critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

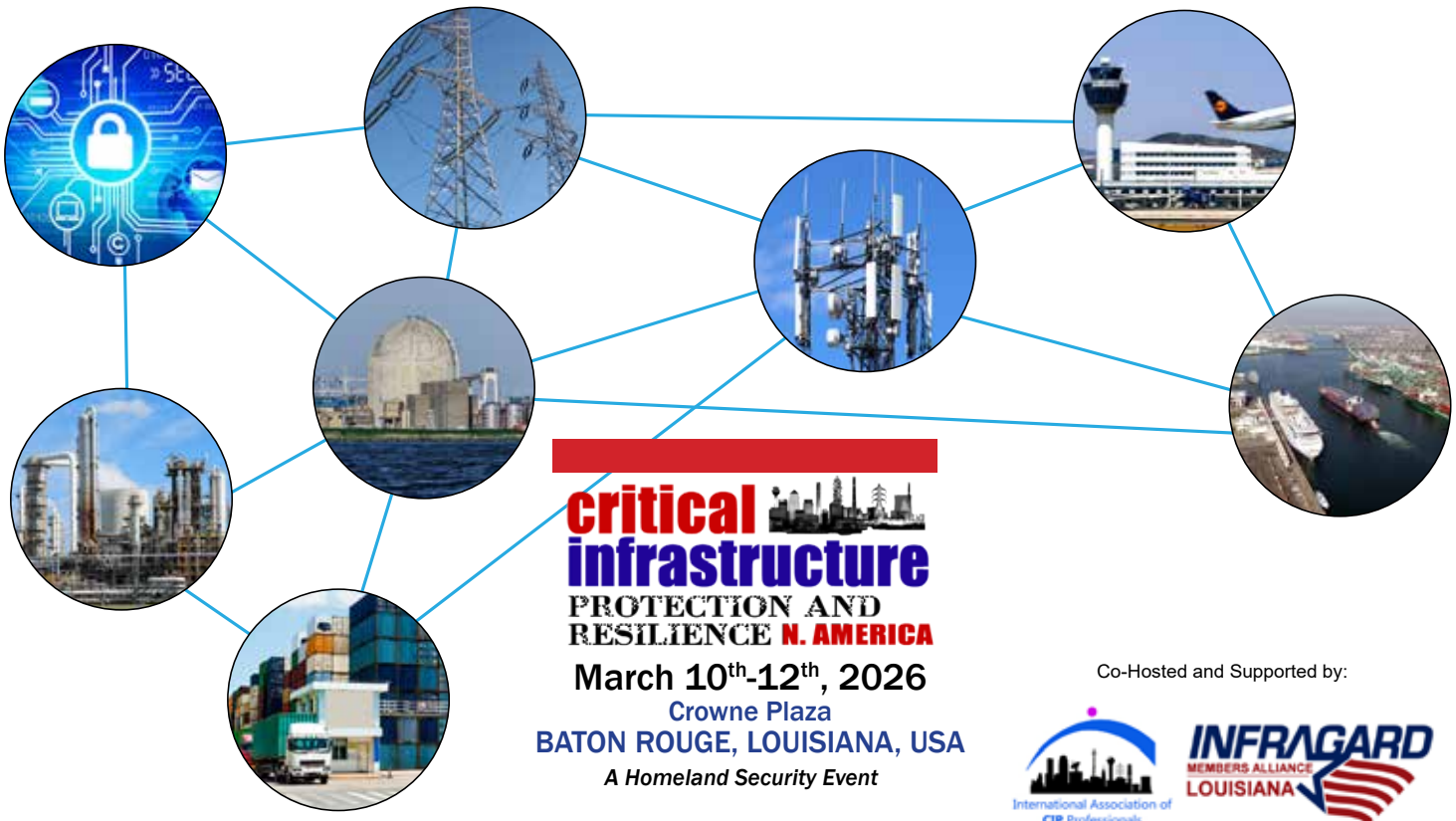
AUTUMN 2025
www.cip-association.org

FEATURE:
About civil protection forces interoperability and citizen crisis real time communication

FEATURE:
Quantum Safe Networks for Critical Infrastructure Protection and Resilience

FEATURE:
Protecting Critical Infrastructure In Nigeria's Border Communities: Counting The Giant Strides Of The NSCDC

GERMANY'S CRITICAL INFRASTRUCTURE PROTECTION (KRITIS)



critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 10th-12th, 2026

Crowne Plaza
BATON ROUGE, LOUISIANA, USA

A Homeland Security Event

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

REGISTER ONLINE TODAY

Securing the Inter-Connected Society

Early Bird deadline - February 10th, 2026

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

The 8th Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

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

If you are responsible or involved in your planning and preparatoin for securing and protecting your critical assets and entities then join us for the next gathering of operators, government establishments and industry tasked with the region's Critical Infrastructure Protection and Resilience.

For further details and to register visit **www.ciprna-expo.com**

CONFIRMED SPEAKERS INCLUDE:

Keynote: Brian Harrell,Former Assistant Secretary for Infrastructure Protection, DHS

Anuj Kumar, Senior Security Architect, Nokia

Benjamin Lampe, Engineer, Idaho National Laboratory

Anthony Adebonojo, Chairman, CCIPR-WG, International Council of Systems Engineers (INCOSE)

Joshua Tannehill, Information Systems Security Officer | VP Louisiana Chapter, Knight Federal Solutions | InfraGard

Josie Ross, Emergency Management Officer, City of Henderson Department of Emergency Management

Joseph Threat, Chief Resilience Officer and Chief Administrative Officer, City of New Orleans

Andrea Davis, President and CEO, The Resiliency Initiative

Michael Lambert, Emergency Preparedness/Homeland Security Planner, Houston-Galveston Area Council of Governments

See **www.ciprna-expo.com** for more.

The premier discussion for securing America's critical infrastructure

Owned & Organised by:

TORCH

Supporting Organisations:

INFRAGARD MEMBERS ALLIANCE HOUSTON

AUTO-ISAC

THE RESILIENCY INITIATIVE

STIME

Help2Protect

CAMO

IACI

ISIO

NS&RC

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

BUILDING RESILIENCE FOR A MORE TURBULENT WORLD

In an increasingly turbulent world, the pressure on critical infrastructure—from energy grids to data centres—has escalated dramatically over the past three months, exposing deep vulnerabilities across regions. In Europe, governments have scrambled to respond. The European Commission published new guidelines to help Member States identify and protect critical entities in sectors such as energy, transport, banking, and digital infrastructure.

In the UK, the National Cyber Security Centre (NCSC) recorded an unprecedented surge in "nationally significant" cyber incidents, with 204 such attacks reported between September 2024 and August 2025 — a 130 per cent increase on the previous year.

Meanwhile, incidents in the Baltic Sea have sharpened alarm bells, as reports emerge of "ghost" Russian-flagged tankers suspected of sabotaging undersea cables and pipelines, threatening the very backbone of Europe's energy and communications networks.

Following the recent CIP Week in Europe, hosted in Brindisi, Italy in October, and Novembers Critical Infrastructure Protection Month in America, we see across the Atlantic, local governments in the U.S., responsible for critical services like water, hospitals, and transport, are coming under sustained cyber pressure. Foreign adversaries, including China and Russia, have been implicated in persistent intrusions.

Cyble's Q3 2025 report also reveals that hacktivist attacks on industrial control systems have nearly doubled, targeting energy, manufacturing, and agriculture in both Europe and North America.

And broader concerns over AI-driven vulnerabilities in network infrastructure continue to mount, especially as next-generation telecom networks proliferate.

Far from being isolated, these challenges paint a global picture: critical infrastructure resilience is no longer just a national priority, but a shared, transcontinental imperative.

We hope you enjoy this edition of CIPR News, where we continue to explore how building resilience means more than thwarting today's threats — it means designing systems that anticipate tomorrow's.

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.

Germany's Critical Infrastructure Protection (KRITIS)

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

Germany is one of the world's leading economies, depending heavily on resilience and reliability of its CI to maintain national security and economic competitiveness. In response to evolving threats including cyber-attacks, natural disasters, and physical sabotage, the country continues to modernize and expand its regulatory and institutional architecture for CI protection.

German Federal government defines Critical infrastructures (KRITIS) as "organizations or facilities of vital importance to the public sector, the failure or impairment of which would result in lasting supply bottlenecks, significant disruptions to public safety, or other dramatic consequences". Such sectors include energy, water, information technology, healthcare, transportation, finance, government and administration, media and culture.

Ensuring protection of organisations is a core task for government and business, and a central theme of Germany's security policy. Resilience of CI increasingly becomes a priority.

KRITIS before CER and NIS2

Necessity of protecting Critical Infrastructure in Germany emerged in 1997 with a creation of a working group within the Federal Ministry of the Interior (BMI). The acronym KRITIS has been used ever since.

The first years of KRITIS protection were characterized by numerous discussions with industries associations, companies and authorities to identify specific sectoral needs. This also led to creation of the first recommendations and guidelines for operators of CI.

A major milestone was reached in 2009 with the adoption of the first National Strategy for the Protection of Critical Infrastructures (KRITIS Strategy). This strategy is still the foundation for overall execution of tasks, and it contributes significantly to their understanding and acceptance.

UP KRITIS

It is estimated that approximately 80% of Germany's CI is owned and operated by private companies. Effective communication with stakeholders including government bodies, sectoral organizations, the media, and the public is often facilitated through industrial (sectoral) associations. These associations play a key role in public-private partnerships (PPPs) for infrastructure protection.

One of the key milestones in the development of Germany's critical infrastructure protection strategy was the establishment of UP KRITIS in 2007. UP KRITIS serves as a cooperation and dialogue platform

between government authorities and private-sector operators of CI. While the initial focus was on IT security, the platform has since evolved. Today, UP KRITIS includes over 1000 members and addresses a comprehensive range of topics related to CIP, encompassing both physical and cybersecurity, as well as resilience and emergency preparedness across multiple sectors.

Given the central role of IT in nearly all critical processes and its continuous and rapid development, protection of information infrastructures has become a key priority within UP KRITIS. This focus reflects increasing complexity and dynamic nature of cyber threats.

In addition to IT-related issues, UP KRITIS addresses broader dimensions of infrastructure robustness, emphasizing that physical protection and cybersecurity must be designed and implemented as interconnected and mutually reinforcing elements of a comprehensive security strategy.

The platform's structure facilitates public-private knowledge sharing, enabling integration of business expertise with governmental capabilities in protecting critical information infrastructure. This collaborative approach has notably strengthened cross-company and cross-sector communication, which is now embedded in all UP KRITIS activities.

Evolving regulations

The Federal Republic of Germany's approach is closely aligned with evolving EU legislation, particularly the CER Directive, NIS2 Directive, and DORA Regulation. National legislation transposing these directives, such as the KRITIS Umbrella Act and the NIS2 Implementation Act establishes obligations for CI operators across physical and cyber domains. This Act regulates resilience and physical security of critical infrastructures, from 2025 onwards.

The Act sets minimum requirements and establishes a catalogue of obligations demanding operators of critical facilities to implement resilience measures. The all-hazards approach applies: every conceivable risk must be considered, from natural disasters to sabotage, terrorist attacks, and human error. Smaller critical infrastructures have the option of voluntarily implementing resilience measures and can rely on industry-specific standards. Potential funding measures are intended to help them improving.

Penalties for violating the law' provisions are intended to ensure that compliance with security standards is taken seriously and that critical infrastructures remain protected. Amounts have yet to be determined.

Federal ministries are authorized to issue legal regulations to specify resilience measures for the areas within their jurisdiction.

The regulatory landscape is set to evolve further.

CER

The forthcoming National KRITIS Resilience Strategy (2026) will provide a strategic roadmap to strengthen national coordination and sectoral resilience planning.

In contrast to cybersecurity, physical security has historically received less focus, partly due to the complex federal structure of the country, which consists of sixteen federal states (Länder) with differing responsibilities and approaches. With Germany transposing the EU Critical Entities Resilience (CER) Directive into national law by the end of the year, framework for physical resilience of critical entities will enhance.

NIS 2

Germany continues to experience a high volume of ransomware attacks and distributed denial-of-service (DDoS) attacks. In 2024, the cybersecurity industry recorded over 720 such incidents, representing a 67% increase compared to the previous year. Number of attacks targeting SMEs, government and municipal administrations increased sharply. Healthcare, and hospitals in particular, are under attacks. As for most of countries, many cyberattacks in Germany originate from foreign jurisdictions, making attribution and prosecution difficult. Perpetrators increasingly rely on cybercriminal supply chain where capabilities such as malware development, access brokerage, and laundering of ransom payments are outsourced or consumed as services within the new Crime-as-a-Service paradigm.

On July 24, 2024, the Federal Cabinet passed the draft law for the (EU Directive 2022/2555) NIS 2 Implementation and Cybersecurity Strengthening Act, bringing comprehensive modernisation of German IT security law. IT security and security incident reporting requirements are extended to more companies in more economic sectors, like energy, transport, health, or digital infrastructure. It is expected that the number of organizations subject to cybersecurity obligations in Germany will potentially exceed 30,000 entities. This presents considerable administrative and enforcement challenges for the federal level, while cybersecurity at the federal administration itself must strengthen too. The new laws replace the KRITIS regulations in place in Germany since 2014, with more operators implicated and more obligations. Originally scheduled for October 2024, its coming into force is delayed until new Bundestag in 2025.

The Federal Office for Information Security (BSI) receives new supervisory tools to enforce compliance with the new legal obligations. Operators of critical infrastructure facilities are required to register with the Federal Office for Information Security (BSI). Organizations must promptly report significant cybersecurity incidents there. Registered entities must submit a biennial report to the BSI, detailing cybersecurity measures they have implemented. For accountability and continuous improvement, organizations need to undergo certification and external audits, in accordance with defined standards and sector-specific requirements.

Institutional Architecture

Germany's CI protection is supported by a range of institutions operating at federal and sectoral levels. The Federal Ministry of the Interior (BMI) provides policy leadership and inter-ministerial coordination. The Federal Office for Information Security (BSI) oversees cybersecurity implementation and maintains national situational awareness. Public–private

coordination is facilitated through platforms such as UP KRITIS, with strong engagement from sectoral associations.

The inter-ministerial Joint Coordination Task Force for Critical Infrastructure (GEKKIS) serves three key purposes:

- Provide situational reports on protection of critical infrastructure, supporting all federal ministries with a cross-departmental overview of the up-to-date threat landscape.
- Enable communication among ministries, identify common challenges, and develop coordinated responses.
- Convene ad-hoc coordination group for relevant incidents, ensuring rapid and cohesive government action.

This collaborative institutional setup enables Germany aligning with EU standards, and ensuring tailored implementation through cross-sector coordination, federal–state integration, and public–private engagement.

Conclusion

Germany's approach to CIP follows evolving EU conceptual framework, compliance with EU directives and national implementation. Key elements include:

- Transposition of EU legal instruments into national law, notably:
  - The Directive on the Resilience of Critical Entities (CER Directive)
  - The Directive on Security of Network and Information Systems (NIS2)
  - The Digital Operational Resilience Act (DORA).
- Lessons learned from previous regulatory cycles.
- Adaptation of EU-wide concepts to Germany's federal system, accounting for sector-specific and state needs.

Most significant conceptual shift is transition from a protection-centric approach to a broader, dynamic focus on resilience, recognising that 100% security cannot be guaranteed. The emphasis increasingly shifts toward ensuring continuity and rapid recovery of services in the face of disruptions.

Key lesson is Germany's well-structured system of communication, coordination, and collaboration across federal, state (Länder), and local levels. Different stakeholders play clearly defined roles in two-way communication, both government actors and public and private sectors. Mechanisms such as centralized platforms for incident reporting, secure information exchange, and cross-sector coordination, help foster mutual trust and transparency. These structures significantly enhance situational awareness, and enable rapid, coordinated responses to emerging threats.

In the energy sector, operational continuity is central. Installed capacity must match national demand while demanding dynamic power management, with renewable energy in mind, for long-term sustainability. German experience demonstrates integration of existing systems, managed decentralization, and flexible response to demand surges and supply disruptions.

Widespread digitization of CI has exposed systems to new and complex threats, rendering traditional protection methods inadequate. Cybersecurity becomes strategic to CIP. Once a peripheral concern, it has now dedicated legislation, enforcement mechanisms, and technical standards. Rules and oversight structures dedicated to cybersecurity is a response to this reality and a model worth consideration by other countries.

Historically, the focus of CIP has been on large, high-value assets. Supply chains and SMEs now have a greater role. Risk management must extend across entire ecosystems, using unified threat catalogues to support all-hazards risk assessments. If one wants compatibility, consistency, and coordinated responses across sectors and involved operators of different organization types.

About civil protection forces interoperability and citizen crisis real time communication

By JP. Monet , X. Joseph1, A. Saint-Jonsson , T.V. Robertson , S. Pirone , S. Poyau , Brian Holecek , Roman Tandlich

Introduction

Climate change and terrorist threats are creating increasing complexity in contemporary civil protection operations. In this evolving context, appointed responders must manage a broad and diverse community of stakeholders — often including international partners.

An effective and well-coordinated first response, extending across national boundaries, is essential to address the growing frequency and intensity of large-scale incidents. Furthermore, various services and agencies must collaborate within their own countries under conditions of uncertainty, well beyond their routine operations. When required, they must also cooperate internationally to achieve the level of efficiency expected by both citizens and policymakers.

For these reasons, the authors began publishing on the topic of interoperability as early as 2014, emphasizing that this concept should not remain confined to the domains of information technology or the military.

Real situations and studies

Building on field experiences (see below) and training exercises, several studies have been conducted to capture and analyze lessons learned on interoperability. Based on these findings, the authors developed an overview of the domains identified as key areas for improving the efficiency of civil protection agencies during joint operations, particularly at the international level.

A broad range of fields have been recognized as essential to strengthening interoperability:

- Science (fundamental and applied), innovation, and research & development
- Legal frameworks (e.g., volunteering, safety, aerial regulations, financial procedures, building codes)
- Prevention, fuel management, and agriculture
- Planning and the development of a citizen risk culture
- Operational practices (logistics, command and control, field techniques, communication, safety)
- Lessons learned and post-incident practices.

After many years of relative neglect, the concept of interoperability has now gained widespread recognition and is increasingly used across international organizations: OCHA (Interoperability: Humanitarian Action in a Shared Space, 2015), the European Commission [DG ECHO, Aerial Interoperability works, 2025], the G7 (Kananaskis Wildfire Charter, 2025), FAO (FireHub Interoperability Working Group, 2025), and COP (Call to Action on Integrated Fire Management and Wildfire Resilience, COP30, 2025).

Prototype of interoperability evaluation tool, for bilateral civil protection missions

TOPIC and weighting coefficient	1/5	2/5	3/5	4/5	5/5	the score (1 to 5) ↓
GOVERNANCE 0.5	National agencies working separately	Non-formal join work between national agencies	Occasional bilateral or multilateral formal group for join work	Multilateral agreement(s) for join work and missions	Specific bilateral agreement(s) for join work and missions	
STANDARDISED OPERATIONAL PROCEDURES (SOPs) 0.5	Harmonized national SOPs	National SOPs to receive international aid	Regional SOPs	Multilateral SOPs	Spécific bilateral SOPs	
TECHNOLOGIES 1 — DATA 0.5	Manual files swap	Bilateral files exchange via a commercial	Sharing by a dedicated ad hoc interface App.	One-way sharing with standards-based software	Two-way sharing with standards-based software	
TECHNOLOGIES 1 — VOICE 0.5	Swap radios	Gateway	Shared channels	Proprietary shared systems	Bi or multilateral standards-based shared systems	
TRAINING AND EXERCICES 1	National unified training doctrine	National full scale exercices	Cross bordered training and exercising	Regional training and exercising	Multilateral or bilateral training and exercising	
LANGUAGE SKILLS 1	Use of intepreters	Acceptable use of third language	Fair use of third language	Good use of third language	Use of host country language	
OPERATIONS 2	Teams working together with limited communication	Teams working together with formalised (briefing, radio) communications	Teams achieved being integrated in the local command system	International teams having knowledge of local ICS and giving relevant interaction	Same incident command system	

Although the precise scope of the term interoperability continues to evolve, the authors have logically focused their work on its most practical and immediately actionable dimension — the operational field — including:

- Technical aspects such as equipment and resource compatibility
- Operational practices and tactical processes, particularly command and control at its highest levels [5].
- Special attention to the provision of accurate and timely information to populations at risk.

In addition to the European Union Civil Protection Mechanism training program — which remains both essential and highly effective — the authors consider that training and knowledge sharing serve as key levers for strengthening cooperation, and thus for enhancing interoperability.

Training as a Mechanism for Improvement

To facilitate the effective sharing of knowledge — particularly in the field of operational wildfire management — a series of targeted training sessions were designed and implemented. These initiatives were tested over a five-year period within the framework of EU-funded projects.

The proposed training model is structured around four main phases:

1. Expert-Led Instruction – Recognized experts provide foundational knowledge, offering a comprehensive overview of existing tools, methodologies, and frameworks.
2. Best Practices and Lessons Learned – Participants exchange experiences and lessons learned, discussing operational challenges and identifying effective techniques in collaboration with specialists from various countries.
3. Hands-On Demonstrations – Whenever possible, live demonstrations (such as ground trials or simulations) and tabletop exercises are conducted, complemented by detailed case studies.
4. Comparative Analysis and Takeaways – Participants examine similarities and differences across European regions, ecosystems, and services, in order to establish

Real Case testimony

"In 2018, I was assigned as a team leader in Sweden, during an exceptionally harsh period when the country was battling 51 wildfires simultaneously.

When I arrived at the Ljusdal fire, I was introduced to my liaison officer in the incident management team — Major Tony.

Thanks to our strong mutual understanding and professional trust, Tony and his Incident Commander succeeded in integrating our forces to achieve the highest level of performance.

Frankly, this outcome was unexpected. I was not supposed having being instructed on the typology of the Swedish command and control system, and Tony learnt and pushed, in real time, the implementation of our operational methods and the expertise of some of my officers."

a shared "baseline of commonalities" for enhanced interoperability.

The experimental workshops and training sessions demonstrated a very high level of participant satisfaction:

1. They were considered beneficial both for established fire-prone countries (by improving operational efficiency) and for newcomer countries (by building essential foundational knowledge).
2. They created lasting momentum for continued exchange on operational practices and contributed to the formation of a cross-border community of knowledgeable and collaborative officers.

Real-Time Communication with Citizens

At the same time, the crucial topic of real-time communication with citizens during crises has been explored. A detailed state-of-the-art review led to several recommendations, recognizing that the responsibility for public warning remains primarily within the competence of each nation affected by a crisis.

In this context, the authors prepared a report proposing a comprehensive framework for adopting a standardized EU Warning and Alert Messaging System applicable across the European Union, covering wildfires and other emergencies. The report examines the core principles, challenges, and opportunities associated with such a system and presents policy recommendations alongside a strategic implementation roadmap. Together, these elements outline a vision for strengthening the EU's collective capability for real-time communication during emergencies.

The adoption of a standardized EU Warning and Alert Messaging System offers a unique opportunity to unify and streamline emergency communication practices among Member States. It would promote interoperability, efficiency, and community resilience during crises. However, its implementation must carefully account for the Union's diverse legal, operational, and cultural contexts, ensuring that all measures respect national sovereignty.

Central to this initiative is a commitment to flexibility and continuous improvement, allowing the system to evolve in response to changing community needs and expectations. It must also ensure that emergency communications remain inclusive, multilingual, and accessible to all populations.

Equally important is the emphasis on collaboration—both within the Union and with international partners—which underscores the value of a collective approach. Such cooperation would ensure that EU citizens receive timely, accurate, and actionable information during emergencies, through standardized alerts and protective guidance designed to safeguard lives.

In parallel with the report, the authors conducted a survey to assess knowledge, confidence, and expectations regarding early warning systems. The survey targeted the network of partners involved in various EU projects, with potential future expansion to additional stakeholder groups. The following questions were examined:

- The level of awareness of existing early warning systems
- The level of satisfaction with those systems
- The most trusted and preferred communication channels — comparing "new technological" tools (e.g., AI, mobile apps) with "traditional" ones (e.g., television, SMS)
- The perceived importance of introducing a standardized communication protocol capable of generating protective actions (so-called "calls to react")

Preliminary findings indicate a generally good level of awareness and confidence in national early warning systems, particularly when managed by authorized public agencies. However, satisfaction is

Improve Security Resilience with Radar

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

EchoGuard®

EchoShield®

Radar for Critical Infrastructure Protection

ECHODYNE

RADAR REINVENTED™

moderate, especially regarding the systems' attention to diversity and vulnerability factors (such as age, education, language, and access to technology).

When comparing communication channels, respondents showed a clear preference for traditional media over newer technologies like mobile applications and social networks.

Finally, an overwhelming majority of participants identified as essential the development and standardization of communication protocols capable of triggering specific protective actions ("calls to react") — such as evacuation, sheltering, or confinement—upon receiving an alert message.

Conclusion

All recent achievements have been realized within the framework of the FIRE-RES (https://fire-res.eu/) and Firelogue (https://firelogue.eu/) projects — both EU-funded initiatives dedicated to wildfire management and to mitigating the escalation of such events into Extreme Wildfire Events (EWEs). However, the model presented by the authors is fully versatile and applicable to an "all-hazards" approach, extending beyond wildfires to a broad spectrum of civil protection contexts.

Within this framework, TIEMS response experts were among the first to identify and define the concept of interoperability for civil protection operations. They subsequently developed a diagnostic tool [8] to evaluate existing weaknesses and to identify potential areas for improvement. Based on this analysis, the authors formulated a set of recommendations and proposed a series of actions aimed at enhancing the efficiency of international joint response operations — including a communication framework designed to improve safety outcomes for affected populations.

These results and proposals were presented in two communications at the TIEMS Conference in Brindisi, October 2025.

UK experiencing four 'nationally significant' cyber attacks every week

In its latest Annual Review, the UK's cyber agency, a part of GCHQ, has revealed that the cyber threats facing the UK continue to escalate. The NCSC dealt with 204 'nationally significant' cyber attacks against the UK in the 12 months to August 2025 – a sharp rise from 89 in the previous year.

Of a total of 429 incidents handled, 18 were categorised as 'highly significant', meaning that they had the potential to have a serious impact on essential services. This marks an almost 50% increase on incidents of this second-highest level categorisation compared with the previous year, and an increase for the third year running.

A substantial proportion of all incidents handled by the NCSC last year were linked to Advanced Persistent Threat (APT) actors – either nation-state actors or highly capable criminal groups.

In response to the rising threat and in the wake of high-profile cyber incidents, the government has written to chief executives and chairs of leading businesses - including all FTSE350 companies - highlighting the importance of government and business working hand in hand to protect the UK economy and make cyber resilience a Board-level responsibility.

The NCSC works around the clock to counter cyber threats and bolster the UK's digital resilience. Supporting organisations to strengthen their defences is part of the government's plan to deliver national renewal focused on security, opportunity and respect.

Nationally significant incidents have a substantial impact on the UK's national security, economy or critical infrastructure, including threats to essential services, sensitive data, or key government functions.

Highly significant incidents represent an even more serious threat, often requiring a coordinated cross-government response due to their potential to cause widespread disruption or long-term damage to national interests.

PQC Migration: Mappings to Risk Framework

The Australian Signals Directorate's The NIST National Cybersecurity Center of Excellence (NCCoE) has published an initial public draft of NIST Cybersecurity White Paper (CSWP) 48, Mappings of Migration to PQC Project Capabilities to Risk Framework Documents.

Cryptographic algorithms are vital for safeguarding confidential electronic information from unauthorized access. For decades, these algorithms have proved strong enough to defend against attacks using conventional computers that attempt to defeat cryptography. However, future quantum computing may be able to break these algorithms, rendering data and information vulnerable. Countering this future quantum capability requires new cryptographic methods that can protect data from both current conventional computers and the quantum computers of tomorrow. These methods are referred to as post-quantum cryptography (PQC). The NCCoE Migration to PQC project is a collaboration with industry and government to demonstrate capabilities that support an organization's migration to PQC.

The Need for Action

Organizations should start planning now to migrate to PQC, also known as quantum-resistant cryptography, to protect their high value, long-lived sensitive data.

Historically, it has taken a long time from the moment that a new algorithm is standardized until it is fully integrated into information systems.

No one knows how long it will take to build a cryptographically relevant quantum computer. Predictions vary widely, but some people think it may be possible in less than 10 years.

Even if computer security experts implement post-quantum encryption algorithms before sufficiently powerful quantum computers are built, a lot of encrypted data remains under threat because of a type of attack called "harvest now, decrypt later." This attack describes an adversary who can't crack the encryption that protects our secrets at the moment who works to capture encrypted data and hold onto it, in the hopes that a quantum computer will break the encryption down the road.

Quantum Safe Networks for Critical Infrastructure Protection and Resilience

By Giampaolo Panariello, CTO Network Infrastructure Nokia, Italy

As the world increasingly relies on interconnected digital systems, the vulnerability of critical infrastructure to cyber threats has become a pressing concern. Traditional cryptographic methods, while effective for securing communications today, are at risk of being compromised by the advent of quantum computing. Quantum-safe networks, which incorporate cryptographic techniques and key distribution methods resistant to quantum algorithms, offer a promising solution to ensuring the long-term security and resilience of critical infrastructure.

Increasingly powerful quantum computers make the threat to current cryptographic systems loom large. The timeline for a cryptographically relevant quantum computer (CRQC) is uncertain, but the cybersecurity migration needed to counter this threat is the largest we've ever faced and will take considerable time and effort.

Telecommunication networks, responsible for transporting our data, are a crucial element in this equation. However, there is no one-size-fits-all solution to make a network "quantum-safe". Quantum safe network is not a technology,

but an outcome of different measures that can reduce the risk of a CRQC attack

In the 1990s, Nokia Bell Labs researcher Peter Shor invented a new algorithm for prime factorization, specifically designed to run on quantum computers. Using Shor's quantum algorithm, a sufficiently powerful quantum computer would be able to crack encryption algorithms that are widely used today.

Recent advancements in quantum computers heighten the threat of a "cryptographically relevant" quantum computer. However, not all cryptographic algorithms are vulnerable to this threat.

Symmetric and asymmetric cryptography

Only asymmetric cryptography (a.k.a. public-key cryptography) can be broken by future quantum computers using Shor's quantum algorithm. Symmetric cryptography, though vulnerable to Grover's quantum algorithm for brute force attack, remains safe.

Primitive quantum computers have been available for a while, but they are still far from being able to break today's asymmetric ciphers.

Although the exact timeline is uncertain, experts envisage a cryptographically relevant quantum computer becoming available within the next decades. Despite this, Harvest Now Decrypt Later (HNDL) possible attacks and increasing investments on quantum computer research, supported by AI, are shifting much closer the risk of CRQC on the cryptography.

To address this threat, a new generation of quantum-safe

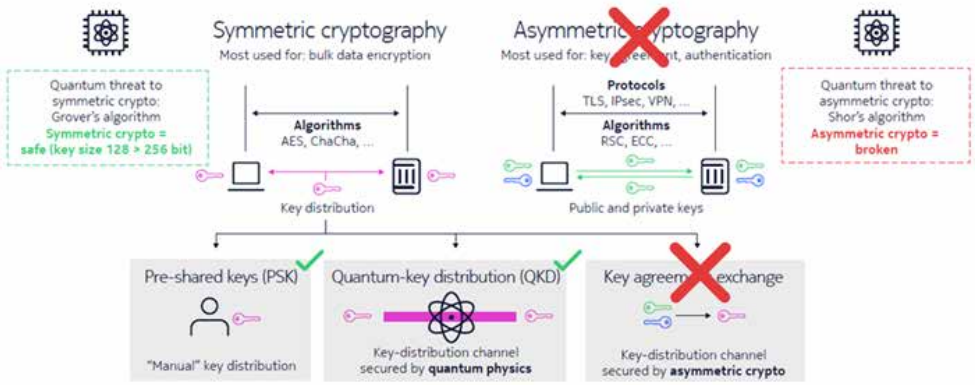


Figure 1: Symmetric and asymmetric cryptography

asymmetric cryptography, called post-quantum cryptography (PQC), is being actively researched and developed. The "post-quantum" designation shows that these new algorithms have—so far—been proven to be un-hackable, even by a quantum computer. The first versions of such PQC algorithms were standardized in August 2024 by NIST.

Symmetric and asymmetric cryptography are typically used for different purposes today (see Figure 1).

Symmetric cryptography is mostly used for the encryption of static connections carrying large volumes of data, owing to the larger computational complexity of asymmetric cryptography. Asymmetric cryptography, on the other hand, is mostly used for authentication and for the exchange of symmetric keys in ephemeral connections between endpoints that are not preconfigured (combining the advantages of symmetric and asymmetric cryptography). Both symmetric and asymmetric cryptography can achieve quantum safety, albeit through distinct methods.

Quantum-safe solutions

Quantum-safe solutions are already commercially available today. Their applicability is uncontrolled/static environments with a small number of endpoints and a large volume of traffic (e.g., transport network links or enterprise connectivity).

Seven different main measures can be put in place to reduce the risk of CRQC attacks. The first five are summarized below:

1. Use Symmetric encryption on the user plane, with secure encryption algorithms like Advanced Encryption Standard (AES). AES encryptors can be used in different layers of telecommunication protocol stack, implementing secure protocols like OTNSec, MACSec, ANYSec, IPSec, TLS etc…
2. A sufficiently large secret key size (256 bits), following the results of the Grover algorithm applied to CRQCs that reduces the complexity of a brute force attack quadratic speedup for searching unsorted databases
3. Key entropy: ensuring sufficient key randomness (entropy) by, e.g., using a physics-based random number generator that never repeats itself. This increases key unpredictability, crucial

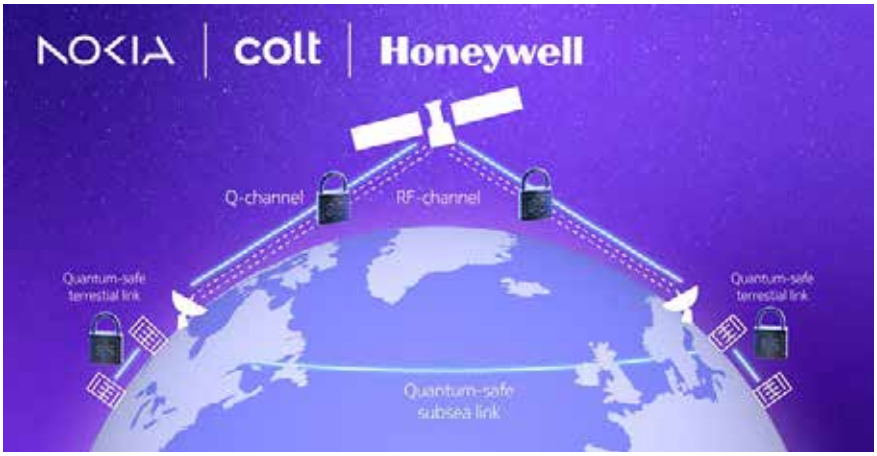


Figure 2: Nokia – Colt – Honeywell partnership for Satellite Quantum Key Distribution

for countering brute-force and cryptanalytic attacks.

4. Key rotation: periodically refreshing keys limits the volume of data encrypted by a single key, making it harder to hack and limiting the blast radius in the case of successful hacking

5. Sharing the secret key. There are multiple ways to establish a shared secret key in a quantum-safe manner:

   - Using pre-shared keys (PSK), relying on a manual provisioning process or automatic centralized symmetric key distribution (Symmetric Key Infrastructures – SKI). The PSK is not necessarily used to encrypt the data itself. Data is often encrypted by another key (the security association key or SAK) that is securely distributed leveraging encryption from a PSK (used as a key encryption key or KEK) over an out-of-band channel.
   - Using post-quantum cryptography (PQC)-based Key Encapsulation Mechanisms (KEMs)
   - Using Quantum-Key Distribution (QKD), leveraging quantum-physical properties. Two QKD-capable endpoints can establish a common secret key across a dedicated quantum communication channel that is immune to eavesdropping. However, it's important to note that, for now, QKD is a partial solution that needs to be complemented by other methods.

Quantum Key Distribution: a partial solution

Although sometimes perceived as a complete solution for quantum-safe networking, QKD occupies a specific place in the quantum-safe solution landscape: it is a partial solution for generating a shared secret key for symmetric encryption. QKD also uses an additional classical channel of communication that requires authentication (to ensure information is exchanged with the correct entity on the other side). Authentication on this channel, however, requires using another cryptographic method such as asymmetric cryptography or pre-shared keys.

Terrestrial QKD also still faces some practical limitations impeding its large-scale adoption. It is severely restricted by distance limitations over terrestrial networks (current operation is limited to ~100 km over optical fiber) and requires special-purpose equipment. Furthermore, it is highly susceptible to denial-of-service attacks, as any manipulation of the quantum states of the transmitted photons destroys the ability to exchange a key over the QKD link.

Practical implementation of terrestrial QKD is today limited to short distances: the use of trusted nodes could extend the distance, at the cost of more quantum appliances and security constraints in the trusted node itself. Moreover, it is strongly suggested to implement QKD protection in "crypto-agility" with other quantum safe key distribution techniques like SKI.

Satellite QKD will soon solve the distance limitations, considering that optical attenuation in the fiber is exponential, while optical attenuation in free-space is quadratic: the use of satellites as intermediate trusted nodes can extend the range of the QKD to thousands of kilometers (figure 2).

Quantum-safe asymmetric solutions (PQC), yes but….

PQC will replace current asymmetric cryptography, which is used in more dynamic and uncontrolled environments with many endpoints. Since asymmetric cryptography is more complex than symmetric cryptography, they are often used together for data encryption. This combines the best of both worlds, establishing the secret key with asymmetric algorithms while doing the encryption with symmetric algorithms.

World Border Security Congress

14th-16th April 2026

Vienna, Austria

www.world-border-congress.com

Developing Border Strategies Through Co-operation and Technology

SAVE THE DATES

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

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

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

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

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

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

www.world-border-congress.com

for the international border management and security industry

Co-hosted by:

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

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

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

Supported by:

OSCE Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

African Young People Support Centre

ISIO

International Association of CIP Professionals

NSaRG

Media Partners:

World Border Security Network

BORDER SECURITY REPORT

World Security-Index.com

PQC is based on new mathematical algorithms conjectured to be difficult to solve, even with quantum computers. Those new PQC schemes will be used, for example, for exchanging keys in protocols like Transport Layer Security (TLS), and digital signatures used for authentication, code-signing or message digests (with different uses being addressed by different PQC algorithms).

Since 2016, the US National Institute of Standards and Technology (NIST) has been running an open competition and standardization effort for evaluating and selecting PQC algorithms, which do not rely on quantum computing and run on traditional computing platforms. NIST released the first PQC standards in August 2024.

But there are some limitations also in PQC: it is based on mathematics algorithms, and, like RSA, it could be broken by a quantum/ supercomputer in the next years.

Then, migration of classical asymmetric cryptography to PQC will take time (NIST has recognized that, historically, it has taken 10 to 20 years to fully implement cryptographic migrations), in the mean-time Harvest Now, Decrypt Later (HNDL) attack is ongoing and CRQC attack asymmetric cryptography could start to be available.

This make PQC a brick of the Quantum Safe solution, but not the only one…

Defense-in-depth: Crypto Redundancy and Crypto Agility

The above considerations are bringing to the last two measures

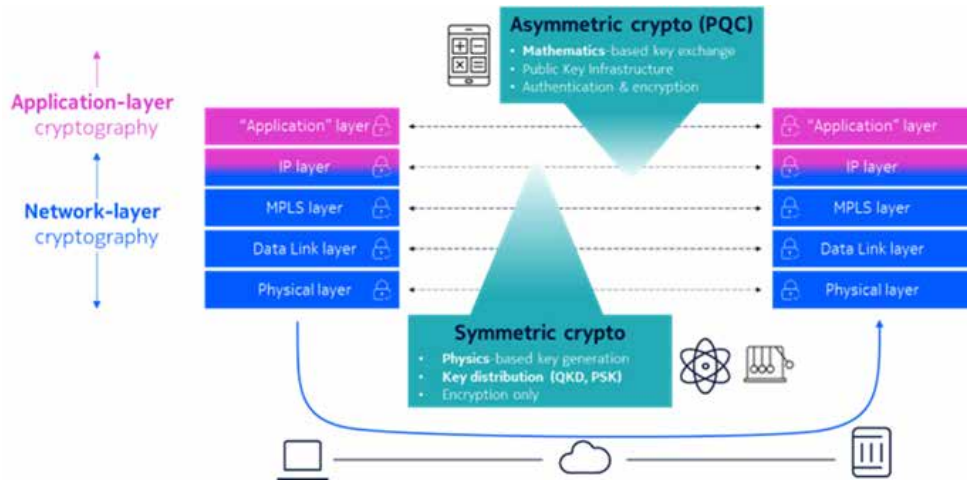


Figure 3: Crypto-Redundancy

to reduce the risk of CRQC attacks: Crypto Redundancy and Crypto Agility, in general the Defense-in-Dept concept.

A Communication stream is composed of a multi-layer protocol stack. In modern communications, encryption is implemented at application layer, using algorithms like TLS, based on asymmetric, not quantum safe, key agreement.

Even if migration of conventional cryptography to quantum safe PQC is already started or will start soon, best practice would be to protect application layer encryption with encryption on one (or more) network layers: this can strongly reduce the risk of CRQC attack during migration phase to PQC, protecting at the same time against HNDL attack. Moreover, after the migration of application layer encryption to PQC, the network layer encryption can further protect against the risk of future PQC algorithm break: this is what we call crypto redundancy (figure 3).

Crypto-agility is the ability of a system, protocol, or application to easily and safely switch between different cryptographic algorithms or protocols.

It's an important design principle in cybersecurity because cryptographic algorithms can become obsolete over time due to advances in cryptanalysis, increased computing power or Evolving standards.

In general, crypto-agility is the best answer against the change of threats.

Examples of Crypto-Agility are:

- Network layer quantum safe cryptography protection during the application layer cryptography migration to PQC
- Network layer quantum safe cryptography protection during upgrade to safer PQC algorithm at application layer
- QKD seamless switch to SKI during a denial-of-service attack to the QKD layer (e.g. attack to the fiber to steal quantum material for key decrypting)

Conclusions

The advent of quantum computing poses a significant threat to the security of critical infrastructure, highlighting the urgent need for

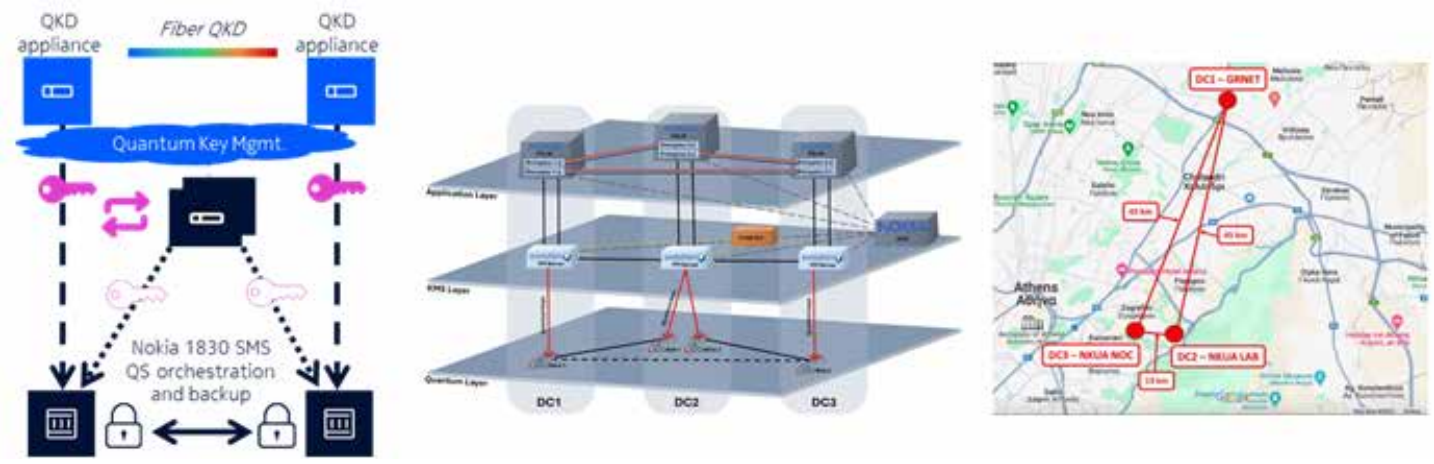


Figure 4: Example of crypto-agility: QKD protection with SKI. Conceptual block diagram and on field implementation in the frame of EuroQCI program in Greece.

the adoption of Quantum Safe Networks. The importance of early migration to quantum safe protection cannot be overstated, as it will enable the protection of sensitive information and prevent potential disruptions to critical services.

Network encryption technologies play a crucial role in safeguarding the Post-Quantum Cryptography (PQC) migration at the application layer, ensuring the confidentiality, integrity, and authenticity of data transmitted over critical infrastructure networks. The implementation of a Defense-in-depth approach, incorporating multilayer cryptography (crypto redundancy) and crypto agility, is essential to counter the evolving threat landscape.

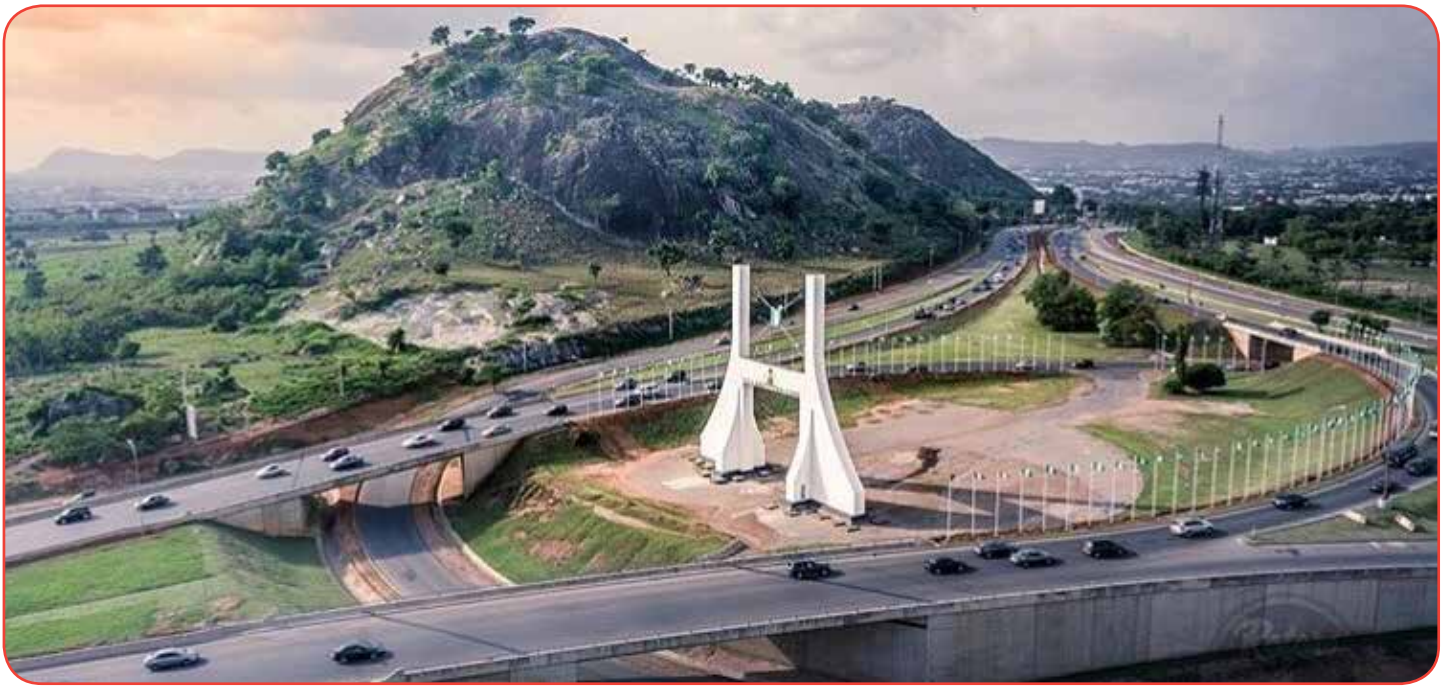
The use of multilayer cryptography provides an additional layer of security, ensuring that even if one layer is compromised, the other layers remain intact, protecting the data. This crypto redundancy is vital in mitigating the risks associated with the potential compromise of a single cryptographic algorithm or protocol.

Furthermore, crypto agility is critical in enabling the swift adaptation to changing threats and the seamless integration of new cryptographic protocols and algorithms as they become available. This agility ensures that critical infrastructure networks can respond effectively to emerging threats, minimizing the risk of disruption and ensuring the continued availability of essential services.

The evidence suggests that a proactive approach to quantum safe protection, incorporating a Defense-in-depth strategy with multilayer cryptography and crypto agility, is essential for protecting critical infrastructure from the threats posed by quantum computing. By prioritizing migration to quantum safe networks and adopting a robust and agile cryptographic framework, organizations can ensure the long-term resilience and security of their critical infrastructure, safeguarding the integrity of sensitive information and preventing potential disruptions to vital services.

To take the next step, it is recommended that organizations begin by conducting a thorough risk assessment to identify areas of vulnerability and develop a comprehensive migration plan to quantum safe networks. This plan should include the implementation of network encryption technologies, multilayer cryptography, and crypto agility, as well as ongoing monitoring and evaluation to ensure the continued effectiveness of these measures. By taking a proactive and multi-faceted approach to quantum safe protection, organizations can ensure the security and resilience of their critical infrastructure in the face of emerging quantum threats.

Protecting Critical Infrastructure In Nigeria's Border Communities: Counting The Giant Strides Of The NSCDC



By: George-Okoli Francisco Chidi, Director Of Programs - West African Action Network On Small Arms (Waansa) Nigeria

Critical infrastructure refers to physical or virtual systems, assets, and resources that are essential for the functioning of a society, its economy, and the overall well-being of the public. Examples include water and sewage systems, transportation networks, communication systems, and healthcare facilities. The destruction of such infrastructure can have a crippling effect on national development.

Infrastructure plays a vital role in sustainable development by providing essential services, supporting economic growth, promoting resource efficiency, enhancing resilience to climate change, fostering social inclusivity, and ensuring long-term economic viability.

Border communities are groups of people living near the boundaries

of two or more nation-states or sub-national regions, whose social and economic lives are significantly shaped by their proximity to these borders. In Nigeria, many border communities are characterized by weak governance, inadequate infrastructure, and in some cases, complete absence of basic amenities. Where infrastructure does exist, it is often vulnerable to vandalism by cross-border criminal elements. Despite these challenges, Nigeria's borders remain critical sources of trade, migration, and regional cooperation.

To address these issues through strategic security restructuring, the Nigeria Security and Civil Defence Corps (NSCDC) Act No. 2 was enacted and signed into law by former President Olusegun Obasanjo, granting the Corps full paramilitary status.

One of the biggest challenges in protecting critical infrastructure in border areas is the sheer length and porosity of Nigeria's frontiers. Spanning over 4,000 kilometers, the borders shared with Niger, Chad, Cameroon, and Benin are difficult to monitor continuously. Criminal elements exploit poorly guarded stretches to smuggle arms, sabotage pipelines, and vandalize installations before retreating across national lines. This problem is compounded by the proliferation of illegal small arms and light weapons (SALW), often hidden in legitimate cargo or carried across unmanned routes, feeding a cycle of insecurity that threatens both the population and the infrastructure they rely on.

According to the Nigeria Customs Service (NCS), a total of 3,897 arms and ammunition, including 1,599 firearms and 2,298 cartridges were handed over to the National Centre

Gallant officers of the NSCDC showcasing readiness and unity in service to national security

for the Control of Small Arms and Light Weapons (NCCSALW) on February 13, 2025. The Comptroller General of Customs, Adewale Adeniyi, noted that the seizures, made between 2018 and 2024, underscore continuing port and border interceptions, with significant coordination across inland routes in partnership with the Nigeria Security and Civil Defence Corps (NSCDC) and other security stakeholders (Punch Newspaper, February 14, 2025, Anozie Egole). This highlights how persistent and organized arms smuggling continues to challenge Nigeria's border security and infrastructure protection efforts.

In many locations, law enforcement presence is limited, with understaffed posts and officers lacking adequate training or equipment to deter well-armed groups. Complicating matters further, there is sometimes a gap in trust between residents and security agencies, which reduces community cooperation and intelligence sharing. Weak coordination between different security bodies such as customs, immigration, police, and the military has also slowed rapid responses to emerging threats, allowing criminals to evade capture. Economic hardship in border towns adds another layer to the challenge, as some residents are tempted to collaborate with those who damage or exploit critical infrastructure.

Amid these difficulties, the Nigeria Security and Civil Defence Corps (NSCDC) plays a vital role in safeguarding critical national assets, particularly in sensitive border zones. Tasked with the protection of infrastructure such as oil pipelines, power installations, telecommunications equipment, and border facilities, the NSCDC has deployed specialized units trained in both physical security and intelligence gathering. In several northern border communities, NSCDC operatives have successfully intercepted attempts to vandalize oil pipelines and have dismantled makeshift storage facilities used for smuggled petroleum products. Along the Benin border, the Corps has worked with local vigilante groups to protect rural electrification projects from theft and destruction, ensuring that power supply to these remote areas is maintained.

The Corps' Critical Infrastructure Protection Unit, often operating in collaboration with other agencies,

The NSCDC Commandant General, Dr. Ahmed Abubakar Audi, OFR, mni (Ph.D) with gallant officers on water patrol; strengthening maritime security and safeguarding Nigeria's critical assets.

conducts regular patrols, rapid-response missions, and community outreach programs. By engaging directly with traditional rulers, local leaders, and youth groups, they have improved trust and encouraged timely reporting of suspicious activities. NSCDC's approach combines deterrence with engagement, making it harder for criminal elements to operate unnoticed.

Similarly, in the Northeast, the NSCDC and the Nigeria Immigration Service (NIS) pledged tighter joint action with the NCCSALW in Borno State, committing that all seized or recovered SALW would henceforth be handed over to the Centre for disposal. The move, announced in Maiduguri, is expected to strengthen border-facing arms control efforts in the Lake Chad corridor (National Accord Newspaper, August 16, 2025, Tom Chiahemen). This kind of inter-agency synergy shows how arms control and infrastructure security are increasingly linked in Nigeria's border management strategy.

Improving protection for critical infrastructure in Nigeria's border communities requires a blend of technological, human, and economic strategies. Modern surveillance systems such as drones, satellite monitoring, and motion detectors can close the gaps left by physical patrols. Expanding law enforcement capacity, providing specialized training in counter-terrorism and anti-smuggling operations, and improving officer welfare can strengthen the frontline. Building community trust through development projects, recruitment of locals into security services, and incentivizing whistleblowing will make residents partners in protection rather than bystanders. Inter-agency coordination can be enhanced through joint command centers and shared intelligence platforms, ensuring faster and more effective responses. Addressing the root economic drivers of collaboration with criminals through vocational programs, microcredit schemes, and agribusiness opportunities will further weaken the incentives to attack or sabotage national assets.

Ultimately, securing Nigeria's border infrastructure is not just about stopping crime; it is about strengthening national resilience. The NSCDC's ongoing efforts, backed by partnerships with agencies like Customs, Immigration, and the NCCSALW, demonstrate that with the right mix of enforcement, technology, and community partnership, it is possible to defend these critical systems. Protecting them is not only a matter of national security but also a prerequisite for sustainable economic growth and regional stability.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

Help2Protect.info

Protect your company from Insider Threats

In Collaboration with:

International Association of CIP Professionals

See below for 20% Off Special Offer

THREE TYPES OF INSIDERS - ONE TOOL TO DETECT THEM

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

BE PROACTIVE
AWARENESS TRAINING

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

BE READY
PROGRAM DEVELOPMENT TRAINING

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

An eLearning Platform dedicated to Security and the Insider Threat

www.help2protect.info

SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE

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

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

CLOSING COMMENTS - 10th CRITICAL INFRASTRUCTURE PROTECTION & RESILIENCE EUROPE & 2nd CIP WEEK

The Critical Infrastructure Protection and Resilience Conference (CIPRE) took place between the 14th and 16th October this year. This was the 10th annual conference and exhibition in Europe and this year the event was delighted to partner with The International Emergency Management Society (TIEMS) as the two key events delivering the second Critical infrastructure Protection Week in Europe.

The conference took place in the historic venue of the Teatro Nuovo Teatro Giuseppe Verdi. This is the main theatre in the centre of the beautiful city of Brindisi, Italy.

This was an excellent event bringing together people from across Europe and beyond to consider the considerable challenges faced by those within the world of Critical Infrastructure and Information. It was Chaired by John Donlon QPM FSyI and detailed below are his closing comments reflecting on the success of CIPRE and CIP Week 2025.

Ladies and Gentlemen, before we all head off home, I just wanted to close the conference with a few comments. It has been fantastic to be here in Brindisi with so many talented and professional people.

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

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

We are extremely grateful to all the people and the organisations who have supported us and shared their knowledge, expertise and enthusiasm with us. In particular, I need to thank the Mayor of Brindisi, Giuseppe Marchionna and his team for hosting us in this fantastic venue and for ensuring that the glass floor over these beautiful ruins was strong enough to take the weight of all the delegates after so many biscuits and pizzas. I also need to thank Alessandro Lazari who has provided his time and energy over many months to ensure everything was arranged perfectly.

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

We had a great start on Tuesday afternoon with the keynote session. The Mayor did the welcome address where he spoke about the complexities of the times in which we live, marked by hybrid threats, geopolitical challenges and natural events all of which severely test the stability of our societies. He went on to highlight how important it was to strengthen sharing, cooperation and innovation.

The complexities and unpredictability of our time continued as a constant theme throughout the last few days.

Harald Drager, the President of TIEMS shifted the focus of the keynote session for a short time, providing us with a brief history lesson. Harald spoke of the Norman Conquest and then the Battle of Hastings which took place on the same date as the start of the conference, the 14th October, only being 959 years earlier in 1066. I wonder in years to come which event, the battle or CIPRE will be most remembered!

The Plenary Session later on Tuesday afternoon explored the Developing and Implementation of Risk Assessments

and Emergency Management within CER and NIS2. The panel within this had representatives from the Joint Research Centre (JRC) of the European Commission, the Organisation for Security and Co-operation in Europe (OCE), TIEMS and from the University of Salento.

Also on this panel was Oleksandr Sukhodlia, the Head of Critical Infrastructure, Energy and Ecological Security Department within the National Institute for Strategic Studies in Ukraine. Oleksandr provided a fascinating insight into the significant challenges of protecting infrastructure in wartime conditions. He also articulated his concerns around the preparedness of Europe to be in a position to deal with the ever increasing and concerning threats created by the increased use and capability of Drones.

Drones and Unmanned Aircraft Systems (UAS) were a topic which attracted a great deal of discussion. We had a whole session dedicated to the work being done by the Joint Research Centre, the PRESERVE Project and Industry to accelerate, not only the mitigation stance against such weapons, but also their use as a protection tool.

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

- The progress being made with CER and NIS2
- Emerging Threats
- Terrorism
- Risk Assessments and Emergency Management
- Communications
- A great deal of discussion on Collaboration, Information Sharing and Public Private Partnerships – and a session on
- Maritime and Ports

Cyber Security and Artificial Intelligence (AI) were, as expected, extremely topical with several speakers. Many of whom were urging caution at the pace of change through AI going as far as to say that AI activity should be paused until we have a greater understanding of the drawbacks it may bring.

We were provided with a snapshot of what the most common cyber attack methodologies were during 2024 and then a deep dive into what the cyber threat landscape looks like this year.

I was a little surprised that we did not hear more on the issues connected to Insider Threat. Catherine Piana from The Confederation of European Security Services (CoESS) made reference to this in her video presentation but there was only a smattering of references to this subject of rising concern.

Catherine did provide some interesting statistics on the subject showing that most insider cases, 74% to be exact, are caused by negligence & accident. She provided some useful guidance about how that number can be greatly reduced through a focus on organisational security culture and enhancing levels of awareness and training.

So it was a very busy week which was nicely concluded with our Workshop/Table Top exercise this afternoon. Thank you to Alessandro and his colleague, Shkumbin, for the time and effort that they put into developing this scenario and moderating the session. They posed a number of challenging situations to the delegates generating some very interesting discussions and conclusions.

As I said on day one, our world continues to be Unpredictable and is Changing at an Incredible Pace. The

protection and resilience of our infrastructure and information requires us all to continually change, adapt and innovate and though events such as this we all have the opportunity to:

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

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

Next year, CIPRE will take place in Brussels between the 20th and 22nd October and Critical Infrastructure Protection and Resilience North America (CIPRNA) will take place in Baton Rouge in March 2026.

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

Safe journeys home and thank you once again.

John Donlon QPM FSyI
Conference Chairman
Chairman, IACIPP

Energy resilience in the Netherlands: application of the CER directive and identification of critical entities.

By J. Santiago Patterson, J. van Diemen, M.J.J. Scheepers, TNO

The resilience of essential services is a cornerstone for national security and societal stability in the European Union. With this in mind, and as a response to emerging threats and interdependencies between critical infrastructure sectors, the EU introduced in 2022 the Critical Entities Resilience (CER) directive. One of the main points in this directive instructs member states to identify the critical entities that ensure the continuity of essential services across these sectors, including energy. This paper presents the collaboration efforts between the Netherlands Organization for Applied Scientific Research (TNO) and the Dutch Ministry for Climate and Green Growth (KGG) to apply the CER directive to the Dutch energy sector. The project aims to develop a reliable and repeatable method to determine the list of critical entities for each of the selected sectors: natural gas, oil, electricity and district heating.

The proposed method is based first on the definition of the value chains for each subsector followed by the development of a threshold

Critical Infrastructure Protection Week *in Europe*

20th–22nd October 2026 – Brussels, Belgium

International Association of CIP Professionals

critical infrastructure PROTECTION AND RESILIENCE EUROPE

SAVE THE DATES

Building Resilience for the Critical Connected World

The International Association for CIP Professionals is delighted to be hosting the next CIP Week in Europe in Brussels, Belgium for the next annual industry gathering in October 2026.

Critical Infrastructure Protection and Resilience Europe (CIPRE is Europe's go-to event for critical infrastructure protection and resilience — bringing together top minds from industry, government, and beyond to shape the future of security and resilience across vital sectors.

CALL FOR PAPERS - Deadline 31st March 2026

The CIPRE Conference Committee are currently accepting abstracts for consideration for inclusion in the 2026 conference agenda.

Visit www.cipre-expo.com for more details how you can be a speaker or benefit from being a sponsor at the event.

Join us in Brussels for the third CIP Week in Europe and the 11th Critical Infrastructure Protection and Resilience Europe discussion on securing Europe's critical infrastructure.

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Co-Hosted by:

International Association of CIP Professionals

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

To discuss sponsorship opportunities contact:

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

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

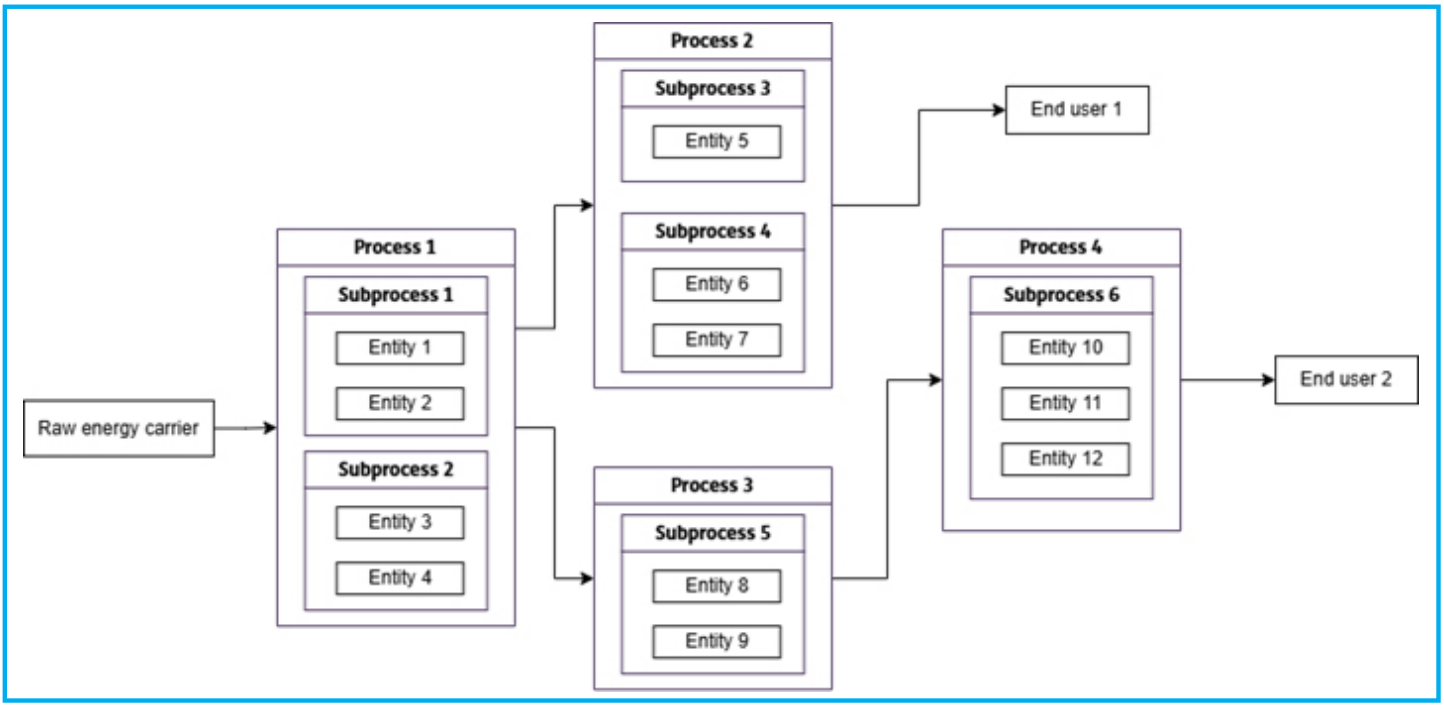


Figure 1 General structure of the energy subsectors value chains.

framework that could be used to assess the criticality of processes and entities within the sector. Both pieces of work are then combined in a systematic way to arrive to the final lists of critical entities. The paper starts by presenting the value chains and how they were assembled in Section 2, followed by an explanation of the threshold framework in Section 3. The combination of both approaches and the full method and its application are then outlined in Section 4. The paper concludes with the main findings and implications of this project in Section 5.

Energy sector value chains

In order to identify the critical entities of the energy sector in the Netherlands, a global overview of each subsector is needed. This overview allows the identification of the critical processes within each energy subsector and the interdependencies between them. This was built in the form of value chains for each subsector.

A value chain is defined as the series of steps needed to convert raw energy carrier into a useful resource to consumers and deliver it to said consumers or commercial agents. For example, in the case of oil, this comprises the whole process from crude oil extraction to the delivery of oil products to users. Each value chain is divided into multiple sections that contain a series of processes, subprocesses and assets. A process is defined as each of the activities that enables the previously established value chain. The type of processes can range from engineering, such as production or treatment of an energy carrier, to logistical like transmission and distribution, or commercial, like energy trading, among other types. Each of these processes is carried out by one or multiple entities. An asset is defined as a piece of infrastructure or equipment that enables the previously defined processes. These assets are usually owned and maintained by the entity responsible for said process. The general structure used to build these value chains is shown in Figure 1.

As seen in the figure, these chains provide a clear overview of the main processes involved in each subsector, the main entities responsible for each process and subprocess, and finally, the interrelation and interdependencies between processes. One of the early challenges when defining these values chains is defining their scope. Since the CER directive focuses on entities that enable the value chain in each member state, the limits of the value chain were placed on the processes that happen within the Netherlands. At the edge of these value chains, are the interfaces with neighbouring countries, usually in the form of border connections. The CER directive focuses on the entities that enable the value chain, so final consumers are excluded from the analysis. To further illustrate this with an example, a portion

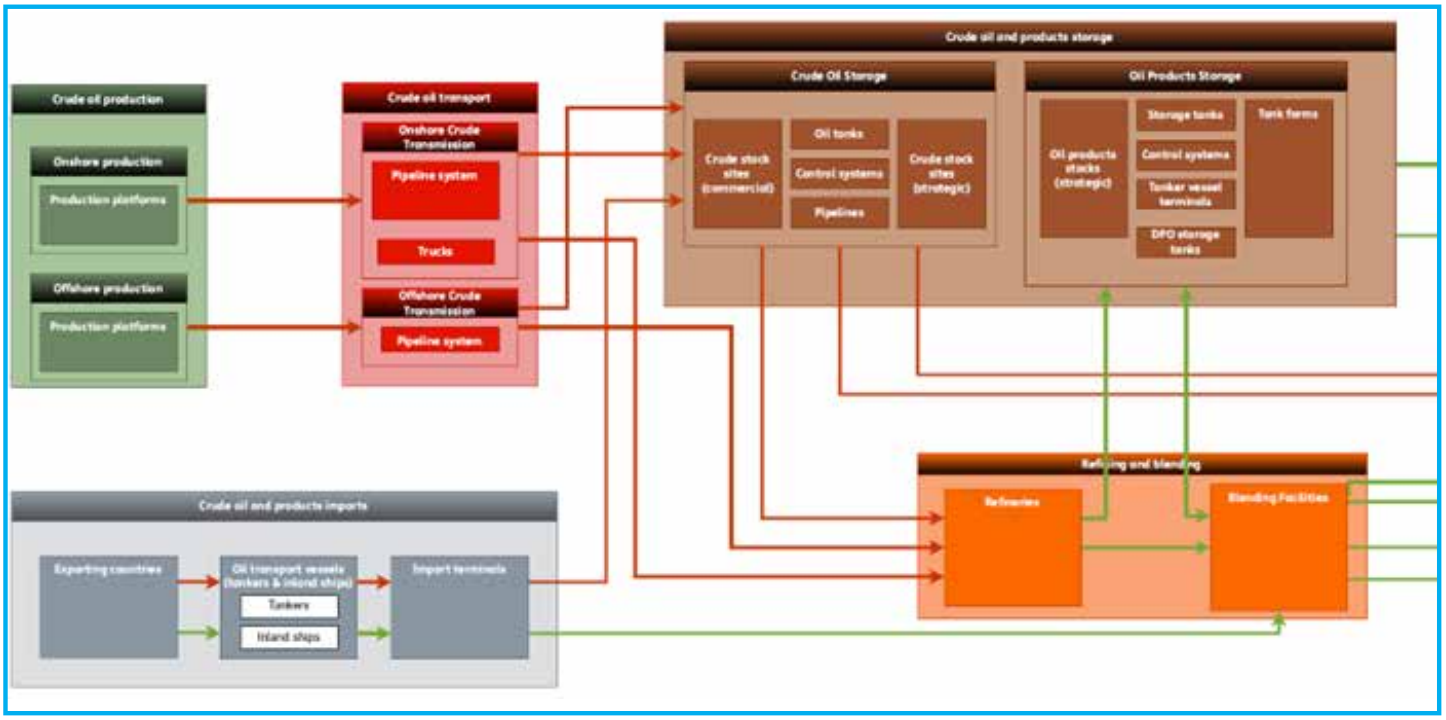


Figure 2 Detail of the oil value chain diagram.

of the oil value chain is shown in Figure 2. This diagram shows the first stages of the value chain, where the oil is produced from different sources or imported into the Dutch system. At each stage, each of the necessary processes is shown, such as onshore and offshore production or crude and oil products storage.

The identification of the processes for each sector was elaborated through a combination of sources. The main one was internal expertise across departments specialising on different energy carriers within TNO. At the same time, during the construction of these value chains, experts from the field, belonging to different entities responsible for each process, were consulted. Aside from this visual representation, a separate spreadsheet mirroring the diagram for each subsector was built. These spreadsheets contain more detailed information on the subsector, including energy volumes, detailed lists of assets and the full list of entities present at each process. The information used to build these overviews was extracted from public sources such as [1], [2] and [3]. This data allowed a better understanding of the weight of each process and subprocess, facilitating the later identification of the critical entities.

All of the processes discussed until now refer to the state of the sectors at the time of writing in 2025. An additional exercise was performed, where an outlook on the state of each subsector was analysed for 2035. In this case, instead of elaborating the whole value chain, only differences with 2025 were illustrated. Examples of this are the expected drop in production of natural gas in the Netherlands [4] or changes in the Dutch refinery market [5]. Additionally, hydrogen was included as a new sector that could play a more significant role in 2035.

Threshold framework

After defining the value chains for each subsector, a clear overview of all the processes and entities is now possible. In order to identify which of these processes are critical, a quantitative framework was established in order to identify the critical processes in a clear, repeatable and uniform way.

For each subsector studied, the CER directive [6] identifies a series of critical entity categories, shown in Table 1. In turn, each of these entities has a series of processes and entities that enable their services. In order to determine if an entity is critical according to the CER, this entity must be essential to enable said process. The question then comes down to what makes an entity essential in the context of a given service. This assessment can be done through a threshold framework. Each service can be assigned one or more thresholds based on a series of criteria. If an entity that

provides such service exceeds one or more of these thresholds, it can be then considered critical. The CER directive defines a series of criteria to define these thresholds, shown in Table 2. As seen, all these criteria have a qualitative description and the challenge then becomes the quantification of these thresholds.

The first criterion refers to the number of users that are dependent on an entity that provides one of the services listed in Table 1. To establish a threshold for this parameter two different sources were used: the Dutch risk assessment guideline for integrated national security risk analysis [7] and the values already used by neighboring countries such as Germany, Belgium and Denmark. Each of the subsectors studied have different characteristics and scales they operated within, resulting in different threshold values for each subsector.

To asses interdependencies between CER sectors, first the dependencies between the energy subsectors needs to be determined. Firstly, all of the subsectors are directly dependent on the electricity subsector, powering a significant part of the processes that enable all of the value chains. In the case of natural gas, dependencies were identified in the electricity and heat subsectors, mostly related to natural gas powered boilers and energy stations. In the case of oil, some of the electricity processes, such as emergency diesel power generation were identified. Finally, in the case of heat, no other sector was identified as dependent on it. Furthermore, the

Subsector	Entity category
Electricity	• Electricity supply companies. • Distribution system operators. • Transmission system operators. • Electricity producers. • Electricity market operators. • Market participants that provide aggregation, demand response or energy storage services.
District heating and cooling	• Operators of district heating and cooling.
Oil	• Operators of oil transmission pipelines. • Operators of oil production, refining and treatment facilities, storage and transmission. • Central stockholding entities.
Natural gas	• Gas supply companies. • Distribution system operators. • Transmission system operators. • Storage system operators. • LNG system operators. • Natural gas production companies. • Operators of natural gas refining and treatment facilities.

Table 1 CER essential entity categories per subsector.

CER directive identifies ten other critical sectors, such as transport, government services, wastewater or public health among others. Additionally, member states can add their own sectors to the list, with water management being an important one for the Netherlands. All of these critical sectors can be dependent on the studied energy subsectors. When trying to identify critical entities, it is also important to evaluate whether any of these critical sectors are dependent on them.

An entity can be considered critical if an incident that would affect it would cause a significant disruption to society. In this context, the magnitude of this impact depends on the duration and the severity of the incident. The main source used to assess the weight of a potential disruption duration was [7]. This national guideline defines the severity of an incident based on the duration of it and the number of users affected by it. In the case of electricity, gas and heat this threshold can also be addressed from the angle of security of supply. In the Netherlands, operators are obliged to compensate users economically depending on the duration of the outage. In the case of the oil sector, a national emergency plan exists, born from the legacy of past oil supply crises [8], where different severity levels are activated based of established thresholds. At the same time, entities have been appointed to permanently maintain established strategic stock levels of crude oil and products at all times to mitigate the impact of potential disruptions.

In addition to the duration of the disruption, in [7] the impact on societal interests are also considered when evaluating the impact of a disruption. In the context of energy, special mention is made to critical off-takers. Regular households are usually covered by the 'number of users' criterion, but critical users, such as schools or hospitals, need to be

Criteria mentioned in the CER
The number of users relying on the essential service provided by the entity concerned.
The extent to which other sectors and subsectors as set out in the CER Directive Annex depend on the essential service in question.
The impact that incidents could have, in terms of degree and duration, on economic and societal activities, the environment, public safety and security, or the health of the population.
The entity's market share in the market for the essential service or essential services concerned.
The geographic area that could be affected by an incident, including any cross-border impact, taking into account the vulnerability associated with the degree of isolation of certain types of geographic areas, such as insular regions, remote regions or mountainous areas.
The importance of the entity in maintaining a sufficient level of the essential service, taking into account the availability of alternative means for the provision of that essential service.

Table 2 List of criteria used to define critical processes and entities, defined in the CER directive.

evaluated separately. Entities that directly supply these users can be also considered critical, even if the total number of users does not meet the other thresholds. Additionally, possible severe impacts on the environment can also be considered as severe societal impact. Entities that, in case of failure, would cause environmental disasters, can also be considered critical.

The size and composition of the market that provides the critical service can also play a role in the critical entities determination. A market share threshold can be used to assess this. In the case of a market with a monopoly or oligopoly (either natural or regulated), entities responsible for it are directly critical. In the case of a competitive market, an appropriate value has to be defined as a threshold.

Regarding the threshold of geographic area, two aspects are of importance: the geographic cover of the entity and connections to neighboring countries. In the case of electricity and gas in the Netherlands, the sector is divided into geographic areas that are supplied by given network operators. In most of these cases, the areas contain enough households to reach the number of households threshold previously defined, making most of these operators critical. In the case of the heat networks, they tend to be more localized and cover a smaller number of users, requiring extra analysis when defining the critical operators. In the case of cross border-connections, the Netherlands acts as an energy hub for the electricity, natural gas and oil energy carriers.

The final criterion suggested in the CER is the importance of a given entity for the supply of a critical service. This is the most general criterion described in this section and can be used to appoint as critical entities that play a special role in the supply chain of an energy subsector. This usually concerns entities that, if disrupted, can cause major failures or fallouts in the rest of the value chain without reaching any of the previously defined thresholds.

Using all of the criteria and sources described in this section, a collection of thresholds for every CER service was compiled for each subsector. For the sake of illustration, an extract of this threshold collection is shown in Table 3 for the oil sector in the Netherlands. The exact threshold values have been redacted due to confidentiality reasons. An entity that provides at least one of the essential services and has a large enough presence to exceed the thresholds is considered critical. For this reason, exceeding a single threshold value is enough to appoint that entity critical, even in cases where the service has multiple critical thresholds. Additional tables like Table 3, one for each subsector, can then be used to identify the critical entities present within it.

Identification of critical entities

After describing the value chains for every subsector and compiling the full list of threshold values for every essential service, the final step was to apply all this to build the final list of critical entities. Before this took place, a first version of the value chains and the threshold framework was shared with prominent entities within the electricity, natural gas, oil and district heating subsectors in the Netherlands. The list of organizations to consult was assembled together between TNO and KGG, consisting of both private and public entities and regulators. After collecting all the feedback, a final version of the value chains descriptions and the threshold framework was elaborated. With this work in place, it was now possible to determine the critical entities for each sector. The method used to accomplish this is described in this section.

Subsector	Essential service	Criteria	Threshold value
Oil	Pipeline transmission.	Dependency of other critical sectors.	Sectors: XX
		Cross-border connections.	Connections to XX and XX.
	Oil production.	Market share.	XX of national production volume.
	Oil refining and treatment.	Market share.	XX of national refining capacity.
	Storage.	Market share.	XX of national storage capacity.
		Importance of entity.	Storage volume of XXm³.
	Stockholding	Importance of entity.	XX

Table 3 Threshold values established for the CER services for the oil subsector in the Netherlands.

As explained in Section 2, each subsector was described using a series of processes and subprocesses, with each of them having a list of entities assigned to it. These processes are useful to describe the value chains from a physical point of view, identifying the fundamental steps and the relationship between them. The main limitation of this description is that it does not match one-to-one the essential services described in the CER. This can be overcome by mapping every subprocess in the value chain to its corresponding CER service. This can be done by applying specific sector knowledge to make the connections. An example result is conceptually shown in Figure 3, where it can be seen that an essential CER service can cover one or multiple processes from the value chains. At the same time, there are subprocesses that do not match any of the CER services.

As explained in Section 2, each process of the value chain was assigned the main entities that enable it at a national level. Thanks to this, once every service has been mapped onto the value chain, it is now possible to link every entity to its corresponding CER service. Combining this insight, with the threshold framework information, it was now possible to link every entity to its corresponding threshold criteria. This is done by using tables such as Table 3, where each service (and now entity) can be assigned a series of threshold criteria and values.

The final step before being able to appoint the critical entities, is to score each entity according to the threshold criteria assigned to it. Again, using the corresponding table for each sector, such as Table 3, every threshold criterion has a parameter assigned to it. This can be for example, number of connections to other countries, total national market share, or specific energy volumes, among others. By researching each sector and entity, it is usually possible, by using publicly available data, to compute these values for each of the previously identified entities.

After completing all of the previous steps, every entity of the value chain is categorized in one of the CER essential services, its threshold criteria identified and how it scores according to this criteria. The final step is to compare the scores of each entity with the maximum threshold values for each criterion, defined in Section 3. If an entity has a single threshold score above the maximum allowed threshold criteria values, it is defined as a critical entity. Applying this process for each sector, service and entity, results in a list with the critical entities requested by the CER directive.

In summary, the method described is structured as follows:

1. Identify every process and subprocess that enable the value chain of the subsector and the relationships between them.
2. For each process and subprocess, identify and collect the main entities responsible for it.
3. Using the criteria defined in the CER, establish a list of threshold values for every critical service also defined in the CER.

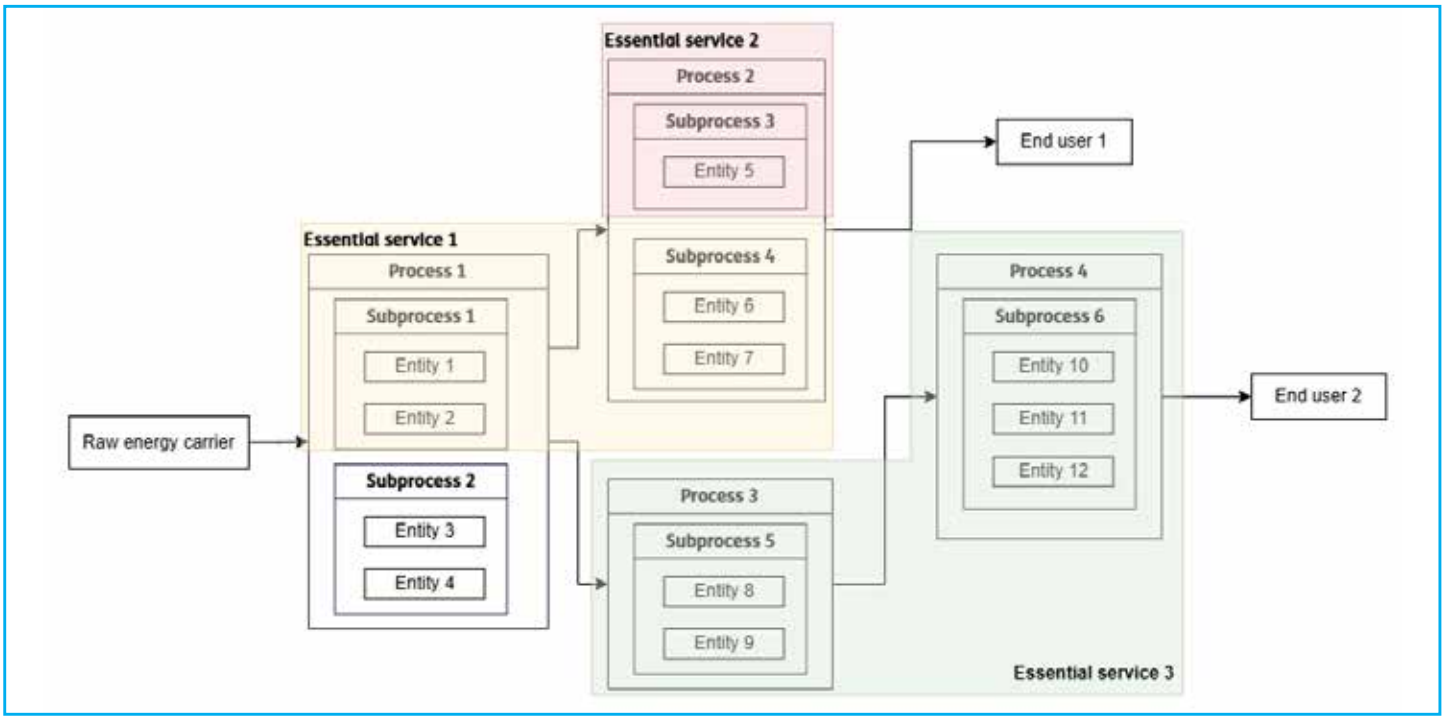


Figure 3 Mapping of the essential services mentioned in the CER for a given subsector to its value chain processes.

4. Map every essential service to its corresponding processes and subprocesses from the value chains defined in step 1.
5. For every essential service, assign it all of the entities previously defined in step 2 that correspond to every (sub) process collected in step 4.
6. Based on the threshold framework developed in step 3, assign the corresponding threshold to every entity, depending on the essential service(s) it is assigned to.
7. Compute every entity's threshold score for every criteria assigned to it in step 6.
8. Identify what entities have threshold values that exceed the threshold limits defined in step 3.
9. All of the entities that come out from step 7 are assembled into the final list of critical entities.

This method was developed by TNO with advice and support provided by KGG and entities and regulators of each subsector. Once the method was developed and all of the necessary data collected, it was then put into practice in a series of workshops. Each workshop was set to cover one subsector with the goal of reaching the final list with all of its corresponding entities. The parties present in these workshops were the corresponding sector expert groups from TNO, the group responsible for the critical entities appointment at KGG and some key experts from entities within the sectors. Aside from the final list of entities, these workshops also yielded some additional insights. One of them was that, while applying the threshold criteria to entities, in cases where there were multiple of them, one usually dominated. This reduced the number of criteria conflicts and could allow to streamline the threshold framework in a second iteration. Another important insight, is that the list of selected entities can vary significantly depending on the exact threshold values selected. In these cases, additional arguments, such as information from neighboring countries, can be useful to define a more robust threshold value. Finally, it was found that not all CER services are relevant to all countries. For example, only a selection of countries will have entities that will meet the minimum threshold values for fossil fuel production services.

Through this process, TNO provided the ministry with a robust, repeatable method. This method can be applied to any of the discussed energy subsectors and used as a blueprint to identify the critical entities within them. However, the ministry is the responsible body that will ultimately decide which entities will be appointed as critical. As previously mentioned, this method was applied to the current energy landscape in the Netherlands. As future work, it would be interesting

to apply this method to different time and geographical scales. The energy sector is expected to change significantly in the coming decades, with new players emerging and old ones fading out. Applying the presented method to the expected sector in ten or twenty years from now could provide useful insights into the evolution of the sector. At the same time, applying it to a European scale could highlight important international dependencies within the continent. Finally, this method does not have to be necessarily limited to the energy sector. It could potentially be applied to other critical sectors that operate in a similar way through value chains and commodity deliveries. Examples of possible sectors could be drinking water management or food production. Finally the current analysis has been performed at a fairly high and abstract level. There could be potential value to be added by including a more quantifiable approach. This could be done through energy network modeling and specific risk scenario analysis.

Conclusion

Through this paper, a methodology was presented and applied for the determination of the Dutch critical entities of the energy subsectors, defined in the EU CER directive. By defining the value chains for each subsector, (natural gas, oil, electricity and district heating), a comprehensive understanding of the main processes and entities present in each of them was established.

After this, a threshold framework was developed to evaluate the criticality of each of these processes and entities. This framework was grounded in the criteria defined also in the CER, including sector dependencies, societal impact and geographic and market shares, among others. The threshold values and categories were tailored for each subsector and service by applying public sources, expert knowledge and consultations to important sector entities.

These two pieces of work were then combined to establish the method applied to appoint the final lists of critical entities. This was done by mapping the processes and entities identified in the value chains to the services and threshold criteria established in the threshold framework. Then, during workshops held between TNO experts, KGG and sector representatives, every entity was classified into its corresponding CER service and their position respect to the established threshold values computed. The application of this method can be used to compile a final list of critical entities for each subsector.

The outcome of this method enables a systematic and robust approach for the determination of the critical entities as defined in the CER directive. This work contributes to a more resilient energy system in the Netherlands, rooted in a repeatable and fact based approach built in collaboration with the subsectors themselves. It also sets the pillars for future updates and refinements and enables the Netherlands to adapt to a changing energy and threat landscape in the coming decades.

UK experiencing four 'nationally significant' cyber attacks every week

Latest Annual Review reveals that the cyber threats facing the UK continue to escalate.

The National Cyber Security Centre (NCSC) has handled an average of four 'nationally significant' cyber attacks every week in the year to September.

In its latest Annual Review, the UK's cyber agency, a part of GCHQ, has revealed that the cyber threats facing the UK continue to escalate. The NCSC dealt with 204 'nationally significant' cyber attacks against the UK in the 12 months to August 2025 – a sharp rise from 89 in the previous year.

Of a total of 429 incidents handled, 18 were categorised as 'highly significant', meaning that they had the potential to have a serious impact on essential services. This marks an almost 50% increase on incidents of this second-highest level categorisation compared with the previous year, and an increase for the third year running.

A substantial proportion of all incidents handled by the NCSC last year were linked to Advanced Persistent Threat (APT) actors – either nation-state actors or highly capable criminal groups.

In response to the rising threat and in the wake of high-profile cyber incidents, the government has written to chief executives and chairs of leading businesses - including all FTSE350 companies - highlighting the importance of government and business working hand in hand to protect the UK economy and make cyber resilience a Board-level responsibility.

The NCSC works around the clock to counter cyber threats and bolster the UK's digital resilience. Supporting organisations to strengthen their defences is part of the government's plan to deliver national renewal focused on security, opportunity and respect.

Nationally significant incidents have a substantial impact on the UK's national security, economy or critical infrastructure, including threats to essential services, sensitive data, or key government functions.

Highly significant incidents represent an even more serious threat, often requiring a coordinated cross-government response due to their potential to cause widespread disruption or long-term damage to national interests.

Today, the NCSC has also launched a new resource for small organisations to help them implement foundational controls. The Cyber Action Toolkit is designed to help sole traders and small organisations put in place some of the basic cyber security measures that help guard against the most common cyber threats.

Businesses are also urged to implement Cyber Essentials, which helps organisations guard against the most common cyber attacks. The certification scheme includes automatic cyber liability insurance for any UK organisation who certifies their whole organisation and has less than £20m annual turnover.

Dr Richard Horne, Chief Executive of the NCSC, said, "Cyber security is now a matter of business survival and national resilience. With nearly half the incidents handled by the NCSC deemed to be nationally significant, and a 50% rise in highly significant attacks on last year, our collective exposure to serious impacts is growing at an alarming pace. The best way to defend against these attacks is for organisations to make themselves as hard a target as possible. That demands urgency from every business leader: hesitation is a vulnerability, and the future of their business depends on the action they take today. The time to act is now."

Securing the Digital Backbone: How Nokia is Building Resilient, Autonomous Critical Networks

As the world's most vital systems go digital, the networks underpinning them must become smarter, stronger, and more secure. Nokia's vision: resilient, cloud-native, and increasingly autonomous infrastructure built for a connected future.

From Carrier-Grade to Enterprise-Critical

The digital transformation of critical infrastructure—power grids, transport, public safety, and defense—is reshaping how societies operate. Behind the scenes, these systems depend on networks that must perform flawlessly under pressure, withstand disruption, and recover instantly.

Prakash Sadagopan, Head of Enterprise Wide Area Networks, Nokia Cloud and Network Services

For Nokia, ensuring that level of resilience requires more than incremental upgrades. It means applying carrier-grade expertise to the enterprise-critical environment.

"What we're talking about are mission-critical, complex deployments which mimic a service provider," says Prakash Sadagopan, Head of Enterprise

Wide Area Networks at Nokia's Cloud and Network Services division. "These are large-scale networks that need the performance, latency, reliability, and security you'd expect from a carrier—but scaled for enterprise."

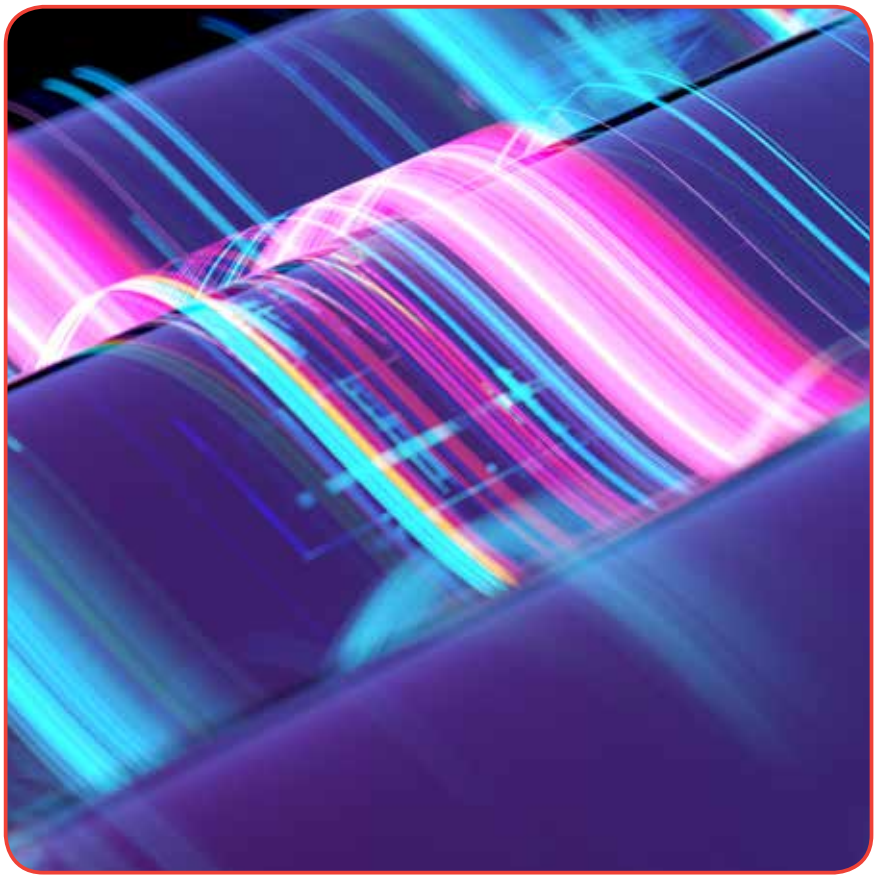
Over the past few years, Nokia has systematically repurposed its telecom technologies for mission-critical sectors. "A couple of years back, we took the CSP solutions—what we would deploy for the likes of Telefónica or T-Mobile—and looked at how to tailor them for enterprise markets," Prakash explains.

The outcome was Nokia Core Enterprise Solutions—pre-integrated, pre-configured network cores designed for verticals such as utilities, transportation, defense, and public safety. Each is fine-tuned for its domain: for example, broadband push-to-talk for first responders or ultra-reliable connectivity for energy networks.

Cloud Native, Built for the Long Haul

At the heart of Nokia's innovation is a cloud-native architecture—a modular, containerized approach that replaces monolithic legacy systems. This shift allows operators to scale services quickly, update without downtime, and deploy advanced analytics or automation in real time.

"Cloud native has become very high momentum," Prakash notes. "You can now deploy microservices and modular architectures that aren't bound by legacy systems. For enterprises, that means they can leapfrog many of the challenges CSPs had to work through."



It's a transformation that's redefining how critical networks evolve—making them more agile, responsive, and ready for autonomous operation.

Security by Design, Not by Addition

As networks grow in complexity, so do the risks. For critical infrastructure, security must be embedded, not bolted on.

"You deploy such a sophisticated system—you cannot have vulnerabilities sitting in the open," Prakash says. "We start with a minimum viable security posture: perimeter protection, endpoint detection, identity and access management. And we build from there."

Nokia's Design for Security framework ensures every layer—from the network core to edge compute—is built around verified, certified development practices. This prevents gaps that can be exploited once systems go live.

Encouragingly, customers are now embracing that philosophy. "A year ago, we often had to convince customers to procure security alongside the core," he recalls. "Today, most of them do it as standard."

Private Cloud First: Control and Sovereignty

In an era where data sovereignty and regulatory compliance are paramount, private cloud remains the architecture of choice for most mission-critical deployments.

"From a mission-critical standpoint, the need to deploy on public cloud is still very limited," he says. "Ninety-nine percent of my deployments today are on private cloud."

Nokia integrates endpoint detection and response (EDR) and identity management within these environments, ensuring operators retain control of their data, access, and infrastructure.

"You cannot leave it to the cloud provider," he emphasizes. "You need your own guardrails around compute, storage, and SDN elements."

Towards Autonomous, Self-Healing Networks

The next phase of infrastructure evolution is autonomy—networks that can monitor, predict, and respond automatically to events in real time.

"We call it autonomous mission-critical networks," says Prakash. "Enterprises will need autonomous operations even more than CSPs—triangulating analytics-led operations, automation, and security."

Nokia's roadmap aligns with the TM Forum's Autonomous Maturity Model, which defines five stages of automation. Today, most operators sit around Level 2; the goal is to reach Level 4, where prediction and prevention replace reaction.

Responsible AI for Real-World Reliability

Artificial intelligence plays a central role in this vision, but Nokia approaches it with rigor and restraint.

"We moved from MLOps to AIOps, and now into what we call the autonomous network fabric, built around the principles of sense, think, and act," Prakash explains. "AI analyzes telemetry and observability data to make networks smarter—but everything is certified before it's deployed."

Every AI model undergoes governance review by Nokia's global CTO office and Cloud and Network Services division. Prakash noted that this deliberate and disciplined approach is what differentiates mission-critical AI, building confidence through certified performance before models ever enter live service.

Bridging the Legacy Gap: From TETRA to Broadband

In public safety and defense, one of the major transitions underway is the move from TETRA radio systems to broadband cellular. Through partnerships with firms like Leonardo, Nokia is enabling a secure, smooth migration path.

"The migration from TETRA to cellular hasn't yet become mainstream," he says. "That's why we integrated Leonardo's mission-critical push-to-X (MCX) platform into our public safety solution. It gives customers a proven pathway to broadband while preserving reliability."

Designing for Resilience

In a hyperconnected world, resilience is no longer just about redundancy—it's about adaptability, prediction, and continuous protection.

"Resiliency, security, and the ability to react faster—or even predict disruptions through AI—that's the holy grail," the Prakash Sadagopan concludes. "We can't predict everything that will happen, but we can design networks that respond intelligently when it does."

Ultimately, Nokia's mission is to build not only networks that connect, but networks that protect—secure by design, autonomous by intent, and resilient by nature.

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

The PRESERVE project

We met Eduardo Villamor, Senior Project Manager at ETRA I+D who is the project coordinator of the PRESERVE project.

Ben Lane (BL): Hello Eduardo. Please give us a brief overview of your work at ETRA – https://www.grupoetra.com – and your involvement with the Horizon Europe project, PRESERVE – https://preserve-he.eu/

Eduardo Villamor: (EV): I am a Senior Project Manager at ETRA I+D. I manage and coordinate the implementation of EU projects in the field of security and defense. GRUPOETRA is a large industrial group based in Spain with multiple locations worldwide. We develop large-scale distributed control systems for critical infrastructure operators, law enforcement agencies, and army forces. We also design and manufacture drones and counter drone systems. And we are the project coordinators of the PRESERVE project, which is dealing with the so far unmanageable threat of weaponized consumer drone swarms.

Eduardo Villamor, Senior Project Manager at ETRA

BL: Please give us an overview

of the PRESERVE project; core mission and specific gaps or threats, for example, of swarm-based drone attacks. How does this project aim to address these areas?

EV: PRESERVE's mission is to protect EU citizens and public spaces from terrorist attacks, articulated through current and emerging drone technologies and open-source knowledge by equipping the police authorities with an advanced shield. PRESERVE's approach enables effective prevention before the attack is unleashed, and timely and informed multi-layer countermeasures within an ongoing attack for seamless operational response and mitigation. It provides tools against drone-related threats with ever-growing cases, including drone swarms and kamikaze drones in conflicts such as the Russian-Ukraine war, or other conflicts in the Middle East.

The objective is the protection of EU citizens proactively before these threats spread through the EU. This has been also highlighted by the European Commission in a communication that was released at the end of 2023, for non-cooperative drones in this case. They highlighted that the modus operandi of terrorist groups and the enhanced skills in the use of off-the-shelf drones could reach our borders and represent a threat. PRESERVE is ahead of the curve, anticipating that such kinds of threats could reach us as we are starting to see in some member states.

BL: Please give us an idea of the four products of the platform and touch on this idea of the C-UAV training program and how that integrates.

EV: PRESERVE will deliver a comprehensive counter-UAS framework with four main products, as you said. The first one is called SECURE, which stands for Swarm-Based Counter-UAS Arsenal, which is a nomadic suite of sensors and data-fusion components for threat prediction and rapid neutralization in complex large-scale environments in public spaces while ensuring compliance with applicable regulations. Then we have ODIN, which stands for Online Drone Intelligence Engine. It is a digital tool for gathering and analyzing multimodal online data, including text, images, and audio to detect early indicators of attack planning or threat escalation in the web. The third product is the PRESERVE Platform, which is an integrated Command, Control and Coordination platform using the data that is collected from the previous products to manage the full spectrum of drone threat prevention, detection analysis and mitigation. And finally, is the PRESERVE training program, which is an advanced training initiative building on previous training programs which are deployed worldwide. Updating this training for the current threat scenarios, updating law enforcement training in line with new technologies, as well as with emerging tactics, techniques, and procedures.

BL: So, let us look at some real-life, real-world case studies and how they are being selected and what is going to happen in this space?

EV: We started this venture by gathering a consortium of 18 partners spread across 11 EU and non-EU countries. Among these partners we have the Spanish national police, the Hellenic police, the Romanian Ministry of Internal Affairs, and the General Police Inspectorate of Moldova.

We discuss between the technical partners and the end users, which are these police authorities, the relevant threat scenarios and how we could tackle them with innovative technologies. And we came across two main challenging scenarios. One is what we call auto piloted drone swarm terrorist attack at a major sporting event. Major sporting events are a key concern for police authorities. Let us imagine that we have a marathon that is taking place with more than 35,000 people attending. After the event begins, a swarm of consumer drones flying at a very high speed and very low altitude enter the marathon carrying explosive and toxic agents. How can we address this? This is a question that we will address in the project.

The second scenario is called orchestrated weapons delivery during, for example, a Christmas concert. So again, celebrations like this are a key concern for the police authorities. And in this case, let us imagine that we have a major concert that is taking place in an open area that could be close to critical infrastructure such as a train station. Imagine there are authorized drones flying in the area that are used to cover the event for the media. On the day of the concert a security officer sees a swarm of flying drones delivering weapons and drops a container on the rooftop of a shopping center, bypassing all security controls. These drones are delivering weapons to terrorist actors on the rooftop. What can we do in these kinds of situations to counter or to prevent the delivery of these weapons?

BL: We touched on compliance

earlier. We can look at that a little bit more, the compliance issue with the EU and national regulations. How is this shaping your design decisions?

EV: This is a very important aspect from many viewpoints. We need to comply with the applicable regulation at both EU and national level. But there is a lack of regulation in many areas when we speak about counter-UAS. So, this is taken into the project in a very comprehensive compliance framework that is under development. At an EU level, we need to consider EASA drone regulation, the NIS2 directive on cyber security, GDPR of course, and the AI Act to ensure that all relevant touch points are addressed. There is also legislation at national levels that require factoring in. So, we are studying this, we are trying to understand the most relevant constraints and taking them into account as technological requirements that will drive our prototyping phase.

A first iteration of these requirements will be finalized this year. There is no EU-wide counter-UAS regulation. There is nothing like this in Europe and this brings the possibility to support policy makers in adapting future regulation or future regulatory frameworks to the needs we identified together with the police authorities. This is one of the core activities of our project, and we are in touch with policy makers at the European Commission to discuss input.

BL: How is the PRESERVE project engaging with police authorities, stakeholders, and end users? What is the engagement policy?

EV: The tool for this is the stakeholder group, which is an opportunity to take part in our activities. It includes, as you said, police authorities, but also citizens, civil aviation authorities, international organizations, technology providers, policy makers, and the scientific community. So, it touches on all areas and all the stakeholders that are relevant to our project.

We are in touch with other EU projects on counter-UAS, and on the development of AI technologies for the security of citizens. During the first year of our project (we are now at month 11) we have already reached eight members confirmed of the stakeholder group, which is an outstanding milestone for us.

The next step for us in terms of activities with this stakeholder group is to launch some webinars and some clustering activities to keep them in the loop and informed about what we are doing. And they can also provide suggestions and recommendations. In fact, we are planning during the whole project four clustering workshops both online and physically. These workshops are intended to bring together stakeholders to discuss and exchange ideas, enhance the project's technical developments, and increase the profile of our project in the scientific community. These clustering workshops are also aimed to attract policy makers and the standardization community to help formulate policy recommendations to the commission and contribute to standardization efforts.

We are also planning pilot demonstrations, which will take place end of 2026, and at the beginning of 2027 in Spain and Greece. We will invite our stakeholders to attend these events and to experience firsthand what we are doing and the results of our project.

If you are interested in what we are doing at PRESERVE, visit our website at https://preserve-he.eu/ and register for the stakeholder group so that we can stay in touch and inform you of upcoming activities.

BL: Thank you and we look forward to seeing you again soon.

EV: Thank you very much.

ENISA Publishes Latest Threat Landscape Report

The 2025 ENISA Threat Landscape shows that threat groups are reusing tools and techniques, introducing new attack models, exploiting vulnerabilities and collaborating to target the security and resilience of the EU's digital infrastructure.

Through a more threat-centric approach and further contextual analysis, this latest edition of the ENISA Threat Landscape analyses 4875 incidents over a period spanning from 1 July 2024 to 30 June 2025. At its core, this report provides an overview of the most prominent cybersecurity threats and trends the EU faces in the current cyber threat ecosystem.

ENISA Threat Landscape 2025 Highlights

- Incident type: DDoS attacks was the dominant incident type and accounted for 77% of reported incidents, the greater part of which were deployed by hacktivists while cybercriminals represent only a minor portion.
- Ransomware is identified as the most impactful threat in the EU.
- Hacktivism took the lead, representing almost 80% of the total number of incidents, primarily through low-impact DDoS campaigns targeting EU Member States organisations' websites, with only 2% of hacktivism incidents resulting in service disruption.
- State-aligned threat groups steadily intensified their operations towards EU organisations. State-nexus actors carried out cyberespionage against the public administration sector, while EU audiences were faced with Foreign Information Manipulation and Interference (FIMI).
- Phishing (60%), followed by vulnerability exploitation (21.3%) are the two leading intrusion access points.
- With regards to the assessed objectives of these incidents, almost 80% were ideology-driven incidents, exclusively carried out by hacktivists through DDoS.

Deep-dive into Key Trends

Based on the updated ENISA Cybersecurity Threat Landscape Methodology and a new format, the findings include updated key trends. With regards to the primary method for initial intrusion, phishing (including vishing, malspam and malvertising) is identified as the leading vector, accounting for about 60% of observed cases. Advancements in its deployment, such as Phishing-as-a-Service (PhaaS) that allows the distribution of ready-made phishing kits, indicate an automation that paves the way for attackers regardless of their experience.

Closely linked to recent events in the EU, an increase in targeting cyber dependencies has been noted. Cybercriminals have intensified their efforts to abuse critical dependency points, for example in the digital supply chain, to get the most out of their attacks. This method is able to magnify the impact of actions by leveraging the interconnectedness inherent in our digital ecosystems.

What also stands out is convergence between threat groups and the current overlap in their Tactics, Techniques and Procedures (TTPs), targets, objectives, etc. This is best demonstrated by faketivism, where intrusions by state-aligned actors employ hacktivist characteristics, as well as with similarities in tools utilised by both hacktivists' groups and cybercriminals.

The growing role of AI has become an undeniable key trend of the rapidly evolving threat landscape. The report highlights AI use both as an optimisation tool for malicious activities but also as a new point of exposure. Large Language Models (LLMs) are being used to enhance phishing and automate social engineering activities. By early 2025, AI-supported phishing campaigns reportedly represented more than 80 percent of observed social engineering activity worldwide. Attacks on the AI supply chain are on the rise. While the focus of threat activities involving AI was the use of consumer-grade AI tools to enhance their existing operations, the emergent malicious AI systems is raising concerns about their capabilities in the future due to the widespread use of AI models.

Last but not least, a higher volume of attacks toward mobile devices has been noted, with a focus on compromising outdated devices.

Top targeted sectors in the EU

The sectorial threat analysis of the report is significant to highlight structural target points of the EU's critical infrastructure. At the top of the targeted sectors list in the EU is public administration (38.2%), being the focus of hacktivism and state-nexus intrusion sets conducting cyberespionage campaigns on diplomatic and governmental entities.

At the second place is the transport sector (7.5%), followed by digital infrastructure and services (4.8%), finance (4.5%) and manufacturing (2.9%). The close match between the sectors with the highest ranking and the sectors under scope for NIS2 Directive underscores the importance of the Directive. 53.7% of the total number of incidents concern essential entities, as defined by the NIS 2 Directive.

Three of the top-five targeted sectors have consistently stayed in the top ranks for two consecutive years, whereas public administration has seen a notable rise in incidents this year, driven by the increased hacktivists' DDoS attacks.

Helping OT Organizations to Establish Defensible Architecture and More Resilient Operations

Developed Through JCDC, CISA's "Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators" is a Strategic Enabler for Cyber Defense Operations

In today's increasingly interconnected industrial landscape, operational technology (OT) systems are no longer isolated islands of automation—they're deeply entwined with information technology and business networks, making them prime targets for cyber threats. Recognizing this growing risk, the Cybersecurity and Infrastructure Security Agency (CISA) collaborated with three U.S. federal agencies and five international partners and received contributions from twelve private sector stakeholders to develop and publish, "Foundations for OT Cybersecurity: Asset Inventory Guidance for Owners and Operators". This key resource helps owners and operators of OT systems create stronger, more secure infrastructures by building a clear inventory and classification of their assets. By identifying, organizing, and managing OT assets effectively, organizations can not only improve cybersecurity but also enhance operational reliability, safety, and resilience.

Created by Operators, for Operators

Through the Joint Cyber Defense Collaborative (JCDC), CISA collaborated closely with critical infrastructure owners, operators and other stakeholders to identify systemic gaps and critical needs across the evolving cyber threat landscape, and work hand-in-hand to co-develop effective and impactful solutions. The technical insights and real-world experiences of professionals that manage OT environments daily are reflected in this guide, both the operational realities and strategic foresight.

In eight focused working sessions, industry contributors played a central role in shaping the content, offering insights that are both practical and field-tested. Separate from these sessions, CISA coordinated technical reviews from industry, federal, and international stakeholders across multiple sectors to ensure the guidance is relevant and applicable. The result is a robust framework for building foundational asset inventories and taxonomies that are actionable and resilient.

What is an OT Asset Inventory?

An OT asset inventory is a dynamic list, containing an updated map of the devices, systems, and software that make up the operational backbone of critical environments. From industrial control systems to sensors, Human-Machine Interface (HMIs), servers, and specialized applications, every component plays a role in the broader ecosystem. Without visibility into these assets, organizations are effectively operating without a full view of their potential vulnerabilities.

When implemented effectively, an asset inventory becomes more than a record; it's a strategic tool. It helps organizations uncover interdependencies across their environment, assess risk, segment networks to limit or eliminate lateral movement, and strengthen overall resilience. Achieving that level of control is possible for operators nationwide, but it demands a disciplined, consistent approach to managing one's environment. This guide helps organizations establish and maintain the appropriate discipline and consistency.

Why is This So Important Now?

In recent years, cyber incidents targeting OT environments have demonstrated just how damaging a lack of asset visibility can be. Attackers often exploit forgotten devices, outdated firmware, or weakly segmented networks to establish initial access, then move laterally across interconnected systems, compromising critical assets and disrupting core operations.

An accurate and regularly maintained asset inventory closes those gaps by ensuring each component is known, categorized, assigned criticality, and protected according to its risk profile. While each operator should strive to collect every asset in

their environment, start by prioritizing assets based on criticality and evolve the list continuously until a complete record is captured.

Moreover, an OT asset inventory is foundational for alignment with industry standards. Whether it's NIST, IEC 62443, or sector-specific frameworks, most cybersecurity best practices begin with "know what you have." Without this initial step, everything else—from vulnerability management to incident response—lack the necessary visibility and structure to be effective.

From Inventory to Action

The real value of an OT asset inventory comes when it is integrated into daily operations. With an asset inventory, operators can:

- Prioritize vulnerabilities based on criticality and exposure.
- Detect unauthorized devices before they become attack vectors.
- Support network segmentation efforts by mapping communication flows.
- Enable incident response teams to act quickly and accurately.

Building Towards the Vision

Having a complete and accurate OT asset inventory is the essential first step toward building a defensible architecture and more resilient operations. CISA's guidance makes that complex process clear and achievable, empowering organizations to take decisive action.

More than just a technical manual, this guidance serves as a strategic enabler for cyber defense actions and operational collaboration with CISA and other key stakeholders. With a precise understanding of the assets within an operator's infrastructure, Common Vulnerabilities and Exposures (CVEs) added to CISA's Known Exploited Vulnerabilities Catalog or to stakeholder notifications and threat advisories become significantly more actionable and timely—helping operators reduce risk proactively, before incidents escalate.

To support this effort, CISA offers tools and resources, including MALCOLM for network traffic analysis, no-cost Cyber Hygiene vulnerability scanning, Cyber Security Evaluation Tool (CSET) and cross-agency support to help validate and manage asset data. Additionally, CISA provides support through regional Protective Security Advisors (PSAs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), and Chemical Security Inspectors (CSIs). Visit CISA Regions webpage to contact this personnel support nearest to your location.

By Clayton Romans, Associate Director for Joint Cyber Defense Collaborative

CISA Announces Steve Casapulla as Executive Assistant Director for Infrastructure Security

The Cybersecurity and Infrastructure Security Agency (CISA) announced the appointment of Stephen L. Casapulla as the Executive Assistant Director for Infrastructure Security.

Prior to joining CISA, Casapulla served as the Director for Critical Infrastructure Cybersecurity in the Office of the National Cyber Director. He previously spent over thirteen years at CISA and its predecessor, holding a variety of senior roles. His prior federal service includes work at the Small Business Administration and at the Department of State in Iraq. He also serves as an officer in the U.S. Navy Reserve, with over twenty years of service and multiple overseas deployments.

"I'm honored to take on this critical role at CISA and deeply appreciate the trust placed in me by President Trump and Secretary Noem," said Casapulla. "I am committed to advancing CISA's mission and ensuring the security and resilience of our nation's critical infrastructure and the American people."

In addition to his Infrastructure Security Division role, Casapulla will continue to serve as the Interim Assistant Director for the CISA's National Risk Management Center (NRMC) and as its Acting Chief Strategy Officer.

Enhancing the response to IP crime through global cooperation and innovative training

Illicit medicines, defective electronics and other fake goods are flooding global markets, endangering lives, damaging economies and undermining security worldwide.

From food and fashion to construction materials and lithium-ion batteries, counterfeiters have now expanded to virtually every product category, while copyright pirates have built lucrative networks to distribute unauthorized books, music and software.

These intellectual property (IP) crimes are often considered by the public as low-harm offences. For law enforcement and industry experts, however, the reality is stark: IP crime is a growing threat to public health, safety and security.

In response to this global issue, 450 participants from some 70 countries and 230 cross sector organizations gathered at the 2025 International Law Enforcement IP Crime Conference under the theme "Working in Partnership to Advance Safety and Security".

The annual conference, co-hosted by INTERPOL and UL Standards & Engagement (ULSE), was delivered by the INTERPOL Global

Academy through its International IP Crime Investigators College (IIPCIC). It brought together senior law enforcement officials, industry leaders, academia and experts in IP crime to exchange best practices, share research, discuss emerging safety challenges, strengthen cooperation and partnerships, and promote capacity building and training initiatives.

In his opening remarks INTERPOL Secretary General Valdecy Urquiza emphasized the critical link between IP crime and organized crime, underscoring the need for a comprehensive approach to dismantling the criminal networks driving these offences.

"IP crime poses profound threats, not only to industries but also to individuals and governments.

It undermines innovation, creativity, and erodes public trust. By building capacity, by strengthening networks and by sharing knowledge and expertise, we secure one essential result: operational readiness. The readiness to anticipate, to investigate and to counter malicious networks."

In his keynote address, World Customs Organization Secretary General Ian Saunders said:

"Only by working together can we enhance intelligence sharing, build capacities, and prevent counterfeit and dangerous goods from moving through the global trade ecosystem."

Other speakers at the conference expanded on the link between the low-risk, high-reward model of counterfeiting and piracy and a broad spectrum of other serious crimes, illustrating its scale with examples ranging from corruption to human trafficking.

Addressing how to confront these challenges, ULSE President and CEO Jeff Marootian highlighted the role of training and partnerships in strengthening the global response, stating:

"Through the International IP Crime Investigators College, UL Standards and Engagement and INTERPOL use state-of-the-art practices to ensure enforcement partners have access to the latest tools and training methods to keep dangerous goods off the market. No country, agency, or organization can face these challenges alone."

The conference also showcased pioneering approaches to strengthening law enforcement capacity against IP crime. Immersive learning virtual reality training workshops run by the IIPCIC took participants from an INTERPOL classroom into simulated operational environments, where officers practiced handling counterfeit goods and fraudulent documents.

eu-LISA Joins Maintenance Effort for Biometric Open-Source Face Image Quality Tool (OFIQ)

eu-LISA has taken on maintenance responsibilities for the Open-Source Face Image Quality (OFIQ) tool, supporting the continued development of a critical biometric standardisation project.

Since August 2024, eu-LISA's Research and Innovation (R&I) team has been contributing to OFIQ's maintenance, supporting the German Federal Office for Information Security (BSI), which leads the project.

The OFIQ development project was launched in 2020 within the ISO Sub-Committee 37 (ISO SC37 for the standardisation of

biometric technology), and its current release serves as the reference implementation for the ISO/IEC 29794-5:2025 standard on face image quality (approved and published in May 2025). The tool addresses a fundamental challenge in large-scale biometric systems – ensuring facial images meet the quality level required for reliable recognition accuracy.

For eu-LISA, OFIQ's importance stems from the key role that it can play in the future in assessing the correct quality level of the face data stored in the different Core Business Systems (CBS) managed by the Agency, as well as ensuring compliance with EU regulations, including the EU Commission Implementing Decision (EU) 2019/329 for the Entry/Exit System, which requires that the quality of facial images complies with the guidelines currently provided for frontal image types in the ISO/IEC 29794-5:2025 standard.

TSA checkpoint with state-of-the-art technology fully opens inside Southwest Wyoming Regional Airport's new terminal

The Transportation Security Administration (TSA) checkpoint at Southwest Wyoming Regional Airport's new terminal is ready for full operations with state-of-the-art technology that enhances the passenger experience. Featuring Advanced Imaging Technology (AIT) and a computed tomography (CT) unit, the checkpoint offers passengers a more convenient way to go through the security screening process before boarding their flight.

"The use of AIT and CT at the new terminal's checkpoint is an enhancement of TSA's ongoing efforts to improve the passenger experience while improving security operations," said Jamie K. Hicks, TSA Federal Security Director for Wyoming. "We have worked closely with the airport on the design of the security checkpoint to ensure it provides an ideal environment for TSA officers to carry out their important role in airport operations, and AIT and CT technology will make a positive impact in our checkpoint."

Advanced Imaging Technology (AIT) units safely and without physical contact screens travelers for both metallic and non-metallic threats, including weapons, explosives and other objects that may be concealed under layers of clothing. The technology uses millimeter wave technology, which is safe and meets national health and safety standards.

The AIT uses automated target recognition software that eliminates passenger-specific images and instead auto-detects potential threats by indicating their location on a generic cookie-cutter outline of a person. The generic outline is identical for all passengers. The unit streamlines the checkpoint screening process and significantly reduces the frequence of full-body pat downs.

AI standards exchange database

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

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

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

Translate, structure, include, connect

"Standards development organizations ultimately translate principles into practical implementation," said IEC Secretary-General and CEO Philippe Metzger.

"We have a real need of translating that in the field of AI into actual governance."

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

Metzger emphasized the importance of inclusive standards processes, building standards capacity around the world, and strongld Standards Cooperation.

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

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

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

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

New resources

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

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

OSCE Guide Encourages Enhanced Cyber Physical Defences for CI

The Organization for Security and Cooperation in Europe has issued new physical security guidance to help governments, owners, and operators strengthen the protection of critical infrastructure. Though the Technical Guide focuses on the physical security threats, it encourages policymakers, critical infrastructure owners/operators, and other stakeholders to strengthen collaboration with their cybersecurity counterparts. Participating States and critical infrastructure owners/operators may find value in breaking down silos between these communities and working towards a comprehensive approach to risk management at the facility, organizational, and sector levels.

The OSCE emphasizes that physical security should be integrated with personnel, procedural, and cybersecurity measures to form a cohesive and sustainable security framework for each facility. The Technical Guide outlines key practices, principles, and considerations to improve the physical security of permanent critical infrastructure sites and facilities, focusing on preventing, preparing for, and mitigating potential terrorist attacks.

While this 220-page Technical Guide does not address the cybersecurity challenge directly, as critical infrastructure owners/operators adopt more emerging technologies to facilitate their operations, both physical and cyber risk management will become increasingly complex. In many cases, OSCE participating States and security managers tasked with CIP approach critical infrastructure security holistically, meaning their policies and practices account for and address both physical and cyber risks. Although the Technical Guide focuses on the physical security aspects of critical infrastructure, this provides an opportunity to illustrate the importance and value of a holistic approach to security and resilience.

CNPIC, The Future CNPREC, Will Be The Central Axis In The Protection And Resilience Of Critical Entities

The National Centre for the Protection of Critical Infrastructures (CNPIC) is playing a major role in the implementation of the new Law on the Protection and Resilience of Critical Entities (CER), approved by the Council of Ministers at the proposal of the Ministry of the Interior.

This regulation will incorporate the most recent European directive into the Spanish legal system, reinforcing the safeguarding of entities essential to the social and economic functioning of the country.

New competencies and framework for action

The CNPIC, under the authority of the Secretary of State for Security, becomes the National Centre for the Protection and Resilience of Critical Entities (CNPREC). This new name reflects its expanded mission as a national reference point and single point of contact for cross-border cooperation in the European Union.

The law aims to guarantee the continuity of essential services provided by critical entities in strategic sectors such as energy, transport, health, water, public administration, food production and distribution, the nuclear industry, research facilities and private security, among others.

Actions and responsibilities

The draft establishes a planning system structured around the National Strategy for the Protection and Resilience of Critical Entities and the National Threat and Risk Assessment, both prepared and approved by the Secretary of State for Security.

Critical entities must draw up resilience plans, designate a security and resilience officer as a point of contact with the CNPREC, and report any incident that may affect the provision of essential services. Likewise, the National Commission for the Protection and Resilience of Critical Entities and the Interdepartmental Working Group are created, collegiate bodies attached to the Secretary of State for Security, responsible for approving sectoral strategic plans and collaborating in the identification of critical entities.

Scope of application

As stated in the draft law, the regulation will be applicable to all critical entities located in the national territory, except those belonging to the banking sector, financial markets and digital infrastructures, which are expressly excluded in those aspects already regulated by specific sectoral regulations, such as the DORA Regulation or the NIS2 Directive.

The exact scope of this exclusion and its fit with current regulations is currently in the regulatory analysis and development phase. Therefore, it is being studied how the exclusion will finally be applied to specific entities in the digital sector and whether it will affect all their activities or only those already covered by other specific regulations.

Urgent processing

The Council of Ministers has agreed to the urgent processing of the draft bill, which implies the reduction by half of the deadlines for the issuance of reports by the departments involved.

CNPIC Commitment

The CNPIC reinforces its commitment to the protection and resilience of critical entities, guaranteeing the security and continuity of essential services for Spanish society. The centre will closely monitor regulatory developments and actively collaborate in the clarification and practical articulation of the regulation, ensuring the most appropriate legal framework for the protection of the country's essential infrastructures.

ESET joins Europol's Cyber Intelligence Extension Programme (CIEP)

ESET, Europe's leading global cybersecurity company, announced its participation in the pilot phase of the Cyber Intelligence Extension Program (CIEP), a new initiative launched by Europol's European Cybercrime Centre (EC3).

The program aims to strengthen public-private cooperation in the fight against cybercrime by enabling real-time collaboration and intelligence sharing. As part of this initiative, ESET Chief Research Officer Roman Kováč, and Senior Malware Researcher Jakub Souček, recently spent several days at Europol headquarters in The Hague meeting EC3 teams and exploring ways in which ESET's threat intelligence can directly support investigations into ransomware operations, payment fraud schemes, or complex cybercrime infrastructure.

Europol functions as a people hub, a data hub, and a case hub, a place where collaboration, intelligence, and operations converge. ESET's team met with law enforcement officers from multiple countries, experiencing firsthand how one central platform fosters effective cross-border cooperation.

"We believe the CIEP sets a new benchmark for actionable intelligence sharing, joint operational readiness, and collective impact," says Roman Kováč, Chief Research Officer at ESET.

The new CIEP initiative elevates this collaboration further, creating opportunities for direct, real-time engagement with Europol's operational teams. Public-private partnerships like this one are crucial in mitigating risks within today's rapidly evolving cyber threat landscape. ESET has a long history of collaboration with global law enforcement agencies, including in EC3's Advisory Group.

Spirent Brings Industry-First Benchmarking to Cloud-Native Infrastructure Testing

Spirent Communications, a leading provider of test and assurance solutions for next-generation devices and networks, today announced the introduction of benchmarking capabilities to the award-winning Landslide Test Solution.

Cloud-Native Infrastructure Benchmarking further expands the unique capabilities of Spirent Landslide to help service providers accelerate roll-out of cloud-native 5G standalone (SA) networks.

The first comprehensive solution for benchmarking, deploying, managing, and optimizing 5G infrastructure performance to ensure networks are ready and capable of supporting 5G CNFs, Landslide will enable service providers to benchmark the infrastructure itself, including CPU, memory, storage, and networking, which is foundational for CNF scalability and resiliency testing. Critical to accelerating 5G SA and 5G-Advanced adoption, the capacity to validate infrastructure readiness before CNF deployment will reduce the risk of degraded quality of service, outages, wasted investments, and delayed service launches.

"Cloud-native complexity has slowed down the pace of 5G SA adoption because operators need confidence that their infrastructure can reliably support CNF workloads," said Anil Kollipara, VP of Automated Test & Assurance Product Management at Spirent. "With this latest Landslide release, Spirent is delivering the most complete lifecycle solution that benchmarks, validates, and optimizes cloud-native infrastructures. We are helping operators bridge organizational gaps, reduce risk, and deliver the high-quality services their customers demand.

Landslide Cloud Infrastructure Benchmarking addresses the organizational and operational realities of cloud-native transformation.

Eviden awarded by NATO the modernization of communications for the Spanish Air and Space Force

Eviden, the Atos Group product brand leading in advanced computing, cybersecurity products, mission-critical systems, and Vision AI, announces that it has been selected by the NATO Support and Procurement Agency (NSPA) to modernize the ground-to-air-to-ground (G/A/G) communication systems of the Spanish Air and Space Force.

The €12 million contract includes the supply, installation, and maintenance of next-generation communication systems that will enhance operations at Air Traffic Control (ATC) towers across various air bases, Air Force airfields, and Air Surveillance Squadron (EVA) bases of the Spanish Air and Space Force (SASF).

The project, scheduled for completion within a maximum of 18 months, will involve the deployment of several hundred civilian and military radio systems at 35 locations across Spanish territory, providing comprehensive coverage of the mainland, islands, and the autonomous cities of Ceuta and Melilla.

The communications modernization encompasses a variety of radio and ground-to-air-to-ground (G/A/G) equipment, including transmitters, receivers, and transceivers operating in VHF and UHF bands, as well as multiband VHF/UHF radio transceiver systems. The contract also includes management software, recording systems, real-time systems, user training, and full system documentation.

The new communication systems are classified as mission-critical and will be in continuous operation, 24/7, 365 days a year.

D-Fend Solutions Launches EnforceAir PLUS, a Cyber-Driven, Multilayer, AI-Enhanced Counter-Drone System with Integrated RF-Cyber, Radar, and Jammer

D-Fend Solutions, the leader in field-proven radio frequency (RF) cyber-driven, non-kinetic, counter-drone takeover technology, launched EnforceAir PLUS, a transformational new offering for counter-drone defense.

EnforceAir PLUS is a cyber-driven, multilayer, AI-enhanced counter-drone system comprised of foundational RF-cyber detection and takeover technology, now integrated with auto-calibrated radar detection and optional jamming mitigation. EnforceAir Plus optimizes all three technologies to deliver unparalleled detection and mitigation, with operational ease of use for unmatched protection and safety. These counter-unmanned aerial system (C-UAS) technologies are combined in a compact system for holistic and escalating air defense, reinforcing the company's core commitment to overcome current and emerging drone threats.

Because the cyber, radar, and jamming functions are already fully integrated and calibrated, EnforceAir PLUS enables users to quickly respond to drone incidents with a more comprehensive range of options. The system's "SmartAir" technology fusion engine consolidates cyber and radar data to provide unified situational awareness and a clear and simplified operational picture of each target drone, contributing to more informed and tailored mitigation actions, based on real-time insights and artificial intelligence.

The system's optimized radar detection, featuring a compact multi-panel solid-state radar such as those from leading providers like Echodyne, extends threat coverage beyond cyber measures while minimizing false positives and enhancing airspace accuracy.

Milestone's XProtect and Arcules Enhance Cloud Integration and Operational Intelligence

Milestone Systems announced the latest updates in XProtect 2025 R3 and the Arcules platform, delivering new capabilities that accelerate investigations, strengthen security operations, and simplify system management.

The latest releases for XProtect VMS and Arcules VSaaS address the real-world challenges facing security professionals by making surveillance systems more intelligent, accessible, and easier to manage while maintaining the open-platform flexibility that has made Milestone a trusted partner worldwide.

XProtect Remote Manager introduces new comprehensive monitoring and management capabilities that enable security teams to maintain system health and respond to issues before they impact operations, eliminating time-consuming site visits.

Remote management, along with improved monitoring of recording servers, allows administrators to detect and resolve critical issues, such as full databases or server health problems, without local access. Event-based notifications keep teams informed through customized email alerts when cameras, servers, or other components experience status changes, supporting faster response times across cameras, recording servers, hosts, sites, services, devices, and camera components.

Video permissions control provides granular management of video feed visibility, allowing site owners to define precisely who can view specific cameras to minimize the risk of unauthorized access risks.

Another key feature is the new Role-based Access Control Permissions for access control systems, which allows administrators to restrict the visibility and operation of access control units based on user roles directly within XProtect.

Echodyne Launches EchoWare to Simplify Advanced Radar Integration

Echodyne is pleased to announce the launch of its next-generation software platform, EchoWare, to enable partners and customers to swiftly integrate and deliver advanced radar capabilities into their systems and solutions.

With quickly maturing requirements for precise situational awareness data across markets and applications, from defense and security to drone as first responder (DFR) and a robust drone delivery infrastructure, EchoWare enables customers and integrators to quickly deploy and consistently deliver advanced radar capabilities across fixed, portable, temporary, and on-the-move (OTM) modalities.

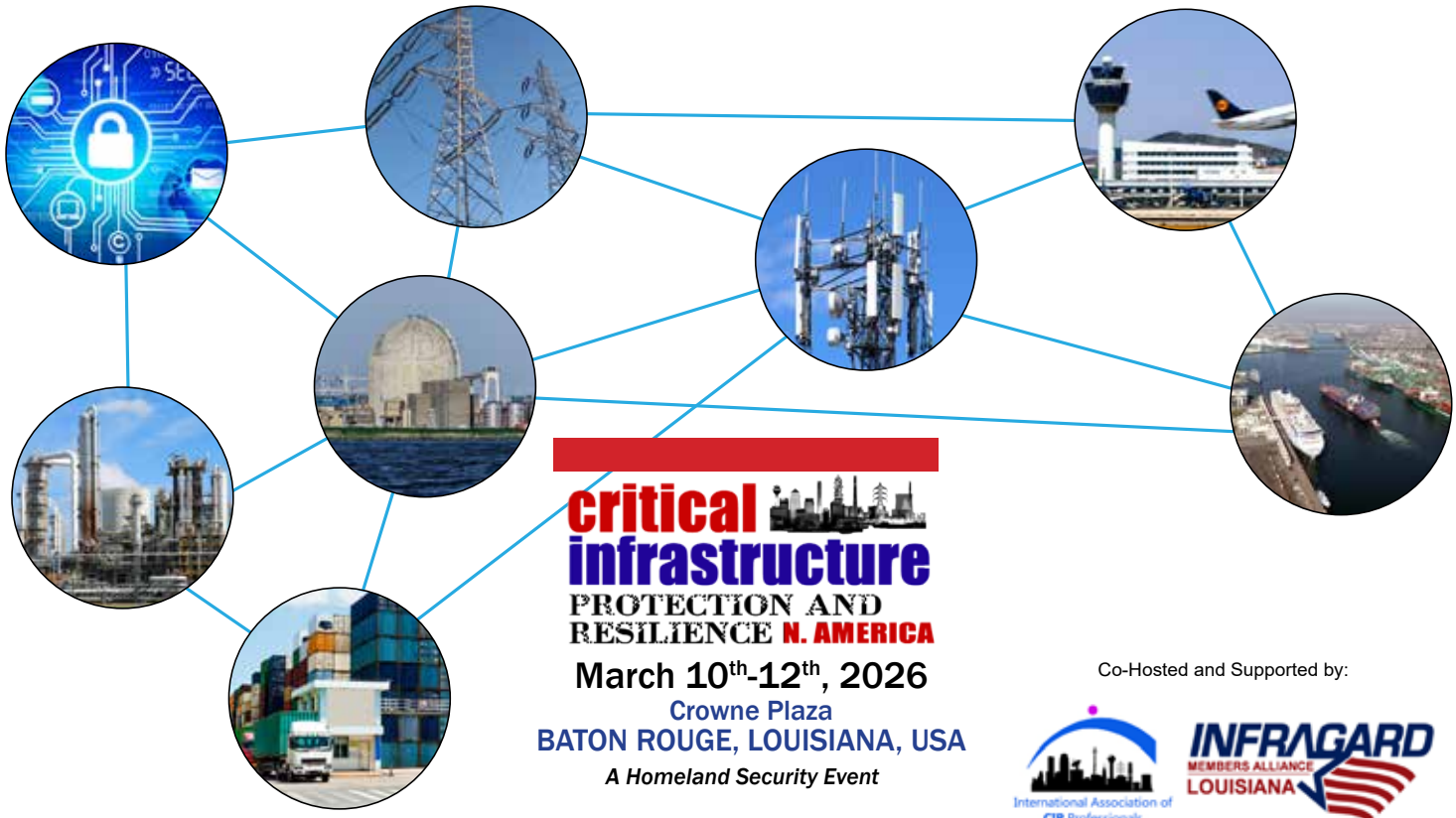
EchoWare is a robust software platform that acts as middleware between Echodyne radars and system Command and Control (C2) and solution platforms, delivering a single high fidelity data interface for Echodyne's advanced cognitive radar capabilities. EchoWare combines configuration, deployment, and lifecycle management of individual radars into a single interface, allowing for seamless control and monitoring of deployed radar systems. The most requested feature across all markets is Single Track ID, which maintains a single data identity across all radars in the system.

"Radar is the foundation sensor, the building block upon which every great system and solution is delivered," said Dr. Tom Driscoll, CTO of Echodyne. "When the building blocks are zeros and ones, MESA radars deliver more accurate and precise data than conventional ESA radars. EchoWare is the connective tissue for networks of radar systems delivering advanced cognitive radar capabilities to global markets."

ADVERTISING SALES

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

Paul Gloc
Rest of World
E: paulg@torchmarketing.co.uk
T: +44 (0) 7786 270820



critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 10th-12th, 2026

Crowne Plaza
BATON ROUGE, LOUISIANA, USA

A Homeland Security Event

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

REGISTER ONLINE TODAY

Securing the Inter-Connected Society

Early Bird deadline - February 10th, 2026

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

The 8th Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

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

If you are responsible or involved in your planning and preparatoin for securing and protecting your critical assets and entities then join us for the next gathering of operators, government establishments and industry tasked with the region's Critical Infrastructure Protection and Resilience.

For further details and to register visit **www.ciprna-expo.com**

CONFIRMED SPEAKERS INCLUDE:

Keynote: Brian Harrell,Former Assistant Secretary for Infrastructure Protection, DHS

Anuj Kumar, Senior Security Architect, Nokia

Benjamin Lampe, Engineer, Idaho National Laboratory

Anthony Adebonojo, Chairman, CCIPR-WG, International Council of Systems Engineers (INCOSE)

Joshua Tannehill, Information Systems Security Officer | VP Louisiana Chapter, Knight Federal Solutions | InfraGard

Josie Ross, Emergency Management Officer, City of Henderson Department of Emergency Management

Joseph Threat, Chief Resilience Officer and Chief Administrative Officer, City of New Orleans

Andrea Davis, President and CEO, The Resiliency Initiative

Michael Lambert, Emergency Preparedness/Homeland Security Planner, Houston-Galveston Area Council of Governments

See **www.ciprna-expo.com** for more.

The premier discussion for securing America's critical infrastructure

Owned & Organised by:

TORCH

Supporting Organisations:

INFRAGARD HOUSTON
AUTO-ISAC
THE RESILIENCY INITIATIVE
STIMEF
Help2Protect
CAMO
IACI
ISIO
NS&RC

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS