuring out which sensors to integrate into your security stack, it may be easy to experience "sensor overload". When considering the drone threat specifically, there are three

sensors that are most commonly used to effectively protect critical infrastructure.

Radar: The Backbone of Drone Detection

Radar serves as the foundational layer in a multi-sensor security system, providing critical data to validate and enhance the performance of other sensors. Unlike RF sensors, radar does not rely on the drone's communication system, making it a vital tool for detecting drones of various sizes, speeds, and classifications. Modern radar technology is highly precise, capable of identifying small, erratic aircraft like drones under all weather and lighting conditions, while effectively filtering out irrelevant objects such as birds.

Optical Sensors: A Visual Confirmation Layer

Cameras, particularly pan-tilt-zoom (PTZ) models, enable security teams to visually track drones and gather detailed observations, such as whether the drone is equipped with a camera or carrying a payload. This information helps determine the drone's potential intent and the appropriate response. However, optical sensors perform optimally when paired with radar, as they struggle to maintain target lock in adverse weather or poor lighting conditions.

Radio Frequency (RF) Sensors: Decoding the Signal Landscape

RF sensors rely on detecting and intercepting the communication signals between a drone and its controller. By analyzing these signals, RF sensors can often pinpoint the location of the drone and, in some cases, identify the operator's position. This comes in particularly handy when security teams need to pass off evidence to local law enforcement to apprehend a drone operator.

Any drone detection technology stack worth its salt will have some combination of these three sensors, with radar and optical sensors being the two baseline components. When these sensors work in unison, they create a system of checks and balances on one another, making sure that no drone can slip through the cracks.

The Playbook: What Critical Infrastructure Security Teams Can Do Once a Drone is Spotted

Now that the right sensors are in place, it's time to discuss what on-site security teams can do with the data collected when a drone shows up.

While the DOJ, DHS, DOE, and DOD are the only entities empowered to take direct mitigating actions—such as neutralizing or capturing drones—private security teams at critical infrastructure sites play a pivotal role in maintaining safety and protecting assets. The integration of advanced, multi-layered drone detection systems allows these teams to monitor the airspace, assess threats, and take localized actions that mitigate risk.

Drone detection technology is crucial for identifying the presence of UAVs, analyzing their behavior, and making informed decisions to protect critical infrastructure. With accurate data and visual confirmation of a drone's activity, security teams can decide whether to continue monitoring, alert law enforcement, or take measures to ensure the safety of personnel and infrastructure.

Key defensive measures for critical infrastructure teams include:

- Locating the Operator: Using RF tracking, radar signals, or a physical search in the area identified by detection systems, security teams can locate and report the drone operator. Once the operator is identified, security personnel can engage with them to determine intent and, if necessary, involve law enforcement for further action.
- Establishing Perimeters and Securing Assets: If a drone is suspected of carrying dangerous

materials or conducting surveillance, critical infrastructure teams can establish safety perimeters to minimize risk and ensure personnel and critical systems are protected.

- Coordinating with Federal Agencies: In situations where the drone poses a significant threat that exceeds the capabilities of on-site security, teams can share detection data with federal agencies, such as the Federal Aviation Administration, FBI, or DHS, as well as state or local law enforcement agencies. These agencies may have a wide range of options, including criminal, civil, or other response options.
- Implementing Proactive Site Security: By maintaining a multi-layered detection system that integrates radar, optical, and RF sensors, critical infrastructure teams can ensure comprehensive monitoring. This system provides a 360-degree view of the airspace, allowing teams to detect drones early and respond proactively.

The above protocol shows just how important these on-site teams play in the larger puzzle of thwarting a drone attack. Without that first-responder knowledge gleaned from a multi-layered system, the potential for a drone to wreak havoc unchecked cannot be underestimated.

A Case Study: Why the Emergence of "Dark Drones" Further Cements the Importance of Multi-Layered Systems

To put the utility of a multi-layered system to light, it's important to consider the emergence of "dark drones"—drones that evade detection by RF sensors. This has

introduced a troubling challenge for critical infrastructure security teams. These drones are modified to operate without emitting identifiable radio frequencies, allowing them to slip past systems that rely solely on RF detection.

And the barrier to creating such undetectable drones is alarmingly low; with basic research on platforms like YouTube or Reddit, nefarious operators can find step-by-step guides to disable their drone's RF signatures. That means that commercial drones, often available for a few hundred dollars at Best Buy or the like, can be transformed into silent intruders with minimal effort.

This vulnerability highlights a critical gap in counter-drone solutions that depend exclusively on RF sensors. While RF detection remains an essential tool for identifying most drones, relying solely on it creates a significant blind spot. "Dark drones" exploit this gap, enabling operators to breach security perimeters undetected. To address this challenge, a multi-layered approach incorporating radar technology is vital.

That is, radar serves as the "catch-all layer" when RF sensors fall short. Unlike RF systems, radar is independent of signal emissions, making it immune to the tricks that enable dark drones to fly undetected. However, not all radar systems are created equally, and selecting the right radar for critical infrastructure deployments is critical. Some radars are optimized for slow-moving ground threats, while others may rely on mechanical components that compromise reliability.

To effectively detect and track fast-moving drones, radar systems must meet several key criteria. The radar must excel in identifying and following drones in real-time, particularly in dynamic environments, and possessing the ability to simultaneously track multiple drones is essential, especially in scenarios involving coordinated attacks or swarms. It must also integrate smoothly with other components of the security system, including RF sensors, cameras, and video management systems (VMS), creating a cohesive and efficient layered defense.

The emergence of dark drones underscores the necessity of multi-layered security systems. By combining radar with RF detection, optical sensors, and advanced software, security teams can build a robust defense against increasingly sophisticated threats. Ensuring no single vulnerability can be exploited is the cornerstone of effective drone security.

It's All in the Integration: Why It's Important Your Sensors Work Hand-in-Hand

The true power of a layered security stack lies in its integration. When radar, optical, and RF sensors operate in concert, they provide a comprehensive picture of the airspace and a seamless workflow for critical infrastructure security teams. All this rich data being collected is funneled into the command-and-control center software in real-time, creating a visual representation of the security perimeter that's easy to understand and configured to the needs of the security team.

Here's a snapshot of some of the benefits you get when multiple layers of sensor data feed into the same system:

- Data Fusion for Enhanced Awareness: By combining data from multiple sensor types, security systems can create a unified view of potential threats. For example, radar might detect an approaching drone, optical sensors confirm its identity, and RF sensors analyze its potential communication signals. Together, these technologies enable a coordinated response.
- Automated Threat Classification: Integration with artificial intelligence (AI) and machine learning (ML) can automate the classification of threats, reducing the potential for human error you have when security personnel are tasked with assessing each and every incursion. By prioritizing high-risk targets, these systems ensure that human operators focus on the most pressing challenges.
- Interoperability with Various Levels of Law Enforcement: Integrated systems provide actionable intelligence that can be shared with law enforcement across the local, state, and federal levels, improving collaboration during incident response. As shared earlier, this is especially key, as only the FBI and other authorized federal enforcement bodies can take mitigative action—returning a drone to its operator, grounding a drone, etc. However, sharing this same information with local law enforcement is also key, as pinpointing a drone operator's location allows police to intervene swiftly and attempt to apprehend the operator.

Building Resilience Against Drones in and Around Critical Infrastructure

The dynamic threat environment surrounding critical infrastructure demands a proactive and adaptable approach to security. A layered security stack—anchored by radar, optical, and RF sensors—ensures that no single vulnerability can compromise the entire system. It also empowers security teams to alert proper law enforcement bodies as early as possible to engage in mitigation efforts outside their jurisdiction.

By detecting threats early, identifying them accurately, and responding effectively, this approach provides the situational awareness and reaction time that security teams need to protect their assets. Moreover, integrating these technologies fosters resilience, enabling critical infrastructure to withstand and recover from attacks.

As drones continue to evolve, so too must the tools and strategies used to counter them. Embracing a layered security stack is not just about keeping pace with threats; it's about staying one step ahead. In today's complex landscape, the sum of your security stack truly defines the strength of your defense.


BORDER PATROL

Harnessing AI to Secure America's Rural Critical Infrastructure

Cyberattacks on critical infrastructure are escalating in frequency and complexity, imperiling essential services for millions of Americans in rural communities. Artificial Intelligence (AI) technologies bring fresh opportunities for these organizations to shore up their cyber defenses.

Since the end of 2022, phishing attacks have jumped a staggering 1,265 percent, and ransomware attacks have climbed 76 percent, according to Accenture research. Cybercrime losses rose from $3 trillion in 2015 to $8 trillion in 2023 and are forecast to hit $10.5 trillion this year.

Rural and urban critical infrastructure alike, including water utilities, energy providers, telecommunications companies, and healthcare facilities face similar cybersecurity risks, largely driven by outdated, legacy technology and the accumulation technical debt. Over the past 15 years, these challenges have been well documented.

But unlike large urban utilities, which can allocate substantial budgets for cybersecurity operations, rural organizations often operate with limited resources and lingering staffing shortages. Many have no dedicated cybersecurity teams.

This tends to orient these enterprises toward being reactive rather than proactive, rendering them vulnerable to increasingly aggressive nation-state actors and individuals engaged in espionage, data theft, and network disruption.

Recognizing these challenges, the U.S. federal government has initiated a range of programs designed to bolster the cybersecurity of rural critical infrastructure organizations. Most of these programs provide grant funding and technical support to help shore up cyber defenses.

The Department of Energy's Rural and Municipal Utility Cybersecurity (RMUC) Program, launched in August 2022, authorizes $250 million over a 5-year period to assist electric cooperative, municipal, and small investor-owned utilities with detecting, responding to, and recovering from cybersecurity threats, as well as increasing their participation in threat information sharing programs.

Similarly, the Cyber and Infrastructure Security Agency (CISA) provides a myriad of security services such as assessments, vulnerability scanning, threat intelligence sharing, and training and exercises, just to name a few.

But AI should also play a role in identifying and prioritizing vulnerabilities within these systems. AI technologies can optimize many aspects of cybersecurity operations including enhanced phishing detection, threat intelligence collection, and predictive analytics, all the while reducing the workload of security teams.

Often, rural critical infrastructure operators still manually run their

response playbooks and triage processes. But by automating those processes, the same work can be performed in a fraction of the time. In the event of a detected breach, AI can execute predefined protocols autonomously, such as isolating the system or blocking the malicious traffic.

Integrating AI into cybersecurity operations isn't just a technology function. It requires a dedicated team including Information Technology (IT) and Operational Technology (OT) security professionals. Collaboration, training, and education are critical. Starting small is an effective strategy. Organize your stakeholders around a small pilot by selecting a specific area to test AI solutions. This approach will build confidence and experience, adopting the technology at pace that doesn't overwhelm existing systems and security professionals.

Scaling AI should naturally follow successful pilot implementations. As organizations realize the benefits of AI, they should consider reinvesting any savings or efficiencies gained back into their cybersecurity efforts. This reinvestment will help reinforce a more resilient cybersecurity environment, as well as a culture of innovation.

Accenture research shows 97 percent of executives say generative AI will transform their industry, and 67 percent plan to increase their spending in data and AI. Rural critical infrastructure owners and operators need to invest also. The technology represents a significant step-change toward protecting their operations and the communities they serve.

With a thoughtful approach to assessment, stakeholder engagement, small pilots, and scaling, these organizations can harness AI's power and bolster their resilience. Embracing this approach will help to ensure safer delivery of essential services in rural zip codes and a more secure future from coast to coast. The time to act in now.

Rick Driggers is Accenture Federal Services' Cyber Portfolio Lead and the former Assistant Director for Integrated Operations at the Cybersecurity and Infrastructure Security Agency (CISA).

Ensuring Compliance with the EU CER Directive: Protecting Critical Fiber Optic Infrastructure

The European Union's cybersecurity directive (NIS2) became legally binding across all EU member states on October 17, 2024. On the same day, member states were also required to outline measures for implementing the Critical Entities Resilience (CER) Directive, which takes effect in January 2025. Operators of critical fiber optic networks must adapt to ensure compliance.

This article explores how thorough risk analysis, proactive risk-reduction strategies, and continuous effectiveness checks are pivotal to meeting these directives.

Key technologies like fiber integrity monitoring and physical threat detection will be examined, alongside real-world applications in wind farms and pipelines. The article will also outline how these solutions can extend to sectors such as perimeter security, offering actionable insights for operators to strengthen their infrastructure resilience.

Directives Demand Change

The CER Directive has been adopted by the European Union (EU) to enhance the resilience of critical infrastructure and entities that provide essential services. The directive was adopted in December 2022, requiring member states to enact national legislation before coming into effect in October 2024. The previous Critical Infrastructure Directive (2008) is now superseded as the new CER Directive reflects the evolving security landscape characterized by increased cyber threats, climate change impacts, and geopolitical tensions.

To fully address the resilience of those entities that are critical for the proper functioning of the internal market, the directive creates an overarching framework that addresses the resilience of critical entities in respect of all hazards, whether natural or man-made, accidental or intentional.

The directive applies to essential services broadly grouped into 10 key sectors, including energy, transport, banking, health, water supply, and digital infrastructure –ensuring these entities can withstand and recover from a wide range of disruptions. Its scope includes both physical and digital risks, emphasizing a holistic approach to resilience.

Key to the CER Directive is the requirement for member states to identify "critical entities" based on their significance to the functioning of society and the economy. These entities must conduct risk assessments, implement security measures, and report significant incidents to the relevant authorities.

The directive aligns closely with the EU's Network and Information Security Directive (NIS2), ensuring an integrated approach to both physical and cybersecurity.

NIS2 is the EU-wide legislation on cybersecurity that provides legal requirements to enhance the overall level of cybersecurity within the EU. Coming into force in 2023 (member states had until October 2024 to transpose the directive into law), NIS2 replaces the earlier 2016 rules to reflect increased digitization and evolving cybersecurity threats.

Figure: Optical network monitoring system enable operators to detect and localize fiber damage and assess overall fiber health to monitor degradation from harsh environmental conditions.

By expanding the scope of the cybersecurity rules to new sectors and entities, NIS2 further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

Among its provisions, NIS2 mandates that member states have a Computer Security Incident Response Team (CSIRT) and a competent national network and information systems (NIS) authority. Similar to the CER directive, NIS2 promotes a culture of security across information-centric sectors that are vital for economies and society in general such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure.

Fiber Optics are Critical to Infrastructure

Clearly, with the nature and amount of data they carry, fiber optic networks must be considered to be critical infrastructure for the purposes of both directives. This means that operators of these networks must embrace new measures and implement comprehensive risk management processes.

Primarily, this involves conducting thorough risk assessments, planning and executing risk-reducing measures, and regularly confirming their effectiveness. Wherever measures are found to be inadequate, additional steps must be taken to minimize any impact upon the economy or society.

Fiber Integrity: The physical integrity of the fiber is of prime importance, along with controlling access to the cable itself. Operators must be able to detect and localize fiber damage and / or breaks, and other incidents that could negatively impact operation. Many operators use an optical network monitoring system on their dark and lit fiber optic links. As well as assessing damage, the ONMSi system can also assess overall fiber health and monitor for degradation over time.

Maintaining fiber integrity also requires operators to restrict access to cables and identify any breaches. For this, passive, maintenance-free sensors are often used to monitor access points, manholes and distribution boxes to alert operators about any access – legitimate or unplanned / unauthorized. This approach to access monitoring can be implemented with the same fiber monitoring system and many consider this to be essential to meet the requirements of the directives.

Threat Detection: Ideally, potential breaches of any critical infrastructure will be detected before the cable is reached. Another area is of interest is physical threat detection for critical infrastructure. This entails real-time detection, notification, and location of threats, third party interference, perimeter intrusions, and anomalies anywhere along the infrastructure.

Fiber optic sensing technologies such as Distributed Acoustic Sensing (DAS) are valuable due to their ability to differentiate between various types of disturbances, such as mechanical or manual digging near cables. Additionally, DAS can be used for virtual fencing or to provide proximity alerts that will detect people or vehicles approaching infrastructure.

DAS technology is essential in ensuring regulatory compliance and operational security, mitigating the risk of accidental damage or deliberate third-party interference by identifying and pinpointing threats.

Besides the physical security, operators must be mindful of data integrity and network availability as well. While fiber optics cannot be 'eavesdropped' in the same way that copper cables can, there are still risks to data being disrupted or networks rendered unavailable. For any data network, accurate timing of clock signals and synchronization throughout the network are critical to ensure basic functioning and operation. Any disruption to the Precision Timing Protocol (PTP), or the timing (clock) information it distributes, can lead to data loss, disrupting a network and rendering it unavailable.

Techniques such as high-precision timing analysis and synchronization verification can prevent this loss of data and disruption of the network itself, thus minimizing failure risks and ensuring the reliability of critical communication systems. This verification is crucial for maintaining the integrity of modern communication networks, including 5G.

Critical Infrastructure in Real-Life Scenarios

Renewable energy installations, such as wind farms, are providing an ever-increasing level of electrical power. This will only increase in the future, making these facilities a crucial component of energy infrastructure. Ensuring the reliability and efficient operation of these installations is paramount, and fiber sensing technology is instrumental in day-to-day operation.

Using the unique properties of optical fibers, operators can detect changes in temperature, strain, and acoustic vibration (sound) along the length of a fiber. With these fibers already integrated into the infrastructure of wind farms

the structural health and operating conditions can be continuously monitored remotely.

By requirement, turbines are located where wind is consistent – either remote onshore locations or, increasingly, offshore where they have to endure waves, tidal forces, tectonic activity, and corrosive saltwater. In either scenario they are connected to the main national power grid through array cables and export cables which are critical for getting energy to where it is needed. Techniques such as Distributed Strain Sensing (DSS) and Distributed Acoustic Temperature Sensing (DTS), or a combined temperature and strain measurement (DTSS,) monitor changes in strain and temperature to provide valuable data on the structural integrity of these cables, often allowing a repair or remedial action to be effected before a

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

complete failure occurs.

By utilising fiber already embedded into or bonded onto those cables, DSS, DTS or DTSS can be used to monitor cable integrity, detecting issues such as depth of burial changes for underground cables, stress and strain due to movement or icing, mechanical damage, or thermal anomalies. Understanding cable temperature is also critical to optimise cable power transfer, too much power and you risk overheating and potentially melting cables, so operators use DTS to calculate the Real Time Thermal Rating (RTTR) of cables which enables them to maximise/optimise power transfer while preserving the operational life of the cables.

Offshore turbine power cables are also subject to some unique risks such as damage from ship's anchors or fishing trawlers. Distributed Acoustic Sensing (DAS) can detect threats in the environment around infrastructure, like disturbances caused by fishing gear or ship anchors, providing proximity warnings and identifying potential risks. As this is done in real-time, operators can take immediate action to mitigate the impact, such as intercepting or rerouting vessels or triggering an investigation to identify which vessel was in the areas so that any damage claims can be made against the operator, cable repairs at sea can be a costly thing.

With the continuous data available on the condition of the turbines, cables and other aspects of the power infrastructure, operators can see change as soon as it happens and track any degradations over time. This allows operators to predict when and where maintenance is needed, preventing unexpected failures, reducing downtime and saving the significant costs associated with total failure.

Pipelines are equally critical in transporting energy in the form of a liquid or gas. Given the volatile nature of these substances, ensuring the safety and integrity of pipelines is paramount. Here also, fiber sensing technology offers unparalleled capabilities for real-time monitoring and early detection of potential issues. Recognizing the benefits of this technology, it has become mandatory to include fiber sensing for new pipelines and in some cases retrofitting the technology to existing infrastructure.

By embedding fiber optic cables nearby or attaching them to pipelines, operators can continuously monitor the structural health and operational conditions of these critical assets. A huge advantage of fiber sensing technology is the ability to detect leaks at an early stage using either DAS or DTS depending on what the pipeline is transporting. In some cases, a mix of both is used.

Unlike traditional inspections that require personnel and equipment to be transported to remote and often inhospitable regions, fiber sensing can be performed remotely. Additionally, fiber sensing is less likely to miss a small leak in the way that an engineer could.

Similar to power cables, fiber sensing can monitor any changes to the structural integrity of pipelines due to environmental factors, operational pressures, and aging infrastructure. It can also use DAS to detect unauthorized activities such as digging or tampering, thereby preventing sabotage and theft.

Regular monitoring and maintenance based on fiber sensing data can significantly extend the lifespan of pipelines. By identifying and addressing potential issues early, operators can prevent the deterioration of pipeline materials and ensure their long-term integrity. This proactive approach not only enhances safety but also maximizes the return on investment for pipeline infrastructure.

Conclusion

Fiber sensing technology is continually evolving, with constant innovation enhancing capabilities and increasing sensitivity. Most recently, technologies such as DAS have enabled even greater sensitivity and accuracy in detecting changes along pipelines and cables. Now, operators can differentiate between various types of disturbances, such as vehicle movements, manual versus mechanical digging, and leaks, offering a very comprehensive monitoring solution.

Fiber sensing technology is transforming the way we monitor and maintain remotely located energy infrastructure. Its ability to provide real-time, continuous data on the condition of assets offers significant advantages in terms of safety, efficiency, and cost-effectiveness.

As fiber sensing continues to advance, operators can expect even greater improvements in energy infrastructure monitoring and management thereby ensuring the integrity and longevity of critical infrastructure, safeguarding both the environment and their investments.

Douglas Clague, Solutions Marketing Manager - Fiber Optic Field Test – VIAVI Solutions.

An Interview with 3B Protection

3B Protection designs and manufactures innovative blast, ballistic, and forced entry-resistant walls, offering unmatched safety for government, military, homes, schools, and critical infrastructure. Combining strength, affordability, and peace of mind, 3B Protection is redefining modern security solutions. Ben Lane, CIPRNA event manager, met Dominic Dillon, President & CEO of 3B Protection.

Ben Lane (BL): Hello Dominic, it is good to have you here today. You will be joining us in Houston, March 11-13 for CIPRNA 2025 as our Platinum sponsor. We look forward to seeing you there and hearing what you have to say during the Conference.

Dominic Dillon (DD): Good morning, Ben, and we are looking forward to the event.

BL: Tell us about 3B Protection, and the journey you have had so far?

Dominic Dillon, President & CEO, 3B Protection

DD: 3B Protection was born in the UK where I owned a concrete company, delivering concrete to people's houses for foundations and extensions. The basic kind of applications for traditional concrete. One day, a company asked us to research a new material that needed "give" in it, and that had a slightly lower PSI than traditional concrete. They wanted us to produce this material by using recycled materials.

We embarked on a research and development program whilst running the existing business. It took two years to produce a material that had the properties we were looking for. We conducted various structural and compression tests on the material and initially it was designed for areas that experienced earthquakes and seismic events.

Later, someone asked us about the blast and ballistic capability of the material and as we were working in the UK where there were very few test facilities, we contacted NATO and went through their test program for new materials. At that time, 3B was just a block. It was not in the panel format that we have today.

We passed the NATO testing program, and we had our product accredited up to UL level ten, which is enough to stop a 50-caliber round. After we became a NATO vendor we embarked on manufacturing in Dubai, Pakistan, and Turkey.

BL: What a great story and what a great history. And getting NATO approval is not easy! What are your clients concerned about? What are their biggest challenges in terms of threats and attacks on infrastructure?

DD: I came to the USA in 2017 and one of the main issues in terms of threats were ballistic attacks on critical infrastructure such as a water plant, a gas plant, or a utility plant. And these attacks could occur any time of day – it could be a malicious attack where someone is attempting to take out the substation or the utility. Or it could be an accident where someone is shooting out in the forest and a bullet goes astray and hits the substation. One of the main problems for our clients is the uncertainty of what level of

protection to specify. So, we focus them on UL level eight, nine and ten, with ten being the highest level.

We find engineers can struggle to specify the right product for their plans because they do not know what level to go to – they do not have a clear idea of what will happen when they come under attack. This also creates a budget problem when designing a facility because there is a difference in cost between UL level eight and UL level ten. It is a significant cost difference and so the end user needs to be clear on what protection level they require.

Also, the companies we deal with can have a perimeter measuring anywhere from half a mile up to five miles long and when you specify substantial protection around a long perimeter, it becomes extremely expensive. So, one of the areas we focus on is offering single-asset protection inside the critical area and covering off, through line of site, particular parts of the substation.

We find it hard to comprehend there is no written standard in the USA telling the client, "Okay, you must do this to this protection level." This is one of the biggest areas that we find our clients struggling with.

BL: This brings us to the question of how you support your clients, and how do you respond to their needs?

DD: We offer ballistic panels, and ballistic gates and doors. We can protect an entire perimeter, or an entire building, we can really do anything with our products. One of the things we focus on with our clients is asking the question, where are the issues? Is it because you are surrounded by hills? Are you worried about someone on a nearby hill shooting into the substation and attacking certain parts of the substation?

We conduct threat assessments on the substation to assess where the line of sight is and the type of walls we could use around the asset to protect it.

We focus on having a one wall solution that protects against ballistic blast fire and high-speed fragmentation in areas that could be subject to fire. We can construct a single wall that covers off four to five different threats, so the client can order a complete solution in one single wall. We also produce an

anti-theft matting system that can be used over areas where criminals may attempt to steal copper.

BL: How does your organization exceed present standards in this area?

DD: When I first came to the USA, we evaluated our products against USA standards, ASTM standards, ballistic blast, and fire. The standards in the USA for ballistic protection were low. For example, with UL level eight, you only need to stop five bullets in your product to become a UL vendor. If you go up to UL level nine and UL level ten, then you only need to stop one bullet for your product to be UL certified.

One of the pushbacks we had when we first went to the market were questions about why a potential client would buy a product that is only going to stop one round. A good question! We went back to the drawing board, and we redesigned the integrity of our material, and we retested it to the point that now we have single panels that will stop anywhere from two to three thousand rounds of ammunition.

So now we have a product that is a real-life situation product and if someone is going to attempt to damage your assets, you can now specify a panel that will stand up to a significant attack. On the back of this we created a standard and secured a trademark. It is the RLS standard. Now many of our clients specify this standard.

And that is really what we focus on. We have our own standard, and we focus very strongly on saving an asset or the lives of those within the asset.

BL: Thanks very much for that. A great story! We look forward to seeing you in Houston, March 11th-13th.

DD: Thank you, see you there.

The evolution of underwater threats

In our globalised world, economic prosperity and growth have always been critically dependent on the use of our oceans. With 96 per cent of goods shipped by sea, it's always been vital that this transport option remains open. Therefore, the security of our seas, ports, harbours and offshore facilities, for both companies and governments, remains a high priority.

Criminals and terrorists have always been aware of the difficulty of keeping such large swathes of water safe from their activities and have used it to their advantage. Only a few years ago, the use of a diver to carry out attacks was the main underwater tactic. Deterring and defeating these criminal enterprises is a constant battle but the intelligent use of technology has been one of the key ways to achieve this.

But, for port authorities, governments and security forces, underwater threats are changing in both their purpose and methodology. Our geopolitical climate has become more volatile with intelligence pointing towards more attacks on global critical national infrastructure (CNI).

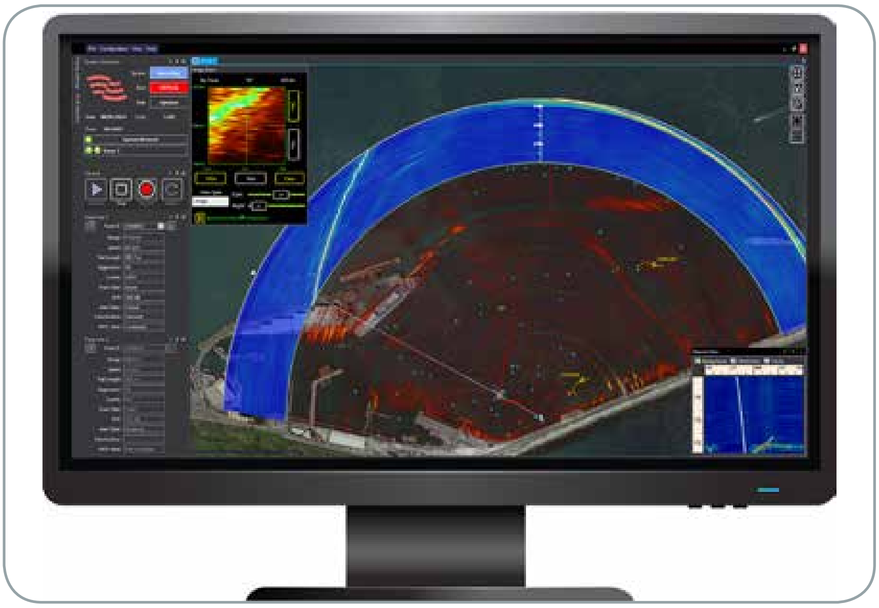
Are we heading towards a new kind of threat?

Threats to CNI installations, maritime assets, political events and navies are constantly evolving, from traditional threats, such as divers, to the new and increasingly sophisticated uncrewed technologies that are sometimes harder to detect.

When thinking of drone threats, traditionally you will think of the aerial domain. Countermeasures have been developed to keep pace with a vast range of drone platforms, from small, homemade devices to large, sophisticated UAV platforms. These threats have evolved quickly with detection and countermeasure systems responding at pace to protect people and assets.

Now, we are seeing an increasing threat posed by uncrewed underwater platforms which presents new challenges for the systems that protect us. Detecting threats on the surface through above water surveillance can be controlled through several means, including CCTV, FLIR radar, and access control measures. However, the subsea domain presents potential foes with a covert environment where visibility, terrain, noise, and naturally occurring fauna, animals, and debris make threat detection and classification a seemingly insurmountable challenge, leaving vessels and crews extremely vulnerable to interference and attacks.

The underwater space is no longer solely the domain of large, manned platforms, and new threats are quickly emerging from autonomous, agile UUVs. Should the development of these platforms reflect even half the pace at which aerial drones evolved, it becomes critical that we are equipped with solutions to



detect, classify and track these threats.

The nature of subsea threats

The development of uncrewed subsea vehicles has moved on significantly. The fact is that these threats will continue to evolve means detection and countermeasure technologies have to keep up.

For detection and navigation, the key difference between surface and subsea drones is GNSS, as the satellite-based navigation system does not work underwater making accurate positioning an issue. Visually you cannot see very far, making it harder to use cameras to find threats and in the case of combat divers for example, the threat is incredibly small and extremely quiet, whereas a UUV is also fast-moving.

Traditional subsea detection technologies, deployed extensively for subsea intruder and diver detection, rely on acoustics and sonar, however, this becomes incredibly challenging in areas such as ports and harbours. These areas are some of the noisiest environments, where multiple, often large, and therefore 'noisy' vessels operate, and depth sounders may be continually active. In addition, the relatively still water creates a complex thermal structure and one where you're unlikely to be able to rely on a low reverberation seabed. In congested and challenging port and harbour areas, the sound velocity profile will constantly change.

It's not just detection that presents a challenge. Once detected, a target must be classified and distinguished from marine fauna. Identifying whether a potential threat is a harbour seal, a terrorist diver, combat diver, SDV or UUV is a determination that must be made correctly otherwise the consequences could be dire.

Knowledge is power. You can't react if you don't know it's there

New solutions need in-depth technical knowledge to identify, classify, and track a range of new threats. The better the understanding of the threat

Hanwha Vision

Powering the next generation.

Protecting the critical infrastructure that powers our lives requires 24/7 surveillance. Hanwha Vision delivers everything municipalities need: low-light performance, custom explosion-proof camera housings, temperature change detection analytics and more.

landscape in the unseen subsea environment, the more protection that can be offered.

Wavefront looked to address challenges by bringing a portable, lightweight detection system to market that could detect threats in shallow waters and over a wide range. As a result, Wavefront developed Sentinel IDS® which emits a 360° pulse and using 256 receive beams equally spaced along a perimeter to detect targets at up to 1500m range. The system is capable of being deployed stand-alone or as part of a sonar network to protect a wide-area perimeter.

Simultaneous Active and Passive Sonar capability (SInAPS®)

It now includes passive detection. SInAPS® is Wavefront's highly innovative approach combining the very best that both tracking methods have to offer by using the same acoustic array for both active and passive processing, simultaneously within the same operating band. This allows the tracking of discrete and obscured targets that stand-alone active sonars would historically not be able to identify. Thus, leaving the threat nowhere to hide.

Simon Goldsworthy - Global Business Development Manager – Intruder Detection Systems

EU's first ever report on the state of cybersecurity in the Union

The report provides an evidence-based overview of the cybersecurity maturity state of play as well as an assessment of cybersecurity capabilities across Europe. The report also includes policy recommendations to address identified shortcomings and increase the level of cybersecurity in the EU.

The analysis conducted is based on various sources, including but not limited to the EU Cybersecurity Index, the NIS Investment reports series, the Foresight 2030 and the ENISA Threat Landscape report. This report is the result of extensive consultation with all 27 EU Member States and the European Commission.

The risk assessment conducted on a Union level revealed substantial cyber threat level to the EU, highlighting discovered vulnerabilities exploited by threat actors targeting EU entities.

With regards to the cybersecurity capabilities at the EU level, EU Member States have developed cybersecurity strategies that present an overall alignment in objectives. Critical sectors appear more heterogenous in terms of size and criticality which complicates supervision and uniform implementation of cybersecurity measures. On the citizens level, it is suggested that cybersecurity awareness has likely increased among EU citizens. Digital skills level of younger generations appears higher, despite variations in the availability of education programmes and education maturity among Member States.

Several key themes are expected to require greater policy attention as we progress. Latest cybersecurity policy developments in the EU have established a strong foundation that allows for capability, nonetheless, authorities both at EU and national level face challenges in adapting to their new roles while navigating into the evolving threat landscape. In particular, Artificial Intelligence (AI) and Post-Quantum Cryptography will be attracting greater attention in the years ahead, while the EU has to step up competitiveness in the field through research, development and innovation. To prepare for the challenges of tomorrow, common situational awareness and well-tested operational cooperation are fundamental.

An Interview with SimSpace

SimSpace empowers organizations to confidently manage risk by simulating, testing, and optimizing their teams, tools, and processes in a high-fidelity cyber range. With automated scenario exploration, it enhances readiness, validates security controls, and strengthens cyber resilience against evolving threats.

Ben Lane, CIPRNA event manager, met Graham Westbrook, VP Cybersecurity Sales Engineering at SimSpace.

Ben Lane (BL): Hi Graham, good to see you today. We will be seeing you and your team, SimSpace, in Houston at the conference, Critical Infrastructure Protection & Resilience North America, March 11-13, where you will be speaking in the session: https://ciprna-expo.com/session/cybersecurity-regulations-best-practice-and-minimum-standards/

Tell us about your career and how you got here.

Graham Westbrook, VP Cybersecurity Sales Engineering at SimSpace

Graham Westbrook (GW): Thank you. We are looking forward to the conference in Houston. I am a former cybersecurity practitioner, turned product specialist, and in my current role at SimSpace, I get the opportunity to connect in with OT infrastructure and learn how to simulate the future. An important part of that is being able to simulate future cybersecurity attacks, so that we can train tools and technology.

My background spans from supporting the U.S. Department of Defense, looking at web vulnerability scanning and auditing, all the way through to cybersecurity for healthcare. I have also worked in commercial organizations, specifically in threat intelligence.

I am studying artificial intelligence at the University of Oxford, UK. So that background gives me a particular world view, which helps me support our customers in a way where I can see the threats that are coming, and how we can prepare for the next threat, and not the last one.

BL: On the topic of threats, what are the key emerging cyber threats that you and your customers are seeing now?

GW: In relation to operational technology, we are seeing different ways of hopping into OT subnets. If you take the human machine interfaces, and the programmable logical controllers, there are ways in which the attacks or attackers can pivot into those subnets if improperly protected and manipulate the Modbus traffic and the protocols to turn things on and off to create badness on the OT end.

The reason that is important is that those things can be connected to people where bits and bytes meet flesh and blood. Those things can be connected to water treatment plants, or DOD military facilities with top-secret clearances. This means there are implications for exploitation.

Other cyber threats we are seeing are post-quantum cryptography testing, and quantum-resistant

cryptography testing. If you look at things like Bitcoin, people are wondering, "Will quantum computing harm me? Will quantum computing start to unravel the cryptographic hashes and methods that we have had for the last 10, 20 years, and put us at risk?" So post-quantum cryptography is trying to better understand how we can validate this kind of future cryptographic method and protect and prevent ourselves from harm.

People are doing work in SimSpace on cyber ranges, which are infrastructures in which you can assess potential future cyber-attacks and implications. We are also seeing various artificial intelligence, or adversarial intelligence elements come out, and we can use a range to validate those protections against those AI components. We use things like Zero Trust to utilize detection engineering to potentially find bad, faster.

This is where SimSpace's cyber range technology plays a critical role—by enabling organizations to safely test and refine their defenses against OT-specific threats in a controlled, risk-free environment. Through realistic threat emulation, organizations can validate their security controls and ensure their response strategies are effective against modern adversaries.

BL: What is advanced simulation technology, and how has it been a transformative solution for addressing the challenges you have mentioned in OT?

GW: Well, I think about certain metaphors in life. Would you go play in the Super Bowl if you had not practiced first? Would you drive in an F1 race if you had not simulated the pit with your group? The same goes for the cybersecurity realm. We must simulate the future to learn and prepare for it better. Simulation technology and advanced simulation technology are about emulating three layers.

Advanced simulation technology is more than just running attack scenarios—it's about creating a highly realistic, enterprise-scale environment where organizations can validate their entire cybersecurity strategy. Our cyber

range technology replicates three critical layers:

(1) The infrastructure layer—spanning IT, OT, cloud, and hybrid environments, integrating real-world devices.

(2) The tools layer—mirroring an organization's existing security stack to assess tool efficacy.

(3) The activity layer—generating realistic network traffic, user behavior, and sophisticated attack emulation to test security responses in real-time. Think of attacks and attack emulation to mimic real world APTs and cyber criminals. Once you dial that in, you end up getting this ecosystem in which you can evaluate your people's process and technology.

Unlike static Breach and Attack Simulation (BAS) tools, which run predefined attack scripts, SimSpace provides a fully dynamic, customizable environment where organizations can continuously test, adapt, and improve their defenses against evolving threats.

What we are trying to do is get as close to reality as possible, so that we can simulate the future. The last metaphor is a pilot simulation. So again, with no risk, if I can create a highly realistic pilot flight simulator, those people are able to train like they fight. They can train in a way where when they get in that cockpit and are willing to take on real world risk, they are already ready for the fight.

BL: How can you effectively train cyber defenders in simulation technology when it is only simulating scenarios?

GW: When we talk about making sure that simulation is effective, what we are trying to consider is how realistic we can be. Because the closer we can get to reality, the more likely we are able to train for the future. So, when you say scenarios, I think, "Okay, well that's anything in the realm of what we can come up with." And so maybe we are limited by our ability to perceive the future, but in-between randomness and knowing everything, we try to get as close to omniscience as possible. We try to understand what the likeliest scenarios are, the most dangerous courses of action, and then we can simulate those within a range.

The way we would train those individuals is to be able to interpret new and emerging cyber threats. Then turn those into attack emulations and deploy those attacks within an environment that looks like them, that helps them train for the most realistic future scenarios.

BL: How do you see AI affecting the way cyber-attacks are conducted? And can simulation technology keep up with this tool?

GW: Great question. I think AI in the hands of both good guys and bad guys is a fascinating problem to solve. The way we can keep pace or outpace the adversaries is to forecast future badness. When you look at Google's recent GenCast technology, they have been able to predict future weather patterns at almost 100% accuracy up to 15 days.

We used to rely on a single forecast for tomorrow, or the next week or the next month. Now, what organizations like Google and new weather forecasting agencies are doing is fifty forecasts for the next day. From those fifty forecasts, they are interpreting them for most scenarios, or how things could change, pivot, or persevere. I say all that because what we can do is create simulation labs and simulate different iterations of the future. And we can dupe this probabilistic ensemble analysis as they call it, where they combine all these different predictions of the future, and start to produce probabilities for what is most likely. Or what we should prepare for, and what we are not thinking about yet.

We use our cyber range platform

to proactively test AI-driven attack techniques, helping organizations refine their defense strategies before these threats materialize. By leveraging AI-powered detection and behavioral analytics in our simulations, security teams can stress-test their response capabilities against AI-generated malware, deepfake phishing attempts, and automated attack sequences. Our goal is to ensure that organizations aren't just reacting to AI-driven threats but are actively preparing for the next wave of adversarial AI tactics.

I would say that the best way for us to really consider what is coming is to forecast those futures and start to treat it like different probabilities of what we can expect.

My background is in threat intelligence analysis, and we use what are called words of estimative probability; things like highly likely or our chances are about even. We would take something like that and say, "Okay, it looks like this week, it's highly likely that we're going to experience some kind of new ransomware attack, just based on a new technology that dropped. Or a new kind of AI algorithm that is identifying areas of weakness, or vulnerability in an organization." In short, we need to forecast multiple futures to better understand the present.

BL: I am going to throw one last one in for you, just as a personal question really: What keeps you awake at night?

GW: I think about not being able to detect when malicious actors are at the door, or even inside of our organizations. There is a philosophy in the cybersecurity realm called assume breach. And it is considering that the bad guys are already in the house. I think about how AI giving malicious threat actors an advantage might disable us from being able to understand what is inside the house. I think algorithms like Isolation Forest that help detect anomalies are things that can help us from an AI perspective.

I guess something else that keeps me up at night related to AI, and the threats of the future, is just that it is removing from us the duty that we must create friendships and lean into connecting with other people. And sometimes it seems like there is an inverse correlation with the rise of technology, and the decline of mental health. I think that we cannot shirk the responsibility of striving to create opportunities for fellowship, and walk alongside other people, and get to know them, rather than outsourcing our brains to technology, and hoping that AI protects us.

BL: And that is a fabulous answer and something we should pick up at another point, because there is some interesting stuff in that last point you mentioned. But thank you, Graham, and of course we look forward to seeing you in March.

GW: Thanks, and see you soon.

Cyber Threat Alliance Publishes 2025 Cybersecurity in the Age of Generative AI

The Cyber Threat Alliance (CTA) today announced the publication of its Cybersecurity in the Age of Generative AI Joint Analytic Report (JAR). This report is broken into two parts. Part I, Combating GenAI Assisted Cyber Threats, addresses the use of GenAI tools for malicious purposes. Part II, Navigating Cyber Threats to GenAI Systems, examines cyber threats to these tools.

The rise of GenAI represents both opportunities and challenges in cybersecurity, empowering the community to leverage AI for innovation, efficiency, and enhanced defenses, while also enabling malicious actors to exploit the technology for a new dimension of AI-assisted threats. While GenAI lowers barriers to entry for adversaries and makes them more efficient, the foundational principles of cybersecurity remain integral to combating these threats effectively.

This JAR leverages the collective expertise of the CTA community to demystify the GenAI landscape, moving beyond the hype and providing evidence-based use cases. Through extensive collaboration, CTA members are actively addressing this critical topic across many collaborative efforts.

This report underscores that proactive measures, coupled with established best practices, are essential to mitigate the risks posed by AI-driven threats. Organizations must align their policies and practices to address the unique vulnerabilities associated with GenAI and can adopt a holistic approach that integrates technology, policy, and education.

"Many new technologies experience a hype cycle, but the one for Generative AI seems to have scaled new heights," says Michael Daniel, President and CEO of the Cyber Threat Alliance. "These predictions have included what GenAI could enable malicious cyber actors to do, most of which could be called 'breathlessly apocalyptic.' Of course, the reality is somewhat more pedestrian and, not surprisingly, GenAI's impact on cybersecurity has not matched the hype. That said, malicious actors are adopting GenAI tools in ways that are affecting the cybersecurity landscape. As a result, we thought it important to combine the insights from across our diverse members and partners to look at how our adversaries are actually using these tools in the wild and to provide recommended mitigations given this usage. The flatter than projected adoption curve gives defenders more time to prepare, but we can't afford to squander it."

Key takeaways include:

- GenAI is lowering barriers to entry, facilitating a greater volume of threats as malicious actors apply GenAI through various mediums as text, image, audio, & video, however GenAI has yet to bring more sophistication to threat activity, at this time
- Common myths debunked: AI isn't making adversaries "smarter," but more efficient
- Actionable guidance for organizations to integrate AI-specific defenses into their cybersecurity strategies

GenAI is reshaping the threat landscape, but we still have time to prepare. This report and supplement equip organizations with the knowledge they need to proactively address evolving challenges.

Part II of the JAR addresses the emerging problem of securing AI systems against malicious activity. Many actors want to target these systems, but the best practices for addressing these threats are still developing. This section highlights some of the key threats to AI systems and outlines steps that organizations can take to mitigate them. As the reports makes clear, the cybersecurity industry still has a long way to go in understanding cyber threats to AI systems and urgently needs to develop better technologies, processes, and procedures to protect these valuable assets.

Guidance for Secure OT Product Selection

The National Security Agency (NSA) joins the Cybersecurity and Infrastructure Security Agency (CISA) and other organizations to publish guidance helping operational technology (OT) owners and operators integrate security when selecting OT products.

The joint Cybersecurity Information Sheet (CSI), "Secure by Demand: Priority Considerations for Operational Technology Owners and Operators in the Selection of Digital Products," highlights key security elements to consider when purchasing industrial automation and control systems and other OT products, as well as specific questions to ask manufacturers. Many OT products are not designed or developed securely, and they commonly have weaknesses that make them a target for cyber threat actors, including the following: weak authentication, shared software vulnerabilities, limited logging, default settings, default credentials, and default protocols.

"The guidance not only helps owners and operators of critical systems secure their OT procurement lifecycles, it also sends a message to manufacturers to establish a more resilient and flexible cybersecurity foundation in their products," said Dave Luber, NSA's Cybersecurity Director.

The CSI urges OT owners and operators to select products with the following key security elements:

- configuration management,
- logging in the baseline product,
- open standards, ownership,
- protection of data,
- secure by default,
- secure communications,
- secure controls,
- strong authentication,
- threat modeling,
- vulnerability handling, and
- upgrade tooling.

The other agencies co-sealing the CSI are the Federal Bureau of Investigation (FBI), the U.S. Department of Energy, the U.S. Environmental Protection Agency (EPA), the U.S. Transportation Security Administration, the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), Canadian Centre for Cyber Security (CCCS), European Commission, Germany's Federal Office for Information Security (BSI), Netherland's National Cyber Security Centre (NCSC-NL), New Zealand's National Cyber Security Centre (NCSC-NZ), and the United Kingdom's National Cyber Security Centre (NCSC-UK).

ENISA welcomes the EU Action Plan for the cybersecurity of hospitals and healthcare providers

ENISA welcomes the initiative and remains committed to collaborating with the European Commission, the Member States, healthcare providers and the cybersecurity community to strengthen the sector's digital infrastructure and ensure its resilience to cyber threats. This plan is a key priority, in line with the commitment set out by President Von der Leyen's political guidelines for the new Commission's mandate for 2024-2029. Several specific actions are foreseen to be implemented progressively in 2025-2026, in collaboration with the Member States, healthcare providers, and the cybersecurity community.

Particularly, it is proposed for ENISA to establish a pan-European Cybersecurity Support Centre for hospitals and healthcare providers, designed to provide them with tailored guidance, tools, services and training.

Among others, the proposed tasks include the development of guidance for cybersecurity good practices and procurement, the development of a regulatory mapping tool, the establishment of EU capabilities for detecting cyber threats against the health sector, to introduce an early warning service for the sector, the development of cyber incident response playbooks.

Building on the existing legislative framework for cybersecurity (NIS2, Cybersecurity Act, Cyber Resilience Act, Cyber Solidarity Act), the actions proposed correspond to the current ENISA mandate to help the EU Member States increase the resilience of their critical sectors, while acknowledging that Member States represent different needs. To achieve the goals set out by the Action Plan, a joint effort is needed and adequate resources are required to fulfil the new actions.

New proposals to counter ransomware

The Home Office will today announce a public consultation seeking views on three proposals aimed at striking a significant blow to the ransomware criminal business model.

Ransomware is the most acute cyber threat for most businesses in the UK, and the impact of an attack can affect every aspect of an organisation. This includes disrupting operational delivery, hitting finances, compromising customer data, eroding trust and damaging an organisation's reputation.

The ransomware threat is borderless, and with criminals constantly adapting their techniques to gain efficiencies and maximise profits, it is an issue that senior leaders in all organisations should take seriously by allocating resources to robust cyber security measures and comprehensive incident response planning.

The NCSC, alongside wider government, is committed to making the UK an unattractive target for ransomware attacks, and the launch of this consultation represents a significant milestone on that journey.

The consultation will consider three proposals:

- A targeted ban on ransomware payments for all public sector bodies and critical national infrastructure – expanding the existing ban on ransomware payments by government departments and making the essential services the country relies on the most unattractive targets for ransomware crime.

- A ransomware payment prevention regime – increasing the National Crime Agency's awareness of live attacks and criminal ransom demands, providing victims with advice and guidance before they decide how to respond, and enabling payments to known criminal groups and sanctioned entities to be blocked. This regime would support disruptive operations such as the recent success of Operation CRONOS, the NCA-led global collaboration to disrupt Lockbit in 2024, one of the most dangerous cyber crime networks in the world.

- A mandatory reporting regime for ransomware incidents – bringing ransomware out of the shadows and maximising the intelligence used by UK law enforcement agencies to warn of emerging ransomware threats and target their investigations on the most prolific and damaging organised ransomware groups.

Commenting on the consultation, NCSC CEO Richard Horne said, "Organisations of all sizes need to build their defences against cyber attacks such as ransomware, and our website contains a wealth of advice tailored to different organisations. In addition, using proven frameworks like Cyber Essentials, and free services like NCSC's Early Warning, will help to strengthen their overall security posture."

Digital Operational Resilience Act (DORA) becomes binding for all financial entities across the EU

DORA is a harmonised and comprehensive regulatory framework on digital operational resilience. The regulation is designed to strengthen digital operational resilience and oversight over Critical Third-party ICT Providers (CTPPs).

The regulatory framework entered into force on 16 January 2023 and financial entities had until January 17th, 2025 to fully deploy and implement it.

ENISA signed a multilateral Memorandum of Understanding (MoU) with the European Supervisory Authorities (EBA, EIOPA, and ESMA - the ESAs) in June 2024 to strengthen the cooperation and information exchange on tasks of mutual interest, which includes policy implementation.

This agreement will also help support regulatory convergence and consistency across Member States to reinforce the cybersecurity resilience needed for such essential services such as financial entities.

CISA Partners with ASD's ACSC, CCCS, NCSC-UK, and Other International and US Organizations to Release Guidance on Edge Devices

CISA—in partnership with international and U.S. organizations—released guidance to help organizations protect their network edge devices and appliances, such as firewalls, routers, virtual private networks (VPN) gateways, Internet of Things (IoT) devices, internet-facing servers, and internet-facing operational technology (OT) systems. The published guidance is as follows:

- "Security Considerations for Edge Devices," led by the Canadian Centre for Cyber Security (CCCS), a part of the Communications Security Establishment Canada.
- "Digital Forensics Monitoring Specifications for Products of Network Devices and Applications," led by the United Kingdom's National Cyber Security Centre (NCSC-UK).
- "Mitigation Strategies for Edge Devices: Executive Guidance" and "Mitigation Strategies for Edge Devices: Practitioner Guidance," two separate guides led by the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC).

Foreign adversaries routinely exploit software vulnerabilities in network edge devices to infiltrate critical infrastructure networks and systems. The damage can be expensive, time-consuming, and reputationally catastrophic for public and private sector organizations. These guidance documents detail various considerations and strategies for a more secure and resilient network both before and after a compromise.

CISA and partner agencies urge device manufacturers and critical infrastructure owners and operators to review and implement the recommended actions and mitigations in the publications. Device manufacturers, please visit CISA's Secure by Design page for more information on how to align development processes with the goal of reducing the prevalence of vulnerabilities in devices. Critical infrastructure owners and operators, please see Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products for guidance on procuring secure products.

Estonia and Ukraine strengthen ties to protect critical infrastructure

Vladimir Svet, Estonia's Minister of Infrastructure, and Rostislav Zamlynsky, Deputy Head of Ukraine's State Agency for Communications and Information Protection, signed a memorandum in Kiev to strengthen their cooperation on critical infrastructure protection.

The countries will implement the Memorandum in the coming weeks, exchanging experiences on risk assessment, threat identification and infrastructure protection. Estonia will also support Ukraine in developing sectoral legislation and aligning with EU regulations.

"Critical infrastructure protection is increasingly vital in today's security climate, especially with the growing frequency of cable disruptions on the Baltic Sea bed," said Vladimir Svet. "In recent years, Ukraine has gained valuable experience in protecting critical infrastructure, not only from potential risks but also from actual attacks. This knowledge will also help Estonia enhance its preparedness."

On the other hand, Estonia's support is crucial for Ukraine on its path to European Union membership, according to the Estonian minister. "We have been through this journey ourselves, and we are happy to share our experiences with Ukraine," he added.

Joint Publications Focus on Mitigation Strategies for Edge Devices

The National Security Agency (NSA) has joined the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), the Canadian Centre for Cyber Security (CCCS), and others to release three Cybersecurity Information Sheets (CSIs) that highlight critically important mitigation strategies for securing edge device systems, including firewalls, routers, and virtual private network (VPN) gateways.

Collectively, these reports – "Mitigation Strategies for Edge Devices: Executive Guidance," "Mitigation Strategies for Edge Devices: Practitioners Guidance," and "Security Considerations for Edge Devices" – provide a high level summary of existing guidance for securing edge devices, with comprehensive recommendations for tactical, operational, and strategic audiences to enhance network security and improve resilience against cyber threats.

"Edge devices act as boundaries between organizations' internal enterprise networks and the Internet; if left unsecured, even unskilled malicious cyber actors have an easier time finding and exploiting vulnerabilities in their software or configurations," said Eric Chudow, an NSA cybersecurity vulnerability analysis subject matter expert. "As organizations scale their enterprises, even though securing all devices is important, prioritizing edge device security is vital to defend the many endpoints, critical services, and sensitive data they protect."

The guide, "Mitigation Strategies for Edge Devices: Executive Guidance" is intended for executives within large organizations and critical infrastructure sectors responsible for the deployment, security, and maintenance of enterprise networks. It outlines seven key mitigation strategies for managing and securing edge devices within traditional network architectures:

1. Know the edge
2. Procure secure-by-design devices
3. Apply hardening guidance, updates, and patches
4. Implement strong authentication
5. Disable unneeded features and ports
6. Secure management interfaces
7. Centralize monitoring for threat detection

The companion guide, "Mitigation Strategies for Edge Devices: Practitioners Guidance," is written for operational, cybersecurity, and procurement staff and provides an overview of what edge devices are; risks and threats to them; relevant frameworks and controls by some of the authoring nations; and a more in depth discussion on the seven mitigation strategies. Additionally, the report includes a case study of a successful exploitation to show how malicious actors compromise edge devices when they are not secured properly and to highlight further how edge devices are critical to the security of a network.

Expanding on the other reports, the "Security Considerations for Edge Devices" guidance details threats to edge devices from common malicious techniques and ways organizations can reduce the risk of compromise with mitigation recommendations. The publication also outlines factors organizations should consider when evaluating the security of edge devices, along with recommendations for edge device manufacturers to improve the built-in and default security of devices they produce.

TSA intercepted 9 firearms in 30 days at Detroit Metropolitan Airport

Transportation Security Administration (TSA) officers intercepted a firearm at Detroit Metropolitan Airport (DTW) in 30 days at the airport.

Including the firearm detected Friday, two have been stopped so far in the month of November. TSA officers also detected seven firearms at DTW checkpoints between the dates of Oct. 9 and Oct. 30. A total of 55 firearms have been stopped at DTW this year.

In all firearm detections at DTW, the Wayne County Airport Police were alerted, responded to the checkpoint, and confiscated the weapon.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

TRAINING

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

Robust thermal cameras for reliable detection in all light and weather conditions

Axis Communications announces three robust thermal cameras offering outstanding thermal imaging, regardless of light and weather conditions. These cameras deliver reliable detection and verification with a low false alarm rate—all while protecting privacy

AXIS Q1972-E offers high-resolution thermal imaging in a bullet form factor. With four lens alternatives (10 mm, 19 mm, 25 mm, and 35 mm), it ensures optimal installation. There are also two box thermal cameras available. AXIS Q2111-E comes with a 60 mm lens making it ideal for long-range detection to capture events taking place at great distances. AXIS Q2112-E offers high-resolution thermal imaging and a choice of lens options (10 mm, 19 mm, 25 mm, 35 mm, 60 mm) for a wider or narrower field of view, including long-range detection. The thermal box cameras can be mounted on a positioning unit (sold separately) to deliver a 360° unobstructed field of view.

These powerful thermal cameras deliver actionable insights to support informed decision-making. They come with AXIS Motion Guard, AXIS Fence Guard, and AXIS Loitering Guard preinstalled for proactive surveillance. Plus, AXIS Perimeter Defender is available with AI-based functionality for enhanced protection. Built on a powerful analytics platform, it's also possible to add custom-made third-party analytics.

These IK10-, IP66/67-, NEMA 4X, and NEMA TS2-rated cameras are impact- and weather-resistant. With I/O ports and edge-to-edge technology, it's possible to integrate and trigger other devices such as a network speaker or strobe siren. They include Axis Edge Vault, a hardware-based cybersecurity platform that safeguards the device and protects sensitive information from unauthorized access. Plus, they offer secure key storage with FIPS 140-2 Level 2 certified secure cryptographic key storage and operations.

HID Signs Agreement to Acquire 3millID and Third Millennium, Expands Physical Access Control Presence and Portfolio

HID, a worldwide leader in trusted identity solutions, today announced it has signed an agreement to acquire 3millID Corporation and Third Millennium Systems Ltd. The addition of 3millID and Third Millennium expands HID's physical access control portfolio of readers and credentials with new products in complementary geographies.

"Welcoming 3millID and Third Millennium into the HID family demonstrates our continued investment in core physical access control technologies," said Björn Lidefelt, EVP and Head of HID. "This acquisition brings new opportunities to increase customer choice and relevance within our portfolio and it enhances our presence outside of the United States."

Founded in 2015 and headquartered in Highlands Ranch, Colorado, 3millID is a leading solutions provider of proprietary access control readers and technology-enabled products to enterprise end customers in North America. Third Millennium, founded in 1996 and based in Wales, is a leading provider of access control solutions and software to enterprise and government end customers in the UK and Europe, with robust in-house technology expertise. Since 2015, the two companies have had a commercial partnership, encompassing technology development and sales.

Martin Huddart, SVP and Head of Physical Access Control Solutions, HID, said, "We look forward to welcoming the 3millID and Third Millennium teams into HID PACS. The commercial and technical expertise of these two companies expands our relevance and product range, resulting in a better ability to serve our collective customers across the globe."

Both 3millID and Third Millennium are now part of HID's Physical Access Control Solutions Business Area and will benefit from HID's sales and other global functions to support its offering.

The acquisition is subject to customary closing conditions and is expected to close in the first quarter of 2025.

Cognizant and CrowdStrike Partner to Drive Enterprise Cybersecurity Transformation

Cognizant and CrowdStrike announced a strategic partnership to drive enterprise security transformation by delivering cybersecurity services, powered by the AI-native CrowdStrike Falcon® cybersecurity platform.

Cognizant will work to enable organizations to streamline security operations and threat mitigation, consolidate fragmented legacy point products, reduce the complexity of managing cybersecurity programs, and strengthen cybersecurity posture, leveraging Falcon® Next-Gen SIEM and Falcon® Cloud Security.

Organizations are continuously evolving their IT landscapes by adopting a variety of cloud services, including IaaS, SaaS, PaaS and CaaS1, which can expose them to a wider range of increasingly sophisticated cyber threats. With a growing cybersecurity skills gap and an increasingly complex threat landscape, organizations need solutions that not only transform security operations but also consolidate point products to simplify their cybersecurity environments.

"Cognizant is committed to staying at the forefront of cybersecurity innovation," said Ravi Kumar S, CEO, Cognizant. "As the enterprise digital landscape evolves, it is crucial to leverage AI for cybersecurity and cloud-native security technologies to help stay ahead of threats and ensure the resilience of our clients' infrastructure. Our partnership with CrowdStrike is another important step we are taking to continue providing our clients with some of the most advanced and effective market-leading security solutions available."

Over the past year, cloud exploitation cases have surged by 110%, while the speed and sophistication of cyberattacks continue to accelerate, with breakout times now measured in minutes. The collaboration between Cognizant and CrowdStrike combines the power of the Falcon platform with Cognizant's Neuro® Cybersecurity platform, along with threat and vulnerability management and cloud infrastructure security offerings. This approach is designed to help customers create a flexible operations framework for new technology and threats, powered by an AI-native platform rather than separate legacy tools.

BlackHawk Datacom Evolves to BlackHawk Technology Group, Strengthening Focus on Critical Infrastructure Protection

BlackHawk Datacom, a leader in critical infrastructure protection, announces its evolution to BlackHawk Technology Group. This strategic rebranding reflects the company's ongoing focus on providing advanced electronic physical security and safety technologies. The company specializes in serving energy sector clients across renewable energy, oil & gas, and utilities, with expertise in remote and harsh environments.

As BlackHawk Technology Group, the company delivers end-to-end security solutions, industrial communications, and custom-engineered technology innovations. The company's unique ability to provide both standard and custom services ensures clients receive complete solutions that address 100% of their requirements. With over 300 renewable energy facilities secured and projects completed in 38 states and 34 countries, BlackHawk has established itself as a trusted partner in critical infrastructure protection in an increasingly complex and interconnected world.

"This rebrand represents a significant milestone for our company as we evolve to meet the growing demands of our industry," said John Poindexter, CEO of BlackHawk Technology Group. "For over a decade, we have been a trusted provider of electronic physical security and safety technologies, and our new name reflects this heritage while reinforcing our dedication to serving the industrial markets, especially in the Energy sector. Our ability to deliver solutions in remote and harsh environments sets us apart, and we look forward to continuing to provide innovative solutions and exceptional service to our clients."

BlackHawk Technology Group will continue to operate its 24/7 Incident Command Center in Lafayette, LA, and maintain its regional operations centers in Port Fourchon, LA, Houston, TX, San Antonio, TX, Lake Charles, LA, and Midland, TX. The company remains committed to its world-class safety record of zero lost-time accidents in over ten years while expanding its innovative solutions for critical infrastructure protection across the energy sector.

A New addition to the PureTech Toolbox: Integration with Echodyne's EchoShield Radar for Enhanced Security and Counter-Drone Solutions

PureTech Systems Inc., a leader in geospatial AI-boosted video analytics for wide-area perimeter and border security, is proud to announce the integration of its patented PureActiv® software with Echodyne's EchoShield radar, enhancing counter-drone detection and tracking capabilities for critical infrastructure and perimeter security applications.

This powerful collaboration delivers superior detection, classification, and situational awareness of aerial threats, including drones, providing customers with enhanced security automation and precision monitoring.

"PureTech Systems is dedicated to staying at the forefront of innovation to address emerging security challenges," said Larry Bowe, President of PureTech Systems Inc. "Our integration with the EchoShield radar sets a new benchmark for counter-drone solutions, enabling our customers to detect and monitor aerial activity with greater accuracy and reliability."

The collaboration provides a multi-layered approach to security, combining radar detection, real-time tracking, and visual verification through PureTech's advanced camera and sensor fusion software. This integration is ideal for securing critical infrastructure, military installations, airports, and other high-security areas where drone threats pose significant risks.

Going into specifics, the integration of PureActiv® software and EchoShield radar would be particularly beneficial for border security and several types of critical infrastructure.

Correctional Facilities: Detect and prevent the delivery of contraband via drones.

The system's capacity to detect and track small, unmanned aircraft systems (UAS) at long ranges while minimizing false alarms makes it especially suitable for protecting large-scale, high-value assets that are potential targets for malicious actors.

Windward Launches Critical Maritime Infrastructure Protection, an AI Solution to Detect and Counter Threats to the World's Essential Infrastructure

Windward, a leading Maritime AI™ company, announced the launch of its Critical Maritime Infrastructure Protection solution, a first-of-its-kind AI-powered solution designed to protect the world's essential maritime infrastructure including cables, pipelines, and rigs against growing threats.

Recent suspected attacks on undersea cables globally, as well as the sabotage of oil pipelines in recent years, have demonstrated the vulnerability of global energy and data networks and the vital need to secure them. The solution combines the Windward-mapped proprietary cable layer and integrated user data with its best-in-class AI-based behavioral pattern detection to empower organizations ranging from government and intelligence agencies to telecommunication and energy companies to identify, monitor, and mitigate risks before they cause disruption. It also supports post-investigations, providing evidence to insurers and law enforcement agencies.

Maritime infrastructure is the backbone of global connectivity and economic stability. Deep sea cables transmit approximately 95% of all international data and underwater pipelines transport critical energy resources, including natural gas and crude oil, across continents. According to a threat analysis by Insikt Group, there is an average of more than 100 cable faults a year, and the proximity of recent faults to areas of geopolitical conflict and reports of suspected intentional damage are causes for concern. Recent examples of cables damaged by anchors in the Baltic Sea and near Taiwan as well as the explosion that severely damaged the Nord Stream 1 and 2 pipelines in 2022 highlight the need for increased monitoring of critical infrastructure at sea.

Windward's Critical Maritime Infrastructure Protection solution addresses three primary threats to maritime infrastructure, deep-sea research operations, shallow-water sabotage, and attacks on offshore oil rigs and platforms.

critical
infrastructure
PROTECTION AND
RESILIENCE EUROPE

ADVERTISING SALES

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

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

Are you sure your national infrastructure is secure?

Co-Hosted by: International Association of CIP Professionals; INFRAGARD Members Alliance Houston

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 Attend

Register online today

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 recent 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 previous Administration, designated 16 critical infrastructure sectors that will be subject to additional oversight through the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

Trump's official platform, 'Agenda 47', highlights the need to protect critical infrastructure from cyber threats.

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.

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 and to register visit **www.ciprna-expo.com**

Speakers include:

- Steve Harris, Deputy Executive Assistant Director for Infrastructure Security, CISA
- Senator Bob Hall, State Senator, Texas Senate District 2, Texas State Senate
- John Miri, President, Electric Grid Cybersecurity Alliance
- Marshal Wilson, Co-Director, Southwest Border Food Protection and Emergency Preparedness Center
- Robert Russell, Regional Director (A) for Region 6, Cybersecurity and Infrastructure Security Agency
- Sunil Madhugiri, Chief Technology Officer, Office of the Assistant Commissioner, U.S. Customs and Border Protection
- Clint Ladd, Critical Infrastructure Protection Coordinator, Texas Department of Public Safety / Texas Office of Homeland Security
- Waqas Ahmed, Sr. Cybersecurity Advisor, Cybersecurity and Infrastructure Security Agency
- Marco Ayala, President, Houston InfraGard Members Alliance
- Lt. Col. Tommy Waller, USMC Ret., President & CEO, Center for Security Policy, USA
- Nelson Silva, Senior Product Manager, Nokia

For full speaker line up visit www.ciprna-expo.com/speakers2025

The premier discussion for securing America's critical infrastructure

Platinum Sponsor: 3B Protection

Gold Sponsors: SimSpace; Deloitte.

Silver Sponsor: JCI | Security Products

Supporting Organisations: International Association of CIP Professionals; INFRAGARD Members Alliance Louisiana; TSIME; ISIO - International Security Industry Organization

Executive Sponsors: Institute for Homeland Security; TIA; Auto-ISAC; Association of American Railroads

Flagship Media Partner: critical infrastructure protection and resilience news