critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

AUTUMN 2023
www.cip-association.org

FEATURE:
Enhancing transport safety and resilience: trends, challenges and innovations

FEATURE:
Critical Infrastructure: Commission proposes a Blueprint to improve response to disruptive cross-border incidents

FEATURE:
The Power of Iris Recognition for Securing Critical Infrastructure Spaces

CRITICAL ENTITIES RESILIENCE
FAILURE INDICATION

Co-Hosted and Supported by:

International Association of CIP Professionals

INFRAGARD MEMBERS ALLIANCE LOUISIANA

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 12th-14th, 2024

LAKE CHARLES, LOUISIANA

A Homeland Security Event

Collaborating and Cooperating for Greater Security

For Securing Critical Infrastructure and Safer Cities

Register Today

SPECIAL DEAL FOR INFRAGARD LA MEMBERS, GOVERNMENT AND OWNER/OPERATORS

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

The latest Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from operator/owners, agencies, governments and industry to debate and collaborate on securing America's critical infrastructure.

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

Agenda includes Industry Sector Mini Symposiums to focus on your specific CI sector, with the enhanced opportunity to discover and share experiences across these sectors:

- Power & Energy (Grid Resilience) Sector Symposium
- Transport Sector Symposium
- Communications Sector Symposium
- Pipelines Sector Symposium
- Critical Industries Sector Symposium
- CIIP / Cybersecurity Sector Symposium

Join us in Lake Charles, LA, USA for the premier event for operator/owners and government establishments tasked with the region's Critical Infrastructure Protection and Resilience.

Leading the debate for securing America's critical infrastructure

Opening Keynote:

- Dr David Mussington, Assistant Director, CISA

Confirmed speakers include:

- Budge Currier, Assistant Director Public Safety Communications, California Office of Emergency Services (Cal OES)
- Brian Harrell, Vice President and Chief Security Officer (CSO), Avangrid, USA
- Charles Burton, Technology Director, Calcasieu Parish, USA
- Lester Millet, Policy & Planning Director and Safety Risk Agency Manager, Port of South Louisiana & President, Infragard Louisiana
- Jeff Gaynor, President, American Resilience, USA
- Ron Martin, ICAM-Critical Infrastructure, Capitol Technology University, USA
- Tim Klett, Strategic Technology Integration Strategist, Idaho National Laboratory, USA
- Emilio Salabarria, Senior Program Manager for Cybersecurity, The Florida Center for Cybersecurity: Cyber Florida
- Chris Janson, Sr. Market advisor, Nokia, USA
- Rola Hairi, Defense Industrial Base Sector Liaison, Cybersecurity and Infrastructure Security Agency (CISA)
- Richard Tenney, Senior Advisor, Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA)
- Michael Finch, Technology Services Director, Lane County Department of Technology Services
- Jim Henderson, CEO, Insider Threat Defense Group, Inc., Founder / Chairman, National Insider Threat Special Interest Group

For speaker line-up visit www.ciprna-expo.com

REGISTER ONLINE AT www.ciprna-expo.com/registration

WE ARE LIVING IN CHALLENGING TIMES FOR CSO AND CISO'S

Now there's a phrase that seems to go in and out of trend - "We live in challenging times" - but perhaps is more pertinent today than for many years. The latest developments in the Middle East have increased global tensions, following the war in Ukraine, and provide security forces more to think about, as well as our politicians, to prevent further escalation.

All this of course, has its impact on threats to critical infrastructure, as geopolitics is now so intertwined with national and international economics, that heightening the rhetoric and threats against nation states and their allies has an impact on potential targets.

The power of "social" media also plays a huge role in developing threats, as spreading of information, and indeed dis-information (and propaganda), is so easy, speedy and appears with little recourse, that interpreting what may be real, and what is 'fake news' has also become a bigger challenge. When even the 'verifiers' appear to also, more than occasionally, get it wrong makes it a challenging time for everyone to know what is really going on.

So how can be best protect our critical infrastructures if we don't really know what is happening, or what to expect?

Indeed a big challenge for any CSO and CISO!

Collaboration and information sharing of intelligence is key to one's armoury.

The flow of intelligence, whether from government and intelligence/ security agencies to infrastructure operators, and just as importantly from infrastructure operators to security agcnies, becomes increasingly important if we are to understand the evolving threats and what measures should be in place to mitigate any impact of an attack - whether physical, cyber or cyber-physical.

How does a CSO/CISO best plan for an attack if they do not know what they should be planning against?

This failure to plan would inevitably have it's impact on other interdependent infrastructures - the cascading effect - as no infrastructure is now truly independent.

So let's improve the communication and information flow, up and down the chain, to help each other better prepare for what may seem the inevitable, and make a probability into a possibility - after all, once a plot has been foiled, the cycle will only start again.

Enjoy this issue of Critical Infrastructure Protection & Resilience News.

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.

Critical Entities Resilience Failure Indication

An exerpt from 'Critical Entities Resilience Failure Indication - Reference: SAFETY_106371' by David Rehak, Alena Splichalova, Martin Hromada, Heidi Janeckova and Josef Ristvej.

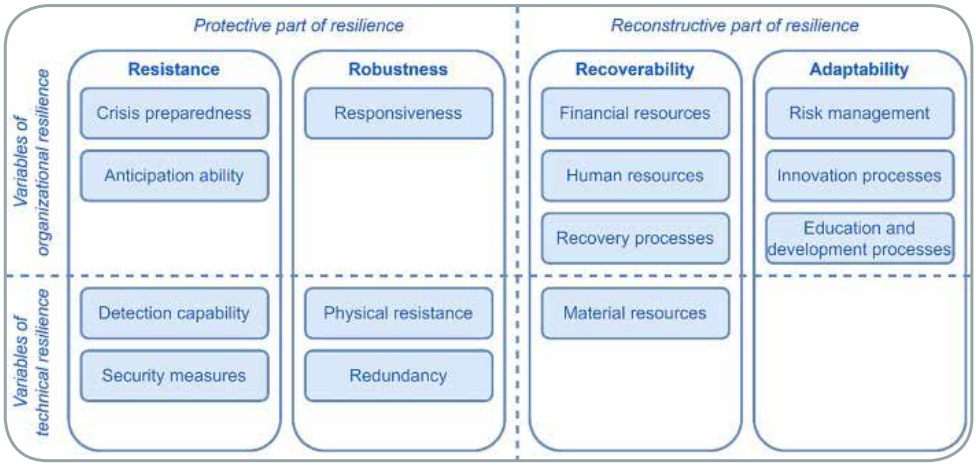
The adoption of the new Directive (EU) 2022/2557 on the resilience of critical entities has raised the question of how to assess the level of resilience of these entities in relation to current security threats. Until now, approaches have focused only on assessing the resilience of critical infrastructure elements. However, the new Directive exemplifies the need to pay attention not only to the element resilience, but also and more importantly to the resilience of their owners and operators, i.e., critical entities. Based on this fact, the authors of the article created a tool for Critical Entities Resilience Failure Indication (CERFI Tool). The essence of this tool is a probabilistic algorithm that predicts the relationship between the threat intensity and the protective part of critical entity resilience through indicators (to be created by the assessors themselves). The result of this prediction is an indication of the critical point of failure of the critical entity's resilience in phases of prevention and absorption of impacts. The CERFI Tool thus contributes to increasing the safety of technically oriented infrastructures, especially those of an energy and transport nature.

This is an exert of the paper that concludes with an example of the practical application of the developed tool on a selected critical entity in the energy sector.

Introduction

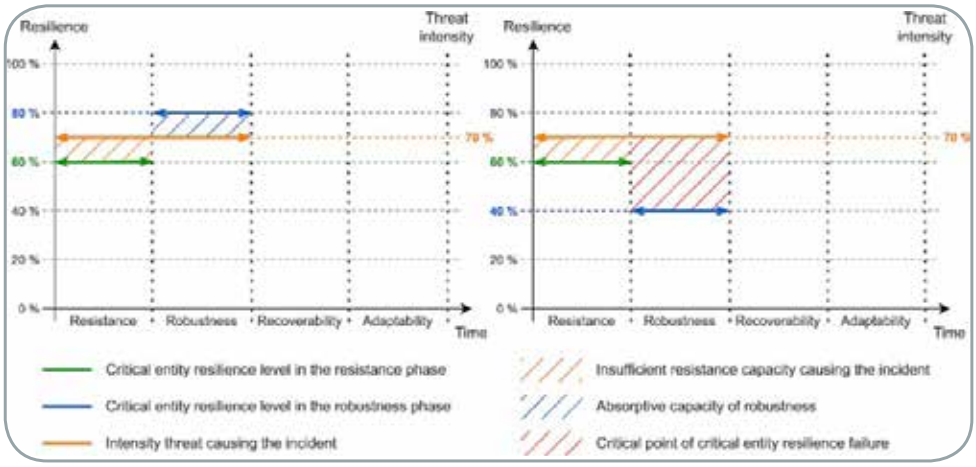
People living in large urban agglomerations are increasingly dependent on a reliable supply of essential services that are necessary to maintain vital social functions and economic activities, along with public health and safety services (Directive (EU), 2022). These essential services are provided through critical infrastructure (CI), which can be classified as technical and socio-economic. The most important technical CI systems have long included energy and transport (Council Directive, 2008). For example, the energy sector was identified as a uniquely critical sector in 2013 (The White House, 2023), as a failure of its services would cause cascading impacts on the provision of essential services of all other CI systems (Vichova and Hromada, 2019, Rehak et al., 2018a).

Owners or operators of CI systems are referred to as critical entities. The ability of these critical entities to prevent, respond to, withstand, mitigate, absorb, adapt to and recover from incidents is referred to as resilience (Directive (EU), 2022). This resilience can be perceived on two basic levels. The first level is technical resilience, which focuses on the physical protection of CI elements (NIAC, 2009, Kampova et al., 2020). The second level is organisational resilience, which is concerned with the managerial and procedural areas of critical entities (Asis, 2009, Rehak, 2020). However, the same determinant components can be identified for both types of resilience, which are resistance, robustness, recoverability and adaptability (Rehak et al., 2018b, Rehak et al., 2022a).



In the context of the timeline, resistance can be seen as the most important resilience component, whereby resistance is perceived as the ability of a critical entity to prevent an incident from occurring, whereas the essence of robustness is the absorption of the effects of an incident that has already occurred (Rehak et al., 2022a). The resilience of critical entities is currently determined by several important approaches. These include emergency preparedness (Philpott, 2016), risk management (ISO 31000, 2018), activities taken by an entity to define the hazard environment to which elements of the CI are exposed (Carlson et al., 2012), monitoring (Tracht et al., 2013) or a physical protection system (Kampova et al., 2020). All of these approaches have been successfully applied in practice, but their predictive potential in relation to an impending incident is very low. For this purpose, approaches based on the use of indicators in the context of CI resilience are clearly more appropriate (Rehak and Splichalova, 2022).

A number of methods and tools are currently used within the CI systems that use indicators to detect weaknesses, measure and assess resilience, or evaluate its security or vulnerability. The most prominent of these is a method in which individual questions asking about specific resilience-related issues are considered to be indicators (Øien et al., 2017). Through these questions, they try to define whether the system is sufficiently resilient. In contrast, static resilience assessment



INVITATION TO PARTICIPATE

Securing the Inter-Connected Society

Co-Hosted by:

International Association of CIP Professionals

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

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

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

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

Join us in Madrid, Spain for the the 9th 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

To discuss sponsorship opportunities contact:

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

Sam Most
(Rest of World)
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

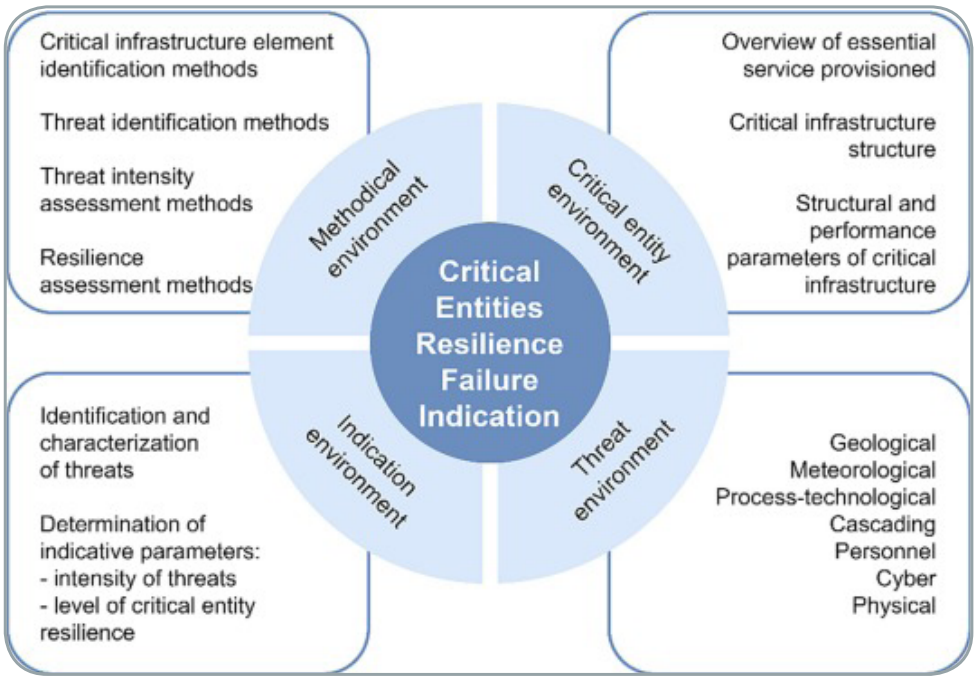
Jina Lawrence
(Rest of World)
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234 750

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

methods (Rehak et al., 2019, Nan and Sansavini, 2017, Kozine et al., 2018) use indicators to obtain information about the integrated level of resilience and also to model the failure behaviour of infrastructure systems. A different perspective is provided by holistic methods (Mazur et al., 2019, Fu et al., 2021), which identify indicators based on their benefits for enhancing resilience and stakeholder preferences. Another approach is to define indicators based on economic aspects, which are presented in a three-dimensional form, namely functionality, time and cost (Abbasnejadfard et al., 2022).

It is also common practice to use indices, which can then be considered as a specific type of indicator that is also able to identify significant shortcomings and weaknesses that can threaten the functionality of infrastructure systems. The Resilience Measurement Index can be considered as one of the most important indices, which is complementary to other indicators such as the Vulnerability Index (Collins et al., 2011), the Protective Measures Index, the Consequences Measurement Index (Petit et al., 2013), and the Total Resilience Index (Mottahedi et al., 2021).

Therefore, the essence of all the methods and tools presented above is the assessment of the static resilience/vulnerability level (i.e., the level at the time when the element is not exposed to any incident) in order to identify weak points of the assessed CI elements. Such an approach to CI protection has certainly been correct in recent years, but in the context of the new Directive (EU) (2022) it is necessary to shift the focus to critical entities. As a result of this change, it is now possible to view CI resilience in an integral way that links technical and organisational resilience into a single unit. In this context, it is also appropriate to redistribute indicators from the current CI elements to a new position located between threats and critical entities.

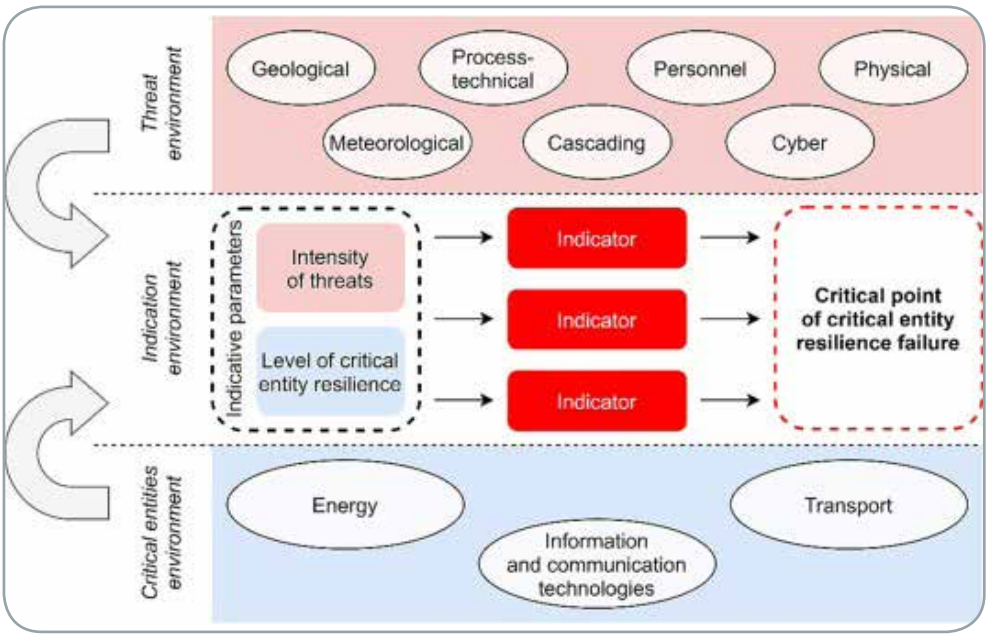


On the basis of these newly established conditions, research was launched in 2020 on the indication of CI resilience failures in the energy, transport and ICT sectors. As a result, the CERFI Tool was developed to enable the predictive indication of failure of critical entity's resilience in phases of prevention and absorption of impacts. The essence of this tool is to link the knowledge of threats and the protective part of resilience. Based on this information, entities can detect the most significant threats that could cause a failure in the delivery of their essential services.

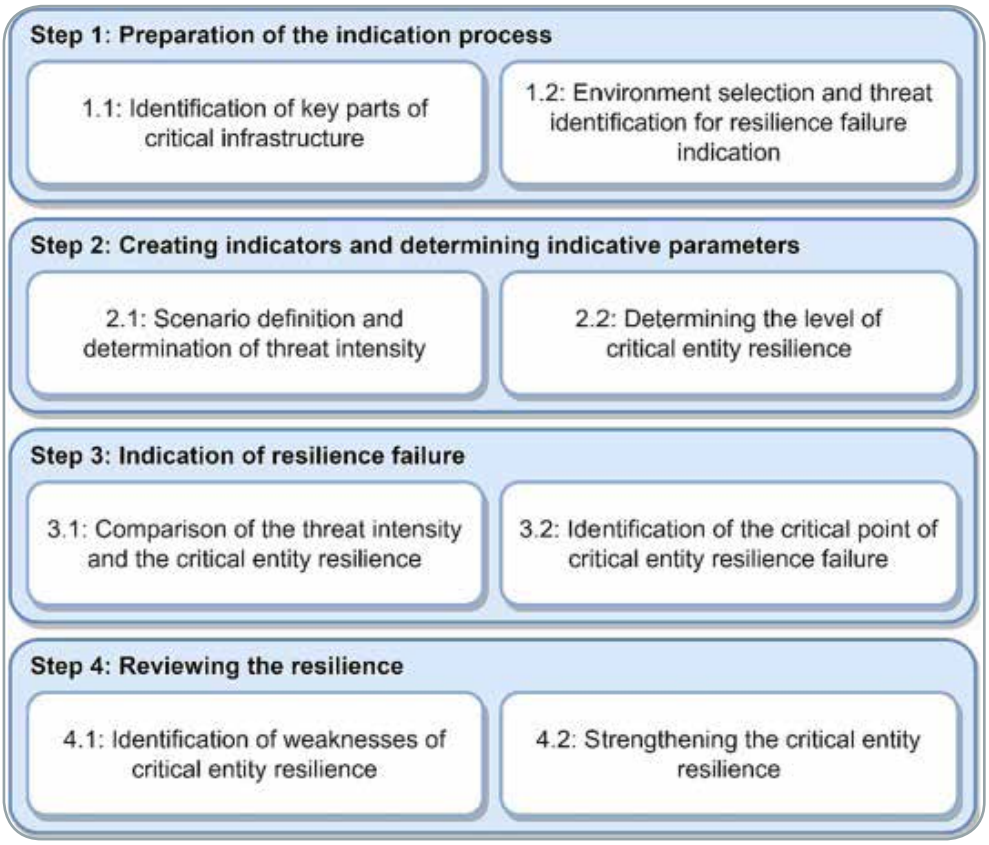
Conclusion

With the adoption of Directive (EU), 2022/2557, the focus on CI has shifted from elements to entities. This change in perception is very positive, as the basis for reliable CI is sufficiently resilient critical entities. However, the adoption of the Directive has raised the question of how to assess the resilience of critical entities in relation to contemporary security threats. Until now, all attention has been devoted exclusively to assessing the resilience of CI elements. An important solution to this problem could be a predictive indication of resilience failure of critical entities. For this purpose, the CERFI Tool was developed by the authors of the paper.

The essence of the CERFI Tool is a probabilistic algorithm that predicts the relationship between the intensity of the threat and the protective part of critical entity resilience through indicators (to be created by the assessors themselves). The result of this prediction is an indication of the critical point of failure of the critical entity's resilience in phases of prevention and absorption of impacts. Failure of the critical entity resilience in this context refers to a situation where the level of the protective part of resilience is not



sufficient to protect the critical entity, as a result of which there is an immediate failure of the supply of basic services provided by the critical entity. At the same time, it is necessary to mention some limitations of this approach. The CERFI Tool enables the indication of the failure of resilience of only one critical entity as a result of the action of only one threat and the subsequent occurrence of only one incident. As part of the assessment, it is therefore not possible to consider the interdependencies of critical infrastructures or actually occurring cascading or synergistic effects.



The CERFI Tool thus contributes to improving the security of technically oriented infrastructure systems, especially those in the areas of energy and transport. However, in some cases it can also be applied to selected socio-economic infrastructure systems, e.g., in the field of emergency services or healthcare. The CERFI Tool is primarily intended for security liaison officers of individual infrastructure systems. By applying this tool, they can obtain valuable information about the level of the protective part of resilience of a critical entity and its elements. However, this information is only predictive in nature and is essentially an indication of weaknesses that require subsequent attention.

The CERFI Tool has already been successfully tested in practice on selected critical entities in the energy and transport sectors. This is illustrated by the case study presented at the end of the article. This study focused on the indication of a substation resilience failure due to a physical assault using a motor vehicle. The results of the study show that the CERFI Tool indicated an insufficient level of critical entity resilience in question and identified weaknesses that need increased attention. According to the findings, it is proposed that further research be directed particularly in the area of tools for strengthening the resilience of critical entities and assessing their effectivity. It would also be appropriate to pay attention to research on the critical entities' resilience failure indication in the recovery and adaptation phase.

The Full Report can be downloaded at https://www.sciencedirect.com/science/article/pii/S0925753523003132

Cybersecurity Investment: Spotlight on Vulnerability Management

The new report of the European Union Agency for Cybersecurity (ENISA) confirms investment continues to grow but stresses the importance of vulnerability management.

Despite a 25% increase of the cost of major cyber incidents in 2022 compared to 2021, the new report on cybersecurity investment reveals a slight increase of 0,4% of IT budget dedicated to cybersecurity by EU operators in scope of the NIS Directive.

However, if organisations are inclined to allocate more budget to cybersecurity, 47% of the total of organisations surveyed do not plan to hire information security Full Time Equivalents (FTEs) in the next two years. Besides, 83% of these organisations claim recruitment difficulties in at least one information security domain. Such hiring issues surfacing in the report could be one of the factors when it comes to managing vulnerabilities.

Indeed, an analysis on patching of critical IT and OT assets in the transport sector shows that 51% of the organisations in the transport sector need one month to patch critical vulnerabilities and 21% need a time between 1 month and six months. Only 28% of the surveyed organisations fix critical vulnerabilities on critical assets in one week.

The new report investigates how operators invest in cybersecurity and comply with the objectives of the NIS Directive. Collected from a total of 1,080 Operators of Essential Services (OES) and Digital Services Providers (DSP) from all 27 EU Member States, the data apply to reference year 2022.

Scope of the report

For the purpose of the analysis published today, the survey performed looked at OES and DSP as identified in the European Union's Directive on Network and Information Security Systems (NIS Directive). The objective of the report was to identify how organisation invest in cybersecurity in relation to the objective of meeting the requirements set by the initial NIS Directive.

However, the concept of investment also extends to the human element. 2023 is the European Year of Skills. This is why particular emphasis was placed on the topic of cybersecurity skills among OES and DSPs and to cybersecurity workforce hiring and gender balance.

The report therefore delves into IT security staffing and organisation of information security by OES and DSP with a special focus on the transport sector.

Key findings

- The part of IT budget OES/DSPs dedicated to cybersecurity reached 7,1% in 2022, representing an increase of 0,4% compared to 2021;

- 42% of OES/DSPs subscribed to a dedicated cyber insurance solution in 2022, representing a 30% increase from 2021. Still only 13% of SMEs subscribe to cyber insurance;

- OES/DSPs allocate 11,9% of their IT FTEs for information security (IS) a decrease of 0,1%

- OES/DSPs employ an average of 11% of women in IS FTEs. With median being at zero percent most of surveyed organisations do not employ any women as part of their IS FTEs;

- 47% of OES or DSPs do not plan to hire IS FTEs in the next two years,

- The organisations planning to hire information security FTEs in the next two years aim to hire 2 FTEs, with an average of 4 FTEs but 83% of the surveyed organisations claim recruitment difficulties in at least one information security domain.

- The NIS Directive is the main driver for cybersecurity investments for 55% of OES in the transport sector;

- 51% of the transport organisations manage OT security with the same unit or people as IT cybersecurity.

Vulnerability Management

Vulnerability management describes the process to identify and assess the associated risk of security vulnerabilities in order to resolve the cause before these can be exploited or intelligently reduce the risk of it by implementing adequate mitigation measures.

Managing vulnerabilities and ensuring patches are available protects the end-users and helps to ensure security is applied across the whole lifecycle of any product. The 2022 edition of the NIS Investments report found that for 46 % of organisations surveyed it takes more than 1 month to patch critical vulnerabilities. Improving interoperability, automation and streamlined processes in order to exchange information can go a long way towards ensuring vulnerability disclosure. At the same time, vendors need to have the appropriate tools, processes and people in place to implement secure-by-design practices in order to reduce the risk for users, whereas organisations are responsible to reduce the time between the

disclosure of vulnerabilities and their remediation by enabling tooling for automated vulnerability information sharing.

EU Vulnerability Coordination and Vulnerability Database

The NIS2 establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creates an EU vulnerability database for publicly known vulnerabilities in ICT products and ICT services, to be operated and maintained by the EU agency for cybersecurity (ENISA). The combination of national and EU efforts will form the basis for a mature vulnerability disclosure ecosystem within the EU. Importantly, these initiatives will contribute to an enhanced vulnerability management landscape.

The EU cybersecurity policy framework includes a number of proposed policy files. These include the Cyber Resilience Act (CRA) and the Cyber Solidarity Act (CSoA) which include provisions that propose to further improve vulnerability management in the EU, such as additional measures ensuring the quality of products and services that will contribute to the application of security aspects throughout the entire product lifecycle.

Background

The objective of the Directive on Security of Network and Information Systems (NIS Directive) is to achieve a high common level of cybersecurity across all Member States. The revised directive known as NIS2 came into force on 16 January 2023 extended the scope to new economic sectors.

One of the three pillars of the NIS Directive is the implementation of risk management and reporting obligations for OES and DSP.

OES provide essential services in strategic sectors of energy (electricity, oil and gas), transport (air, rail, water and road), banking, financial market infrastructures, health, drinking water supply and distribution, and digital infrastructure (Internet exchange points, domain name system service providers, top-level domain name registries).

DSP operate in an online environment, namely online marketplaces, online search engines and cloud computing services.

The report investigates how operators invest in cybersecurity and comply with the objectives of the NIS Directive. It also gives an overview of the situation in relation to such aspects as IT security staffing, cyber insurance and organisation of information security in OES and DSP.

New York lost $775M in cyberattacks on critical infrastructure in 2022, report says

Cyberattacks on New York's critical infrastructure are on the rise, according to a recent report from the state comptroller's office. The state experienced more than 25,000 cyberattacks in 2022, up 53% from 16,400 incidents in 2016, costing the state in excess of $775 million.

New York had the third highest number of ransomware attacks and corporate data breaches in 2022, behind California and Texas.

Critical infrastructure attacks involve systems and assets that are vital for the functioning of society, the economy and national security, the report said.

"Cyberattacks are a serious threat to New York's critical infrastructure, economy and our everyday lives," DiNapoli said in a statement. "Data breaches at companies and institutions that collect large amounts of personal information expose New Yorkers to potential invasions of privacy, identity theft and fraud."

Attacks against critical infrastructure in New York last year included nine incidents in health care and public health, eight incidents in financial services and seven incidents in both commercial and government facilities.

The report also stated that even more troubling are incidents such as ransomware or distributed denial of service attacks that have the potential to shut down systems that we rely on for water, power, health care and other necessities

NCSC warns of enduring and significant threat to UK's critical infrastructure

The UK's cyber chief has signalled that the threat to the nation's most critical infrastructure is 'enduring and significant', amid a rise of state-aligned groups, an increase in aggressive cyber activity, and ongoing geopolitical challenges.

In its latest Annual Review, published today, the National Cyber Security Centre (NCSC) – which is a part of GCHQ – warned that the UK needs to accelerate work to keep pace with the changing threat, particularly in relation to enhancing cyber resilience in the nation's most critical sectors.

These sectors include those that provide the country with safe drinking water, electricity, communications, its transport and financial networks, and internet connectivity.

Over the past 12 months, the NCSC has observed the emergence of a new class of cyber adversary in the form of state-aligned actors, who are often sympathetic to Russia's further invasion of Ukraine and are ideologically, rather than financially, motivated.

In May this year, the NCSC issued a joint advisory revealing details of 'Snake' malware, which has been a core component in Russian espionage operations carried out by Russia's Federal Security Service (FSB) for nearly two decades.

Today, the NCSC is reiterating its warning of an enduring and significant threat posed by states and state-aligned groups to the national assets that the UK relies on for the everyday functioning of society.

More broadly, the UK government remains steadfast in its commitment to safeguarding democratic processes. Recent milestones include the implementation of digital imprint rules under the Elections Act to foster transparency in digital campaigning, fortifying defences against foreign interference through the National Security Act, and advancing online safety measures through the implementation of the Online Safety Act.

NCSC CEO Lindy Cameron said:

"The last year has seen a significant evolution in the cyber threat to the UK – not least because of Russia's ongoing invasion of Ukraine but also from the availability and capability of emerging tech.

"As our Annual Review shows, the NCSC and our partners have supported government, the public and private sector, citizens, and organisations of all sizes across the UK to raise awareness of the cyber threats and improve our collective resilience.

"Beyond the present challenges, we are very aware of the threats on the horizon, including rapid advancements in tech and the growing market for cyber capabilities. We are committed to facing those head on and keeping the UK at the forefront of cyber security."

Defending Democracy

The Annual Review highlights a new trend of malicious actors targeting the personal email accounts of high-profile and influential individuals involved in politics. Rather than a mass campaign against the public, the NCSC warns that there is a "persistent effort" by attackers to specifically target people who they think hold information of interest.

The NCSC assesses that personal as opposed to corporate accounts are being targeted as security is less likely to be managed in depth by a dedicated team. In response, earlier this year the NCSC launched a new opt-in service for high-risk individuals to be alerted if malicious activity on personal devices or accounts is detected and to swiftly advise them on steps to take to protect themselves.

In response, the Annual Review highlights the work of the NCSC and wider government in weaving resilience into the fabric of the UK's democratic processes ahead of the next election, which includes the establishment of the Joint Election Security Preparedness (JESP) unit.

Enhancing transport safety and resilience: trends, challenges and innovations

A new Joint Research Centre report Research and Innovation in Transport Safety and Resilience in Europe, maps European innovation efforts to achieve this goal and identifies the main areas to focus on, such as human factors, cyber security and climate-proof infrastructure.

To achieve sustainable, smart and affordable future mobility in the EU, it is essential to enhance safety and resilience against natural disasters or man-made disruptions.

The recent Joint Research Centre study highlights road transport as one of the areas with the most need for progress, due to the high number of avoidable accidents that still occur in Europe. According to the researchers, promoting a safety culture and safeguarding human vigilance and performance, safe infrastructure design and maintenance, automation and assisted driving are some of the interventions that could make our roads safer.

Planes, trains and boats show excellent results with low fatalities but similarly to road transport, digitalisation and automation will help maintain this track record in the future.

The report draws its conclusions from a selection of the most pertinent EU-funded projects, identified through the Transport Research and Innovation

Monitoring and Information System (TRIMIS) database. The publication serves as a guide, showcasing how research and innovation are shaping the future of transport safety and resilience in Europe.

Road transport

Research and innovation have been vital in addressing safety challenges across different transport modes. In fact, while the most recent data indicate that more than 20.000 people were killed in road accidents in 2022, the trend has decreased by 10% in relation to 2019. And the total number of fatalities in 2021 was 40% lower than the number of fatalities recorded at the beginning of 21st century.

Of the 143 EU-funded projects selected for the analysis, 48 focus on road transport and the adoption of a safe system approach that combines technological innovations with non-technological measures and behavioural adaptations. Specifically, the areas of interventions identified to reduce the probability of road accidents include infrastructure, with a solid road design and maintenance, and safe vehicle technologies, such as driver assistance systems.

Among the proposed initiatives, the report mentions the use of AI computer vision to detect dangerous traffic situations, alert drivers, and take evasive action. These could help ensure drivers are fit to operate vehicles by detecting any distractions, fatigue, or impairing substances.

All these measures show promise in achieving the goal of getting close to zero deaths and serious injuries on EU roads by 2050. This target is

set out in the EU Road Safety Policy Framework 2021-2030 - Next steps towards "Vision Zero" and includes an intermediate target of a 50% reduction by 2030.

Aviation, rail and maritime transport

The report also highlights the remarkable safety record of aviation, rail, and waterborne transport. With zero fatal accidents for EU commercial aircraft since 2016, aviation is setting new standards in safety despite the rise in air traffic. Ongoing efforts in aviation focus on AI-assisted navigation, air traffic management, safety nets, and airport operations to ensure risk-free travel.

Similarly, the railway sector has made significant strides in safety, with a 38% decrease in accidents compared to 2010, primarily by prioritising infrastructure safety and security. For maritime transport, innovative projects are tackling the root causes of incidents, aiming to eliminate human error as a leading factor. Detection and warning systems, as well as smart safety equipment and procedures, are being developed to protect passengers and crew members.

Transport resilience against natural and man-made crises

Crises such as the COVID pandemic and the Russian war in Ukraine highlight both the importance and fragility of transport systems when facing large-scale disruption.

As the EU transport system will be challenged by climate events and other possible natural or man-made disruptions, various policy measures are in place to strengthen its resilience and ensure the continuity of its services, protect passengers and freight and enhance the cybersecurity of transportation networks.

These measures include the completion of the Single European Transport Area, with emphasis on the Trans-European Transport (TEN-T) Network to ensure multimodality and interoperability; and the Contingency Plan for Transport, which provides guidance to Member States in areas like connectivity, passenger protection and efficient border management during times of crisis.

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

However, resilience is still a major challenge for the EU transport system, considering its complexity and interconnection to address demand, efficiency and sustainability objectives, as well as the potential increase in disruptions. In fact, 50 of the EU-funded projects this report analysed focus on developing advanced monitoring techniques to identify vulnerabilities and facilitate maintenance, detecting and predicting disruptions through ICT and AI technologies, and creating frameworks that take into account factors such as risk assessment, impact analysis and resource allocation to make informed decisions during disruptions.

The research trends the study identifies converge towards operational resilience at the vessel and network levels, developing resilient physical and digital infrastructure, ensuring fleet resilience and addressing critical infrastructure resilience and cybersecurity. Urban mobility resilience is also a critical aspect, necessitating collaboration, knowledge management and monitoring of the entire transport system for real-time information.

The report concludes that several key areas should be considered for future research and policy initiatives, including resilience design and certification to cover structural resilience (e.g. heat-resistant materials); virtual testing to simulate systems' response to disruptions and measures to preserve and restore operations when experimental study is impractical, and data- and AI-driven resilience monitoring and response.

DOE Announces $42 Million To Strengthen Reliability, Resiliency, And Affordability of America's Power Grid

The U.S. Department of Energy (DOE) has announced $42 million for 15 projects across 11 states to improve the reliability, resiliency, and flexibility of the domestic power grid through the development of next-generation semiconductor technologies. Funded through DOE's Unlocking Lasting Transformative Resiliency Advances by Faster Actuation of power Semiconductor Technologies (ULTRAFAST) program, the technologies being developed would enable more effective control of grid power flow and better protection of critical infrastructure assets. Streamlining the coordinated operation of electricity supply and demand will improve operational efficiency, prevent unforeseen outages, allow faster recovery, minimize the impacts of natural disasters and climate-change fueled extreme weather events, and redcude grid operating costs and carbon intensity. Today's announcement supports President Biden's Investing in America agenda to modernize the nation's power grid, accelerate the deployment of clean energy resources, and boost America's energy and national security.

"Modernizing our nation's aging power grid is critical to strengthening our national and energy security, and absolutely essential to reaching President Biden's ambitious goal of a net-zero economy by 2050," said U.S. Secretary of Energy Jennifer M. Granholm. "This new investment will support project teams across the country as they develop the innovative technologies we need to strengthen our grid security and bring reliable clean electricity to more families and businesses—all while combatting the climate crisis."

Managed by DOE's Advanced Research Projects Agency-Energy (ARPA-E), the teams announced today will advance the Biden-Harris Administration's decarbonization goals by enabling a more secure and reliable grid and allowing it to utilize more solar, wind, and other clean energy.

DHS CISA and UK NCSC Release Joint Guidelines for Secure AI System Development

Taking a significant step forward in addressing the intersection of artificial intelligence (AI) and cybersecurity, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) and the United Kingdom's National Cyber Security Centre (NCSC) jointly released Guidelines for Secure AI System Development

to help developers of any systems that use AI make informed cybersecurity decisions at every stage of the development process. The guidelines were formulated in cooperation with 21 other agencies and ministries from across the world – including all members of the Group of 7 major industrial economies -- and are the first of their kind to be agreed to globally.

"We are at an inflection point in the development of artificial intelligence, which may well be the most consequential technology of our time. Cybersecurity is key to building AI systems that are safe, secure, and trustworthy," said Secretary of Homeland Security Alejandro N. Mayorkas. "The guidelines jointly issued today by CISA, NCSC, and our other international partners, provide a commonsense path to designing, developing, deploying, and operating AI with cybersecurity at its core. By integrating 'secure by design' principles, these guidelines represent an historic agreement that developers must invest in, protecting customers at each step of a system's design and development. Through global action like these guidelines, we can lead the world in harnessing the benefits while addressing the potential harms of this pioneering technology."

The guidelines provide essential recommendations for AI system development and emphasize the importance of adhering to Secure by Design principles that CISA has long championed.

"The release of the Guidelines for Secure AI System Development marks a key milestone in our collective commitment—by governments across the world—to ensure the development and deployment of artificial intelligence capabilities that are secure by design," said CISA Director Jen Easterly. "As nations and organizations embrace the transformative power of AI, this international collaboration, led by CISA and NCSC, underscores the global dedication to fostering transparency, accountability, and secure practices. The domestic and international unity in advancing secure by design principles and cultivating a resilient foundation for the safe development of AI systems worldwide could not come at a more important time in our shared technology revolution. This joint effort reaffirms our mission to protect critical infrastructure and reinforces the importance of international partnership in securing our digital future."

The guidelines are broken down into four key areas within the AI system development lifecycle: secure design, secure development, secure deployment, and secure operation and maintenance. Each section highlights considerations and mitigations that will help reduce the cybersecurity risk to an organizational AI system development process.

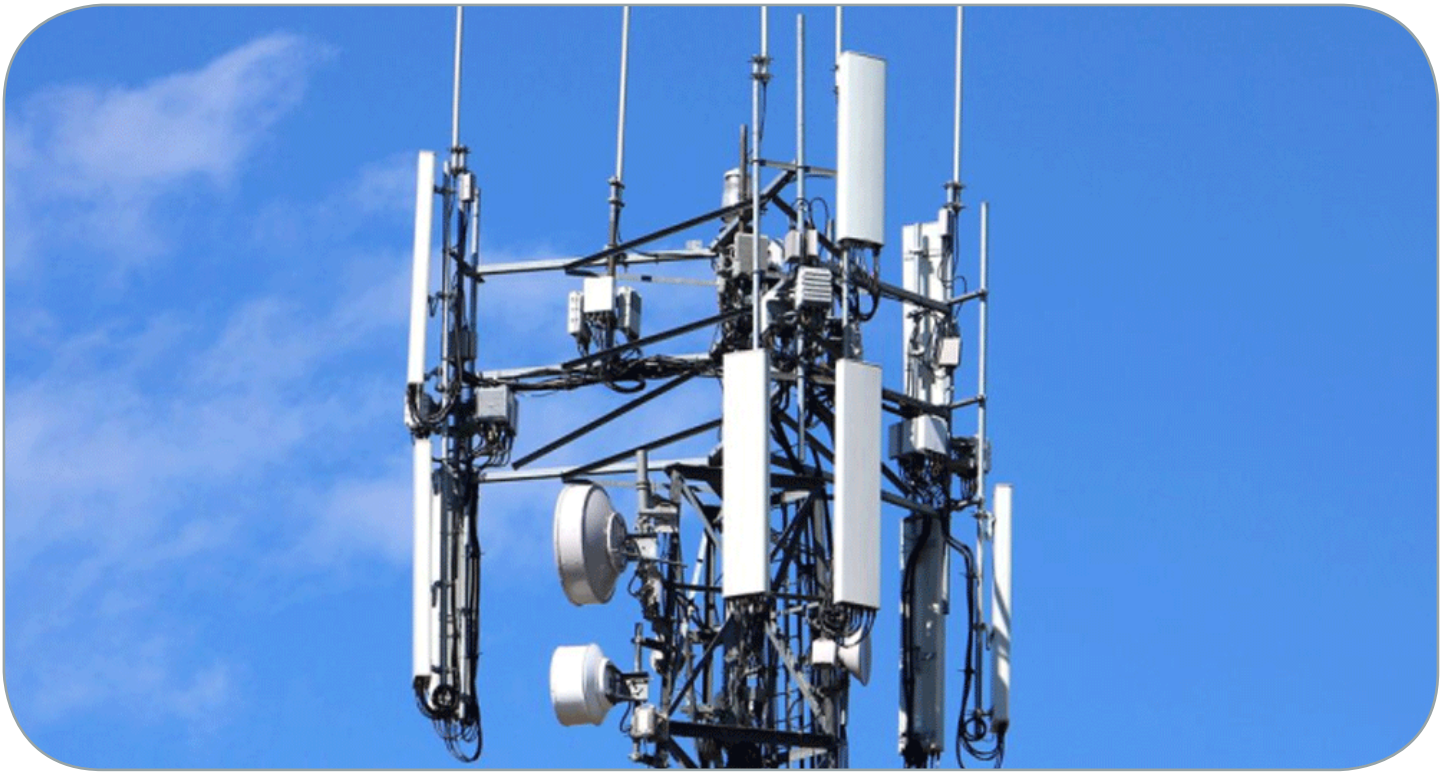
"We know that AI is developing at a phenomenal pace and there is a need for concerted international action, across governments and industry, to keep up," said NCSC CEO Lindy Cameron. "These Guidelines mark a significant step in shaping a truly global, common understanding of the cyber risks and mitigation strategies around AI to ensure that security is not a postscript to development but a core requirement throughout. I'm proud that the NCSC is leading crucial efforts to raise the AI cyber security bar: a more secure global cyber space will help us all to safely and confidently realize this technology's wonderful opportunities."

"I believe the UK is an international standard bearer on the safe use of AI," said UK Secretary of State for Science, Innovation and Technology Michelle Donelan. "The NCSC's publication of these new guidelines will put cyber security at the heart of AI development at every stage so protecting against risk is considered throughout."

These guidelines are the latest effort across the U.S.'s body of work supporting safe and secure AI technology development and deployment. In October, President Biden issued an Executive Order that directed DHS to promote the adoption of AI safety standards globally, protect U.S. networks and critical infrastructure, reduce the risks that AI can be used to create weapons of mass destruction, combat AI-related intellectual property theft, and help the United States attract and retain skilled talent, among other missions.

Earlier, CISA released its Roadmap for Artificial Intelligence, a whole-of-agency plan aligned with national strategy to address our efforts to promote the beneficial uses of AI to enhance cybersecurity capabilities, ensure AI systems are protected from cyber-based threats, and deter the malicious use of AI capabilities to threaten the critical infrastructure Americans rely on every day. Learn more about CISA's AI work.

Cutting industry emissions and fighting the climate crisis



by International Telecommunication Union (ITU)

Digital solutions may be renowned for enabling energy efficiency and reducing emissions in other sectors. But information and communication technology (ICT) companies must also put their own house in order.

"We can only earn laurels for helping other sectors get to zero emissions if we achieve net-zero ourselves," says ITU Deputy Secretary-General Tomas Lamanauskas.

Alongside promoting tech-based climate solutions, the wide-ranging industry needs to tackle its own emissions and energy consumption.

Holding the line on global warming at 1.5°C during the present century means reducing greenhouse gas (GHG) emissions to net-zero by around 2050, according to the Intergovernmental Panel on Climate Change (IPCC).

This can only happen if companies worldwide, in all industries, commit to science-based targets and follow stringent decarbonization plans.

The International Telecommunication Union (ITU) has teamed up with more than 40 companies and organizations aiming to mobilize the whole global digital industry. The Green Digital Action track at the UN climate change conference, COP28, boosts efforts to cut the emissions of the digital industry in line with international standards linked to science-based targets.

To align with the Paris Agreement, the global ICT industry will have to reduce its GHG emissions by 45 per cent from 2020 to 2030.

ITU standard ITU-T L.1470, developed in collaboration with the Global Enabling Sustainability Initiative (GeSI), mobile telecom industry association GSMA, and Science Based Targets (SBTi), sets out the necessary trajectories for the whole ICT sector for the next few years.

Energy-efficient data centres powered exclusively by renewables like solar and wind energy, would go a long way in reducing the sector's own carbon footprint. ITU and the World Bank offer a practitioners guide for green data centres.

Digital companies accounted for 60 per cent of corporate renewable power purchases in 2021, according to the Greening Digital Companies 2023 study by ITU and the World Benchmarking Alliance (WBA). Still, emissions and energy consumption across the industry continue to grow.

Mobile providers taking steps

GSMA is urging mobile operators, particularly, to strive for and uphold global climate goals.

"The mobile industry has a unique opportunity to drive positive change across multiple sectors in collaboration with our suppliers, investors and customers," says GSMA Director General Mats Granryd. "We are proud that the mobile industry continues to align around the 1.5oC decarbonization pathway, demonstrating how the private sector can show leadership and responsibility in addressing one of the gravest challenges facing our planet."

José María Álvarez-Pallete López, CEO of Spanish network operator Telefónica, says his company has "very ambitious targets to achieve net-zero emissions and help our customers in their transition to greener energy solutions."

British mobile and fixed-broadband operator BT Group also cites important steps in the right direction.

"BT Group has led on climate action for more than 30 years," says Gabrielle Ginér, the group's head of environmental sustainability. "We're already purchasing 100 per cent renewable electricity worldwide and have outlined plans to become a net-zero-emissions business by 2031 for our own operations, and by 2041 for our supply-chain and customer emissions."

The next generation of full-fibre and 5G mobile networks that the company is now building across the UK will help support the transition to a low-carbon economy, she added. "We know that technology will play a vital role in reducing global emissions."

Yet all this is only the beginning of what companies need to do worldwide.

"The digital and green transitions are gathering speed," says Pekka Lundmark, President and CEO of Nokia. "But there is still more to do if we want to reach net zero, secure circular supply chains, and combat climate change. In particular, we need to make sure we pursue collaboration – working together to invest in digital infrastructure and digitalized economies."

Clearing up climate accounting

All this is easier said than done. With more countries and companies setting net-zero targets, transparent global tracking and accountability has become paramount.

"To make smart choices in reducing emissions and managing energy demands for the ICT sector, we need accurate data," says Guangzhe Chen, Vice President for Infrastructure at the World Bank. "This information is vital for countries to manage finite resources wisely and to reduce the sector's carbon footprint."

While current reporting on energy use and emissions across the sector is inadequate, there have been steps in the right direction.

Vincent Garnier, Director General of FTTH Council Europe, noted: "We are developing a programme

to help our members better measure their carbon emissions, share best practices and accelerate their transition."

How to quantify emissions and reduction

Tracking ICT decarbonization hinges on emission factors. These indicators – describing rates of emission from any given product, service, or activity – are key in calculating carbon footprints.

Green Digital Action partners have pledged to contribute to a publicly open database, hosted and maintained by ITU,with an accompanying dashboard to assess industry-wide progress towards net-zero goals globally, regionally, and by sub-sectors. These promise to become a powerful tool to make informed decisions, promote sustainable practices, and drive progress towards a net-zero future.

As COP28 approaches, Green Digital Action calls on all ICT companies globally to join in a commitment to:

- Set science-based, 1.5°C -aligned emissions-reduction targets, reduce Scope 1, 2 and 3 emissions, and publish transition plans outlining decarbonization trajectories to meet net-zero targets.

- Report data on all GHG emission scopes and categories yearly in a publicly open database.

- Help create an ICT-sector database on emission factors, join an implementation working group, and take part in ITU-led environment, climate, and circular economy standardization work (ITU-T Study Group 5).

Green Digital Action sessions at COP28 will launch these and other commitments to reduce the sector's footprint, leverage digital technologies to ensure life-saving disaster alerts, and facilitate climate solutions across all industries. The aim is to build critical mass action for effective climate action across the ICT sector.

Enea Evolves Mobile Network Security Portfolio to Improve Resilience Amid Growing Threats

Enea consolidates its suite of network security solutions to serve the unique needs of Mobile Network Operators and CPaaS providers as the volume of messaging and signaling attacks continues to break records and threaten critical infrastructure.

Enea, a leading provider of telecom and cybersecurity solutions, has consolidated its suite of network security solutions to address the mounting challenges of mobile network security and regulatory compliance and addresses two key areas: signaling security and messaging security. The portfolio update emphasizes intelligence-driven adaptability and accuracy and comprises four solutions tailored to the critical and growing demands of Mobile Network Operators (MNOs) and Communication Platform as a Service (CPaaS) providers and aggregators, and a further solution designed for the unique requirements of national security agencies.

The three firewall solutions are based on Enea's latest cloud-native platform technology, which enables deployment in public or private cloud, on virtual infrastructure, or on bare-metal servers. Granular control for multi-site deployments improves resilience and manages regulatory compliance for cross-border needs. The platform uses flexible configurations, allowing swift upgrades to counter new threats. Mobile network operators typically require both messaging and signaling firewalls and therefore benefit from a unified platform for both solutions.

To ensure optimal protection, all solutions integrate extensive threat intelligence provided through a combination of Enea's expert security analysts, machine learning, and intelligent algorithms. Both signaling and messaging security rely heavily on the actionable insights threat intelligence provides to keep defense up-to-date and ahead of threat actors, fraudsters, and scammers.

An Interview with EE-ISAC

Ben Lane, CIPRE event manager, met with Aurelio Blanquet, Secretary General of EE-ISAC - the European Energy - Information Sharing & Analysis Centre.

Ben Lane: Briefly explain the ultimate purpose and goal of EE-ISAC.

Aurelio Blanquet: The ultimate purpose of the ISAC is to provide a trusted community for joint analysis of cybersecurity threats, vulnerabilities, and incidents leveraged by a timely vaulted of information sharing that allows its members to take their own effective measures supported by better informed decisions. The final goal is to make information sharing a cornerstone to improve the resilience and cybersecurity of the European energy infrastructure. As the three main pillars we always tend to talk about technology, processes, and people. However, co-operation and information sharing are a founding base for what we do and without that, we would be lacking a critical building block of the knowledge, awareness, preparedness, and response needed to achieve a more cyber-secure European energy infrastructure.

Aurelio Blanquet, Secretary General of EE-ISAC

BL: That's a good overview. Thank you. Let's drill a bit deeper then into information sharing. What methods do you use to share information and who gets the information?

AB: The methods are embedded in our goals and our objectives, and We have two main approaches:

One at the member level and we aim to contribute to embed information sharing into the cybersecurity processes of our members, or use their processes already in place syncing their own MISP (Malware Information Sharing Platform) if they have one, or pushing them to directly feed the EU MISP, a platform developed under the EC project "Empowering EU ISACs", provided by the EC and hosted by ENISA since September 2022. At the same time, we incentivize our members to work on Threat Analysis and to develop Threat Intelligence skills. We must note that the work developed at EE-ISAC is mainly done by its members; not only because they are the owners of sensitive cybersecurity information, but also because they are the ones that know what kind of actions that they need to take. So, they are the main players in this work and what we do is to help and incentivize them to have these processes in place. The European Commission provided a European MISP platform for all the EU ISACs. Once a member has an incident he should work on it, do a threat analysis, and develop threat intelligence capabilities.

An important part of the methodology is to vault the information that is loaded on the platform. To assist in this task, we have a core IT team made up of volunteers from members to carry out this operation to ensure that all

the information that is fed onto the platform is properly vaulted.

The other approach is at the European level, and our goals and objectives are to target operators and stakeholders from all European countries, including UK. The goal is to have all countries represented in the EEE-ISAC because in this way we can cope with different sensibilities, geographical situations, geopolitical exposure, and we also need to be all connected from the information point of view.

BL: How is information disseminated? And a secondary question is about non-members because it seems there might be some gaps in the information sharing, i.e., your members need to actively find the information. How does that happen? And anyone not within EE-ISAC as a member is not seeing the information, is that correct?

AB: This depends on the confidentiality level of the information. We use a TPL protocol and if the information that is fed onto the platform, as well as the threat analysis that we are talking about, is TPL red, the answer is clearly no: This information will not be delivered outside the group defined in the dissemination. Of course, if the TPL is green or white, the information will become public.

For example, if we are working with a member on a report that later will be made publicly available, from the moment we start working on the report to the moment before delivery, the report is accessible for all members because some of them will be contributors to the report, which means that the information is always delivered in a timely fashion to members. The single most important responsibility of each member is to ensure that they are responsible for their own information and the use of anyone else's information respecting the TPL protocol.

BL: What advantages does a member of EE-ISAC have over a non-member? Can you describe the advantage? Do members support EE-ISAC financially?

AB: This is a not-for-profit organization; the only source of revenue comes from membership fees. We don't attract sponsorship. From the very beginning in 2012, we realized that one of the critical issues was knowledge. We all need knowledge, and we all need knowledgeable information. In the very early draft design of the DENSEK project (a H2020 project

and the founding father of the EE-ISAC), we realized that looking to the energy sector, the knowledge that we had in 2012 and even now around cybersecurity joining all the energy companies was not enough to claim we were a knowledgeable group. So, who could add to and complement our knowledge? The first answer of course is the solution providers; they provide the solutions we need to overcome our challenges. So: we have problems, we have needs as energy operators, and the solution providers develop solutions. But this is not enough because on the 'top of the edge' of knowledge is academia and research institutes. Those are the guys mainly responsible for ensuring that knowledge in Europe is on 'top of the edge'; they are responsible for the research, they are the main actors for learning and teaching. Without academia, we were lacking knowledge, and we were lacking a unique opportunity to learn. And so, we have academia and research institutes as members, and we decided their membership fees would be paid by in "kind", not in money.

We also work closely with EU entities as non-paying member as ENISA for example. ENISA delivers knowledge, reports and other services as the EU Agency for Cybersecurity. We also realized that we need another category of stakeholders that were not able to be members because they were not European, or if they were they were not operators nor service providers. And so, we decided to create partnerships with other ISACs such as the Japanese Energy ISAC (JE-ISAC) as well as the US Energy ISAC (E-ISAC) to widen the knowledge base and viewpoints.

We also launched co-operation with other organizations such as the EUTC (European Utilities Telecom Council) because we realized that if we are talking about the European energy infrastructure as critical, then it goes without saying that they depend on telecommunications. And telecommunications are also a critical infrastructure for energy, so it made sense to partner with EUTC.

The same way with EDSO (European Distribution System Operators) as representative of the European DSO with the largest electricity infrastructures and the ENCS (European Network for Cybersecurity), also an European association with a permanent team of experts that makes it the point of excellence in designing cybersecurity solutions for its members, who are exclusively European energy utilities.

BL: It might be useful to understand how you see collaborations developing in the future because there will need to be increasing collaborations across Europe to ensure these standards and these recommendations are fully promoted to the widest possible audience.

AB: Yes, I think it will be a never-ending process, and very challenging. The EUTC collaboration is a good example of how other collaborations can develop; by having a single voice for cybersecurity in telecommunications for utilities means we are combining numerous telecoms, cybersecurity, and "energy perspective" skills in one place, which means the "whole" is working together much more effectively. We will always be looking for new co-operations and collaborations for the benefit of a wider community.

BL: Thank you for your time, and good luck in your important work.

The Power of Iris Recognition for Securing Critical Infrastructure Spaces

Introduction

In today's world, safeguarding critical infrastructure spaces is of utmost importance. These spaces, such as data centers, nuclear power plants, water reservoirs, power stations-transformers, and airports, often house highly sensitive data, valuable research, resources affecting public health and daily life, and expensive equipment. The security measures implemented in these areas must be advanced, reliable, and efficient to ensure the protection of not only the assets but also the lives of the public and workers involved. One technology that has proven to be highly effective in access control for critical infrastructure spaces is iris recognition.

Understanding Iris Recognition Technology

Iris recognition technology has gained popularity across various industries, including healthcare, education, immigration and border control, law enforcement, and government. Its accuracy in authentication and robust countermeasures against fraudulent attempts make it a preferred choice for many organizations. In fact, except for DNA, iris biometrics are considered the second-most accurate biometric modality, with the fastest search speed in one-to-many search mode. On the other hand, iris biometry is better than DNA for differentiating identical twins.

One of the providers of this technology is Iris ID Systems Inc. has been a pioneer in iris

recognition research, development, and production since 1997. Their IrisAccess® platform is the world's most widely deployed iris recognition platform, authenticating millions of individuals across thousands of locations. The platform offers unmatched speed, as demonstrated in a UK Government-commissioned study where IrisAccess searched records almost 20 times faster than the next fastest technology.

Advantages of Iris Recognition for Critical Infrastructure Spaces

When it comes to securing critical infrastructure spaces, iris recognition technology offers several unique advantages:

1. Reliability

Iris recognition is highly reliable as the iris cannot be stolen, lost, or compromised. Unlike access cards or PINs, which can be forgotten or stolen, the iris remains with an individual throughout their lifetime. Additionally, iris recognition systems employ liveness detection, ensuring that only a living person is identified. This feature rejects static images, making it difficult for impostors to deceive the system.

2. Stability

The iris pattern is formed by the age of 10 months and remains stable throughout a person's life. Unlike other biometric modalities that may change over time, such as fingerprints or facial features, the iris pattern remains consistent. This stability ensures that once an individual's iris is enrolled in the system, they can be reliably authenticated for years to come.

3. Uniqueness

The probability of two irises being the same is nearly impossible. Even identical twins have unique iris patterns. This high level of uniqueness makes iris recognition an ideal choice for accurate identification and authentication purposes. It eliminates the risk of false positives or false negatives, providing a secure access control solution.

4. Flexibility

Iris recognition technology is highly flexible and can easily integrate into existing security systems or operate as a standalone solution. Whether it's integrating with access control systems, surveillance cameras, or other security measures, iris recognition can seamlessly adapt to various environments and requirements.

5. Non-invasiveness

Unlike retinal scanning, which requires the use of bright lights and direct contact with the eye, iris recognition is completely non-invasive. It operates by capturing video-based images of the iris, eliminating the need for physical contact or discomfort. This non-invasiveness enhances user acceptance and ensures a pleasant experience during the authentication process.

GDPR Compliance and Iris Biometrics

Data protection regulations, such as the General Data Protection Regulation (GDPR), play a crucial role in ensuring the privacy and security of individuals' personal data. Adopted in 2016 and enforceable since 2018, GDPR applies to any organization that collects data on individuals living within the European Union, regardless of the organization's location. Iris biometrics align well with GDPR requirements as they

are considered opt-in biometrics. They cannot be taken without the individual's consent, ensuring that permission is actively given before enrollment.

Iris ID's iris recognition algorithm captures and stores encrypted templates of individuals' iris patterns, making it impossible to regenerate the original images. This encryption ensures the privacy and security of personal biometric data. Additionally, iris templates can be securely stored on smart cards, passports, or other tokens, providing two-factor authentication, and giving individuals more control over their biometric data.

Real-World Applications

CERN-The European Organization for Nuclear Research

CERN, the European Organization for Nuclear Research, is renowned as the world's leading particle physics laboratory. Located near Geneva on the Swiss-French border, CERN plays a crucial role in advancing our understanding of subatomic particles and the fundamental laws of nature. In addition to its groundbreaking scientific discoveries, CERN also prioritizes the safety and security of

its international scientists, staff, and valuable research data.

CERN's security team faced the critical task of maintaining the safety and security of its diverse workforce, irreplaceable research data, and high-value assets. With a database of over 10,000 registered individuals, CERN needed an access control solution that was accurate, efficient, and reliable. The primary challenges included:

1. Managing a large database of scientists and staff identities.
2. Controlling access to CERN's underground facilities.
3. Protecting worker safety by limiting access to hazardous areas.
4. Ensuring scalability to accommodate future facility expansions.

After an extensive study of available access control options in 2008, CERN chose to implement an iris-recognition system provided by Iris ID. This cutting-edge technology replaced the existing fingerprint readers, offering improved identity authentication. The iris-based system was not only faster and more accurate but also deemed to be more hygienic, making it ideal for large-scale applications.

CERN's adoption of iris recognition technology has revolutionized access control at the world's foremost particle physics laboratory. The implementation of the Iris ID system has not only enhanced security and safety but also streamlined the movement of personnel within CERN's facilities. With its non-contact, efficient, and highly accurate authentication process, the iris recognition system has proven to be a game-changer for CERN's access control requirements.

As CERN continues to push the boundaries of scientific research and technological advancements, the organization remains committed to maintaining the utmost level of security and safety. The successful collaboration between CERN and Iris ID Systems Inc serves as a testament to the power of innovative solutions in ensuring the smooth functioning of scientific institutions of global significance.

Through its pioneering work in particle physics research and technological innovations, CERN continues to inspire generations of scientists and shape our understanding of the universe. With the implementation of cutting-edge technologies like iris recognition, CERN is leading the way toward a safer, more secure, and more connected future.

Google Data Centers

Google, known for its high-security and efficient data centers, has been utilizing IrisAccess for access control since 2006. These data centers operate 24/7 and store vast amounts of data across multiple locations worldwide. Iris recognition technology has been integrated with multiple existing access control systems at Google data centers across the United States and Europe. This integration highlights the trust placed in iris recognition for securing critical infrastructure spaces.

Not only at Google Data Centers but also at many other high-tech companies' data centers and industry-leading banks and service providers use iris recognition technology to protect their critical infrastructures. Some of them are listed as, Microsoft, Apple, Citi Group, Cisco, NYSE, Saudi Aramco, Exon Mobile, Rolex, etc.

Airports

Iris recognition biometric technology is proven to increase security, speed, accuracy, and user satisfaction when used as an access control solution within the aviation industry. Airport staff, and federal, local, and international agencies depend on the tools they must process large numbers of people in and around airports and as they leave and enter destinations in the US and globally. Iris technology is already in use at hundreds of airports globally. Iris recognition technology is a field-tested resolution that provides highly reliable authentication as well as numerous advantages.

Conclusion

In conclusion, iris recognition technology offers unparalleled advantages for securing critical infrastructure spaces. Its reliability, stability, uniqueness, flexibility, and non-invasiveness make it a compelling choice for access control in environments where safety and security are paramount. Iris ID's IrisAccess platform, coupled with the iCAM 7S series iris recognition reader, provides a robust and efficient solution for critical infrastructure spaces. With GDPR compliance and the ability to seamlessly integrate into existing security systems, iris recognition is poised to continue revolutionizing access control in the modern world.

For more information about iris recognition technology and several use cases globally, please contact Seyit Ali KAYA, Regional Manager of Iris ID Systems Inc.

Critical Infrastructure: Commission proposes a Blueprint to improve response to disruptive cross-border incidents

The European Commission is proposing a Council Recommendation for a Critical Infrastructure Blueprint that will enhance the EU's coordination in response to attempts to disrupt our critical infrastructure.

The geopolitical context in which critical infrastructure operates is highly volatile and this not only in view of Russia's war of aggression against Ukraine, increased hybrid attacks and the sabotage of the Nord Stream gas pipelines. Citizens, businesses and authorities in the EU rely on critical infrastructure because of the essential services that the entities operating such infrastructure provide. Such services are crucial for the maintenance of vital societal functions and must be provided in an unobstructed manner in the internal market.

The EU has already taken a number of measures to enhance the protection of critical infrastructure to avoid or mitigate the effects of disruptions in the essential services. Immediately after the sabotage of the Nord Stream gas pipelines, the Commission proposed a Council Recommendation to accelerate the work to protect critical infrastructure, proposing to enhance coordination in the response to incidents and crises with a Critical Infrastructure Blueprint. Moreover, the EU-NATO Task Force on resilience of critical infrastructure, launched in March 2023, presented on 29 June a final assessment report which maps out the current security challenges and presents targeted recommendations to strengthen critical infrastructure resilience. Today's proposal builds

on these actions, and further complements existing EU-level crisis instruments. It also complements the existing Blueprint in the area of cybersecurity and the EU Protocol for countering hybrid threats.

Scope and objective of the Critical Infrastructure Blueprint

In order to ensure a targeted, proportionate and effective approach, the Blueprint, provides a roadmap with measures that can be applied when Member States are faced with significant critical infrastructure incidents.

The Blueprint aims to achieve three main objectives in response to a significant critical infrastructure incident:

- **Improve shared situational awareness**, by better understanding the significant critical infrastructure incident in the Member States, its origin, and its potential consequences for all key stakeholders at operational and strategic/political level.

- **Ensure coordinated public communication** to minimise discrepancies in the messages conveyed to the public after a significant critical infrastructure incident. Clear public communication is also important to tackle disinformation.

- **Provide effective response** by strengthening the response of Member States and cooperation between Member States and with relevant Union institutions, bodies, offices, agencies, will mitigate the effects of a significant critical infrastructure incident and enable swift reestablishment of essential services.

The Blueprint can be applied when:

(i) the incident has a significant disruptive effect to or in six or more Member States;

(ii) the incident has a significant disruptive effect in two or more Member States, and timely policy coordination in the response at Union level is required, due to the incident's wide-ranging and significant impact of technical or political relevance.

To respond to the significant critical infrastructure incident, the Blueprint sets out several actions that can be taken at EU level, such as the support of the affected Member States through information exchange, the organisation of expert meetings, the preparation of situational awareness reports, and the coordination of public communication lines and of the response. The coordinated response may also include technical support of other Member States or relevant EU institutions, bodies and agencies, if so requested by the affected Member States, and activation of EU crisis coordination mechanisms and use of EU instruments. Points of contact for matters relating to the Critical Infrastructure Blueprint are foreseen for all actors involved. Member States affected by the significant critical infrastructure incident will share with the rotating Presidency of the Council and the Commission relevant information on the incident.

The Recommendation foresees that the Member States, the Council, the Commission and, where appropriate, the EEAS and relevant EU bodies, offices and agencies should apply the Blueprint without delay whenever a significant critical infrastructure incident occurs.

Background

The EU has had a legal and policy framework for the protection of critical infrastructure for almost 15 years. This has been updated with the Directive on Critical Entities Resilience (CER Directive), which entered into force in January 2023. In light of the current security context, a Council Recommendation on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure was adopted on 8 December 2022 following a Commission proposal. In that Recommendation, the Council highlighted, among others, the need to ensure at Union level a coordinated and effective response to risks to the provision of essential services. It invited the Commission "to draft a Blueprint on a coordinated response to disruptions of critical infrastructure with significant cross-border relevance".

Business Continuity and IT Disaster Recovery Resilience Goals

Doniella Mckoy is a certified business continuity professional with 10+ years' experience. She is a Lecturer at Rabdan Academy in the BCM and IEM department

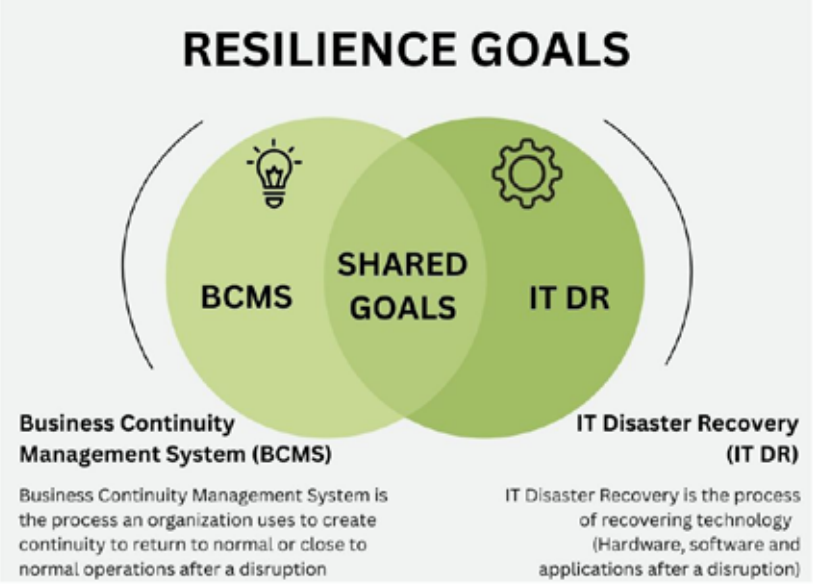
Under the pillar of resilience lies business continuity, born after technology recovery processes emerged in the 1970s. Continuity has been internationally recognized as a crucial part of private sector business and the public sector's ability to overcome disruptions and disasters. Almost a half century later, business continuity is still fighting for its own distinction from its predecessor, technology recovery. It is time to clearly define and promote the separation of skills needed for Business Continuity Management versus IT Disaster Recovery to create more resilient communities and business.

Doniella Mckoy

For several reasons, including climate change and our reliance on technology, the likelihood of business disruption has increased decade after decade. The cost of disruptions and disasters should not be ignored by the public or private sector. Organizations should implement a business continuity management system to include incident response, crisis communications and disaster

recovery (to name a few). The skills needed for business continuity management focus on business priorities identified through the business continuity life cycle. Technical leads and application owners contribute to the continuation of prioritized activities by helping to establish recovery timelines crucial to managing the expectations of a business recovery strategy. The business priorities are often not identified by the technical needs but based on impact ratings determined by the business continuity manager and top management. Though, some exceptions can be found if a company's main business is technology based.

As a certified business continuity practitioner from two international business continuity organizations that have professional practices or good practice guidelines, I have found no organization or standard where IT disaster recovery is mentioned as being interchangeable for business continuity. In fact, in these guidelines when it comes to technology and applications it is highlighted that practitioners should be concerned with the interdependence of technology and its role as a resource to complete the business continuity management lifecycle. This is because business continuity management require various skills without delving into the specific technical skills required for successful IT disaster recovery planning. We should be reminded that even in 2023 with the proliferation of software and applications needed for business it is possible a business continuity event does not require technical recovery.



With a lack of understanding from organizations, particularly individuals who create job descriptions for the continuity and recovery space I surmise they do not understand the value of creating separate positions for business continuity and technical recovery professionals. A general search for job descriptions that have a title related to business continuity often reveals tasks that are disaster recovery related requiring a high level technical expertise. I believe these roles should be separate but closely collaborate to contribute to the resilience of the organization.

Acknowledging the increased focus on cybersecurity could be a reason for the emphasis on technical and cyber skills but with such high (and relevant) concern it stands to warrant providing specific resources to address that risk. The idea that someone who has ten years' technical experience in recovering applications will be successful in business continuity planning is unfounded. The same can be said in the reverse that a business continuity planner with 10 years' experience is not the most qualified to do technical recovery.

Business continuity managers need to be able to talk technically to gain relevant information for risk identified but that does not mean they are experts in technology recovery.

Why are we cutting corners when it comes to resilience, especially with the price tags we have seen across the globe when it comes to response and recovery? The appropriate professionals should work together and have an understanding of these unique attributes of business continuity professionals and IT disaster recovery professionals to better support and obtain resilience goals of our organizations. Collaboration makes our recovery efforts stronger. We should not be replacing each other. I advocate for the separation of business continuity management and IT disaster recovery to human resources, hiring managers, and top management. We should avoid the continued disconnect on the difference of outputs between business continuity management and IT disaster recovery which can leave infrastructure and businesses vulnerable to internal and external risks.

Protecting Our Critical Infrastructure During Uncertain Times

The Science and Technology Directorate (S&T) look at a few examples of how we do our part to protects our nation's critical infrastructure from threats—both current and future—by developing and deploying innovative technology solutions.

Securing Our Infrastructure Against Cyberattacks

S&T is also developing and testing new technologies and tools designed to combat cyberattacks and their potential effects. S&T's Biometric and Identity Technology Center is partnering with the Transportation Security Administration and National Institute of Standards and Technology to create guidelines and regulations that enable the Department of Homeland Security to implement a secure digital identity ecosystem that facilitates the nationwide use and acceptance of mobile driver's licenses.

S&T's Critical Infrastructure Security & Resilience Research Program (CISRR) is collaborating with several government and laboratory partners on Critical-infrastructure Hardening Achieved Through Risk-reduction in Informational and Operational Technology, or CHARIOT, a project devoted to developing at-scale platforms for freight rail, and oil and natural gas pipelines. The platforms will test potential cyber threat-based scenarios that could disrupt system operations, identify potential vulnerabilities in relevant hardware and software components, evaluate new technologies being integrated into our transportation infrastructure, and develop mitigation strategies to harden these systems and components against potential cyberattacks.

Strengthening Our Anti-terrorism Initiatives

Preventing domestic terrorism is a cornerstone of our mission. As part of our efforts to deploy tools that keep us all safe, S&T's Physical Security program tested two cutting-edge security systems during the 2023 National Football League (NFL) Draft held at Union Station in Kansas City, Missouri, back in April (we have a podcast episode about this, too).

The CISRR-funded systems—the Ready Armor Protection for Instant Deployment Barrier and Deployable Expedient Traffic Entry Regulator—were deployed to help the NFL and local law enforcement protect the venue and event attendees from potential attacks via improvised explosive devices and vehicles. This live assessment provided valuable data to our team and will help us improve these systems in the near future.

Protecting Our Critical Infrastructure from Electromagnetic Pulse (EMP) and Geomagnetic Disturbances (GMD)

S&T is helping critical infrastructure owners and operators mitigate the effects of and recover from EMP/GMD events. One way we are doing this is through research to harden 4G and 5G communication infrastructure, assessing and evaluating the potential impacts of these events on our towers and antennas. Findings from these studies will empower owners and operators with crucial information regarding existing vulnerabilities and offer recommendations, best practices, and technology solutions that can better protect their 4G and 5G towers and antennas from potential EMP/GMD events.

Another way we do this within our own DHS family is by using EMP-protected shelters to protect the Federal Emergency Management Agency's Integrated Public Alert & Warning System (IPAWS) and its communications infrastructure. There are 77 IPAWS shelters nationwide.

Adapting to Our Changing Environment

As global temperatures rise, the frequency and severity of weather events have also been escalating. S&T is working to meet the challenges brought on by our changing environment through efforts like the Exploitation of Mesonets for emergency Preparedness and response in Weather Extremes Research initiative, or EMPOWER. EMPOWER is a pilot program supporting emergency providers that respond to weather-related disasters. It will integrate and leverage state-of-the-art analytics, real-time localized weather data, critical infrastructure lifelines, social vulnerability data, and novel visualization capabilities to provide responders with real-time assessments of changing weather conditions and potential impacts on communities and critical infrastructure.

Understanding and Improving the Safety of our Waterways

Our nation is surrounded by thousands of miles of shoreline and waterways. To ensure the safety of those who pass through these waters, S&T's Critical Infrastructure Resilience Institute Center of Excellence is assessing the efficacy of various navigation aids like buoys, beacons, and ranges that are used to mark shipping lanes, potential hazards, and protected areas in and around our shorelines, waterways, and seaports. This study is the first of its kind and will quantify the effectiveness and continuing necessity of these tools, especially as reliance on global positioning systems and other electronic navigation technologies has increased in recent years.

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

Critical Infrastructure Protection & Resilience Europe (CIPRE) took place on 3rd-5th October 2023 in Prague, Czech Republic, co-hosted by the Ministry of Industry & Trade of the Czech Republic and the International Association of CIP Professionals (IACIPP) and supported by the Tomas Bata University in Zlin and Technical University of Ostrava.

We take a look at the success of the conference and exhibiton and some of its highlights reported by John Donlon, Chairman of CIPRE.

It was a great honour to once again Chair the Critical Infrastructure Protection and Resilience Europe (CIPRE) conference in October this year in the beautiful city of Prague. This was the 8th CIPRE conference to be held in Europe. Last year we were hosted by our good friends from ICI Bucharest and earlier this year our connected event in North America took place in Baton Rouge.

CIPRE 2023 was co-hosted by The Ministry of Industry and Trade of the Czech Republic and held in one of their historic buildings in the heart of Prague city centre. It was a fantastic opportunity for networking and for gaining an insight into the current and future European initiatives that are being developed and delivered.

The conference provided some really excellent presentations by some very distinguished, experienced and professional people and those presentations in turn led to a range of great discussions around a whole host of infrastructure protection and resilience issues. There was also significant active participation from a lively, challenging and charming audience. Well, most of them were charming but you always get a few who might buck the general trend!

We were extremely fortunate to have some great support from a number of people and organisations, including:

- The Ministry of Industry and Trade
- The Association of Critical Infrastructure within the Czech Republic
- Martin Hromada from The Tomas Bata University in Zlín and
- David Rehak from The Technical University of Ostrava.

The conference got off to a great start on day one with the keynote session which was led by Rene Nedela representing The Ministry of Industry and Trade. Rene very proudly stated that he firmly believed that The Czech Republic was one of the safest countries in Europe with regards to the protection of its infrastructure. The Czech Government had invested heavily in this area and continued to do so. However, he provided a clear message that it was not all 'sunshine and roses' as he personally believed that as far as any countries infrastructure was concerned there was no safe place in a world which was constantly changing and with new threats emerging all the time.

Rene outlined how the Czech Government was committed to working with partners, both in country and internationally to provide safe and secure infrastructure for their citizens but he was very aware of the fact that although there was good cooperation in place, the State and private operators needed to work better together at solving problems.

The issue of Governments and the private sector enhancing levels of cooperation, communication and trust was a constant theme throughout the conference with one delegate summing it up when stating that we will never move forward on this issue unless we all double up and deliver on trust.

The other speakers within the keynote session included Brigadier Lieutenant-General Vladimir Vicek, the Director General of the Fire and Rescue System, Protection and Civil Emergency Preparedness in the Czech Republic and Adrian Victor Vevera, The General Director of the National Institute for Research and Development in Informatics -ICI-Bucharest, Romania.

Public and Private Partnerships (PPPs) and the sharing of timely and accurate information to allow relevant actions to take place underpinned a significant amount of the debates over the three days of the conference. As did the continual issue of silo working, both within organisations from a physical security and cyber perspective and also across Government and Agencies. It was quite concerning that there was a fair amount of evidence put forward around the lack of progress on PPPs.

However, it was not all doom and gloom. One of the delegates from the Joint Research Centre of the European Commission put forward two areas of good practice, the first being PCII - (have you noticed how everything around infrastructure has to have an acronym!) within the United States. Congress created the Protected Critical Infrastructure Information (PCII) Program under the Critical Infrastructure Information Act of 2002 (CII Act) to protect information voluntarily shared with the government on the security of private and state/local government critical infrastructure.

The second was TISN, The Trusted Information Sharing Network (TISN) which is the Australian Government's primary engagement mechanism with industry on critical infrastructure.

There were, as you would expect, a wide range of topics covered throughout the event. These included, climate change, natural disasters, emerging threats, risk management, interdependencies, communications, supply chains and of course cyber. The delegates heard a great

deal about the 'rise of the machines' and delved into the world of Artificial Intelligence and its use as both a defender and attacker of our infrastructures.

Space was also a popular topic, with it not being so much the final frontier as Captain Kirk first said 50 years ago when Star Trek first started, but now a rapidly emerging frontier. The concept of space as critical infrastructure is gaining prominence. That which was once the exclusive domain of governments and space agencies, has now become a bustling arena for commercial activities.

Other topics which were addressed included terrorism and Lone Wolves although there was not as much reference to these threats as I anticipated and yes we have seen a reduction in the number of attacks in the western world, but we have to remember that terrorism has not gone away. Also, there wasn't too many discussions around Russian cyber attack activity as it related to infrastructure in Europe and there was probably more talk around China. In fact, one delegate stated, 'Things change – just as all roads used to lead to Rome, now they lead to Shanghai or Beijing'.

The conference heard from several speakers about how quickly the world is changing and the impact that has on planning and preparation. In my opening address I spoke about how we are all living in unpredictable times and the need for those involved in the protection and resilience of infrastructure to continually change, adapt and innovate. I think one of the clear messages over the three days was around the speed at which events materialise and just how unprepared we are, at times, to respond them. Therefore, we have to remember that what we did yesterday may not be what we need to do today and tomorrow and as Albert Einstein famously said, 'We cannot solve our problems

with the same thinking we used when we created them'.

The final plenary session of the event was a deep dive into the current range of Horizon, the European Union Critical infrastructure Protection & Resilience (EU-CIP) projects and research programmes. An overview of the whole programme was delivered by the EU-CIP Project Coordinator and this was followed by an insight into four of the individual projects:

- SATIE Project
- Sunrise Project
- CyberSEAS Project and the
- PARADeS Project.

These presentations were excellent demonstrating the professionalism and effort going into a range of activity designed to enhance the understanding and development of European wide policies and good practice as they relate to critical infrastructure.

Overall, this was a great event. We had over 130 delegates registered from 31 countries and from the feedback we have received they all went home having found the event to have been hugely enjoyable, educational and of real value to them.

The next conference, Critical Infrastructure Protection and Resilience North America (CIPRNA) will take place in Lake Charles, Louisiana next March with the European event, CIPRE being located in Madrid in November 2024. I look forward to seeing you at one, if not both of these events next year.

John Donlon QPM FSyI
Chairman
CIPRE

Australia's cybersecurity strategy focuses on protecting small businesses and critical infrastructure

The Australian federal government has released the 2023-2030 Australian Cyber Security Strategy with a focus on protecting the country's most vulnerable citizens and businesses. At first glance, the strategy covers a lot of ground, and the government will need to work hard and fast to ensure some of all the actions proposed are put in place before the next big breach.

As previously reported, the cyber strategy is based on the idea of six cyber shields to provide an additional layer of defence against cyber threats. These shields aim to create strong businesses and citizens, safe technology, world-class threat sharing and blocking, protected critical infrastructure, sovereign capabilities and resilient region and global leadership. "I don't believe that the programs described in the first 'shield' (strong citizens and business) can either be operationalised, or for programs that do already exist, be scaled up to deliver within a meaningful timeframe. While I have significant general concerns regarding the wholly inadequate funding for the 2030 strategy, these concerns become particularly relevant with respect to this first 'shield'," KordaMentha executive director, cybersecurity Tony Vizza told CSO.

On top of $2.3 billion already being spent on cybersecurity, the government has committed $586.9 million to execute the seven-year strategy. The Australian cybersecurity strategy has most, if not all, aspects of cybersecurity covered although there are a lot of things to focus on and the timelines for the delivery of each is not clear.

NATO report on Protecting Critical Maritime Infrastructure

Critical infrastructure in the maritime domain facilitates the continuous delivery of basic services such as energy and communication, particularly the internet. The importance of these networks has dramatically increased in recent years, yet the responsibilities for protecting and regulating them have become less clear.

The need for action is in large part driven by technology. Seabed activities are transforming rapidly due to the proliferation of undersea technology such as remotely operated devices capable of conducting sophisticated operations deep under water. These advancements provide new possibilities for defence, but also enable adversaries to capitalise on existing vulnerabilities. 'Seabed warfare' is no longer a distant concept: it represents an immediate and legitimate threat to Allies.

Further complicating the issue, the majority of maritime infrastructure is controlled or operated by private entities, rendering protection, threat detection, and regulation of these vital networks even more complex.

For too long, this essential equipment has been increasingly utilised yet insufficiently surveyed, protected, and regulated. Although some Allied governments are working to patch vulnerabilities, particularly following the Nord Stream sabotage, additional effort, investment, and coordination are urgently needed. The paper deals with critical maritime infrastructure in general. However, the focus of the report is primarily on the challenges to the Allied underwater critical infrastructure.

Download the report at https://www.nato-pa.int/download-file?filename=/sites/default/files/2023-10/032%20STC%2023%20E%20rev.%202%20fin%20-%20CRITICAL%20MARITIME%20INFRASTRUCTURE%20-%20FRIDBERTSSON%20REPORT1.pdf

Office of Bombing Prevention Recognizes Critical Infrastructure Security and Resilience Month

With an evolving threat landscape, infrastructure security remains a priority at all levels of government and the private sector. November kicks off Critical Infrastructure Security and Resilience Month, and the Cybersecurity and Infrastructure Security Agency (CISA) is highlighting how critical infrastructure stakeholders can "Resolve to be Resilient" through proper planning. This month's resiliency campaign highlights the integration of processes and practices into a response plan that anticipates disruption to infrastructure and reduces recovery time.

Some keys to safeguarding our infrastructure include preventing, protecting against, responding to and mitigating the use of explosives against both public and private sectors, which is the mission of CISA's Office for Bombing Prevention (OBP). According to the 2022 Explosives Incident Report (EIR), a joint product between CISA and the United States Bomb Data Center, 2,538 bomb threats were reported in 2022—a 35% increase from 2021. The EIR also revealed a 23% increase in explosion incidents between the two years (from 785 to 966).

As part of this month's designation, CISA OBP is engaging with stakeholders nationwide on the impact of bombing incidents and threats to critical infrastructure. This effort includes training and resources to reduce the risk of an attack. CISA OBP's approach improves capabilities to protect critical infrastructure, which spans everything from healthcare, water, and education to chemical, transportation systems, energy and much more.

CISA OBP's Associate Director Sean Haglund reminds us, "Part of our society's collective benefit is the protection and resiliency of critical infrastructure. While we cannot guarantee that an attack will never take place, we can work to minimize the potential impact through proper planning and coordination." He adds, "Mitigating risk to our nation's infrastructure is a fundamental component of national security."

Identifying future critical technologies for space, defence and related civil industries

The EC's Joint Research Center's report presents the findings of a participatory technology foresight exercise that listed 46 emerging and disruptive technologies relevant for space, defence, and related civil industries, which are of strategic importance for the European Union (EU).

Throughout the process, participants focused on four future critical technologies that deserve particular attention: (i) quantum communications and cryptography; (ii) space platform; (iii) integrated photonics; and (iv) nuclear micro-reactors. These future critical technologies bear a high level of impact and a high probability of future EU dependency on others. For each one, the report includes a series of recommendations to address risks, challenges and future dependencies.

Beyond the listing and analysis of key technologies, the authors summarised 10 clusters of topics related to technology development and adoption: (i) geopolitics; (ii) cooperation; (iii) investment; (iv) market; (v) skills and knowledge; (vi) ethical issues; (vii) regulations and standards; (viii) development of technology building blocks; (ix) twin transition and security of assets; and (x) data and communications.

These insights can support further research and policy developments. The report concludes with a detailed explanation of the methodology applied and the results of intermediary phases.

Fortifying Defence: Strengthening Critical Energy Infrastructure against Hybrid Threats

The European security order is undergoing a fundamental transformation, where hybrid threats will likely increase. In this context, this study aims to respond to the evolving geopolitical landscape and provide the Ministries of Defence (MoDs) with a more comprehensive conceptual basis to facilitate the development of the necessary measures to counter hybrid threats. This will enhance the resilience of critical energy infrastructures (CEI) on which the defence sector depends for its well-functioning.

To ensure EU-wide coherence, this study follows the conceptual framework on hybrid threats and the comprehensive resilience ecosystem (CORE) model developed by JRC and the Centre of Excellence for Countering Hybrid Threats in Helsinki (HCoE). Thus, it focuses on (sub)domains for identifying defence-related CEI interdependencies and investigating the tools that adversaries could employ to undermine their performance.

In addition, this document provides MoDs and other stakeholders with recommendations for increasing the resilience of defence-related CEI against hybrid threats by promoting civil-military collaboration at the EU level, raising awareness, sharing best practices, stimulating discussion and triggering critical thinking on how to maintain the energy supply and thus safeguard military performance.

Commission adopts a Delegated Act establishing a list of essential services

The Commission adopted a Delegated Regulation establishing a non-exhaustive list of essential services based on the sectors identified by the CER Directive.

Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER Directive) and repealing Council Directive 2008/114/ EC entered into force on 16 January 2023. The CER Directive aims at ensuring that services essential for the maintenance of vital societal functions or economic activities are provided in an unobstructed manner in the internal market and that the resilience of critical entities providing such services is enhanced.

In particular, the CER Directive provides for obligations on Member States to carry out risk assessments and identify those critical entities that provide essential services. In this context, pursuant to Article 5 of the CER Directive and in accordance with the conditions laid down in Article 23 of the Directive, the Commission was empowered to adopt a delegated act in order to supplement the Directive, by establishing a list of essential services in the sectors and subsectors set out in the Annex to the Directive. This list will be used by competent authorities, in accordance with the CER Directive, for the purpose of conducting risk assessments and thereafter to identify critical entities pursuant to the Directive.

EU cybersecurity exercise: foster cooperation, secure free and fair EU elections

To evaluate and strengthen current working methods ahead of the 2024 elections, EU institutions organised a cybersecurity exercise.

National and EU partners tested their crisis plans and possible responses to potential cybersecurity incidents affecting the European elections.

The exercise is part of the measures being implemented by the European Union to ensure free and fair elections in June 2024. It took place in the European Parliament and was organised by the European Parliament's services, the European Commission and the EU Agency for Cybersecurity (ENISA). The drill allowed participants to exchange experiences and best practices, and will help them enhance their capacity to respond to cybersecurity incidents as well as to contribute to the update of existing guidelines and good practices on the cybersecurity of technology used in the election process.

Representatives from national electoral and cybersecurity authorities, together with observers from the European Parliament, the European Commission, CERT-EU and the EU Agency for Cybersecurity (ENISA), participated in the second edition of the exercise.

While the main responsibility for protecting the integrity of the elections lies with EU Member States, this exercise helped fine-tune their common preparedness when facing potential cyber and other hybrid threats and their ability to swiftly develop and maintain situational awareness at national and EU level if a serious cybersecurity incident were to occur.

All is in place to ensure that European citizens can trust the EU electoral process. Risks to elections can take various forms from information manipulation and disinformation to cyber-attacks that compromise infrastructures.

Enhanced EU-Ukraine cooperation in Cybersecurity

The European Union Agency for Cybersecurity (ENISA) has formalised a Working Arrangement with Ukraine counterparts focused around capacity-building, best practices exchange and boosting situational awareness.

The partnership was signed by ENISA, the National Cybersecurity Coordination Center (NCCC) and the Administration of the State Service of Special Communications and Information Protection of Ukraine (SSSCIP) on the Ukrainian side.

This arrangement is broad in nature and covers short-term structured cooperation actions, while paving the way for a longer-term alignment of cybersecurity policies and implementation approaches. Cooperation will be sought in the areas of:

- Cyber Awareness & Capacity Building to enhance cyber resilience: including facilitating the participation as third country representatives in specific EU-wide cybersecurity exercises or trainings, possible secondment arrangements, and the sharing and promotion of cyber awareness tools and programmes.

- Best practice exchange to ensure alignment of legislation and implementation; including on key cyber legislation implementation such as NIS2, and sectors such as telecommunications and energy.

- Knowledge and information sharing to increase common situational awareness: including a more systematic sharing of knowledge and information in relation to the cybersecurity threat landscape to increase the common situational awareness to the stakeholders and communities.

A work plan will operationalise the Working Arrangement.

Piloting New Ground: Expanding Scalable Cybersecurity Services to Protect the Broader Critical Infrastructure Community

In recent years, cyber attacks have intensified in both volume and impact–affecting the day-to-day operations of organizations across our nation's critical infrastructure sectors. When most Americans consider the cyber-physical impact of attacks on critical infrastructure, they may recall when a ransomware attack on Colonial Pipeline's corporate network led to a disruption of fuel supplies to gas stations along the East Coast. More recently, advanced actors such as Volt Typhoon have demonstrated the intent and technical ability to disrupt our critical infrastructure. These types of cyber attacks have the potential to disrupt critical functions on which we all depend, and in the worst cases, lead to the loss of human life.

In response to this evolving threat environment, CISA is excited to announce a pilot program designed to deliver cutting-edge cybersecurity shared services on a voluntary basis to critical infrastructure entities that are most in need of support. CISA has acted as a managed service provider to the federal civilian government for years and observed significant risk reduction along with the benefits of cost-savings and standardization. Leveraging a new authority provided by Congress, we are eager to extend our support and enterprise cybersecurity expertise with non-federal organizations that require additional assistance to effectively address cybersecurity risks.

Scaling CISA-managed cybersecurity services for the segments of our critical infrastructure community that need it most is a cost-effective way to gain greater insight into our evolving threat environment, establish a common baseline of cyber protection, and, most importantly, reduce the frequency and impact of damaging cyber events.

Last month, CISA began deploying our Protective Domain Name System (DNS) Resolver to pilot participants which, until now, had only been available to federal civilian agencies. It is a proven, cost-effective solution that uses U.S. government and commercial threat intelligence to prevent systems from connecting to known or suspected malicious domains. Since 2022, CISA's Protective DNS service has successfully blocked nearly 700 million connection attempts from federal agencies to malicious domains across the globe and continues to reduce the risk of the most common cyber risks like ransomware, phishing and malicious redirects.

Unlocking Tomorrow's Cybersecurity: A Sneak Peek into ReadySetCyber

In the fast-paced world of cybersecurity, staying ahead of threats is essential. And while security is without a doubt a priority for businesses of all sizes, it is easy to feel overwhelmed by all the information available. At CISA, we have been diligently developing a solution aimed at simplifying the way our partners and potential collaborators understand their cyber risk and prioritize their investments, ensuring they can quickly navigate this complexity with ease. Our focus has been on making the process of working with us more intuitive and user-friendly so that every organization can spend more time meeting business goals and less time sifting through cybersecurity resources. We believe this approach will be especially helpful for smaller to medium sized stakeholders with fewer resources, who need help prioritizing actions to help them to reduce the likelihood and impact of damaging intrusions.

In early 2024, we look forward to launching a new way for organizations to understand their cyber risk and receive targeted, straightforward guidance built around our Cybersecurity Performance Goals. This new tool is called ReadySetCyber. While we're not quite ready to unveil all the details just yet, we are excited to share a glimpse of what's on the horizon.

ReadySetCyber will simplify the process of incorporating cybersecurity into your organization's business decisions, regardless of your level of expertise or the number of IT personnel you have on staff. Instead of making cybersecurity a daunting challenge, with the ever-present question of where to invest next, prioritization decisions become a guided, step-by-step process on a user-friendly interface accessible to organizations of all sizes. By providing tailored resources and insights in a streamlined format, ReadySetCyber will empower users to align scarce resources with the most impactful cybersecurity measures for their organization.

AXIS Object Analytics now offers occupancy in area and crossline counting

Axis Communications announces a new release of AXIS Object Analytics including the scenarios Occupancy in area and Crossline counting. Occupancy in area counts objects within an area so users can estimate occupancy levels in real-time.

Crossline Counting counts whenever a human, vehicle, type of vehicle, or both cross a virtual tripwire in a defined direction. Data is easily accessed in real-time and can be integrated into third-party applications for easy overviews and actionable insights.

AXIS Object Analytics comes preinstalled on compatible Axis network cameras adding value at no extra cost. It uses AI-based algorithms and behavioral conditions to analyze the scene and spatial behavior of the objects within, ignoring common irrelevant sources of unwanted events. Designed to enable proactive monitoring, users can focus only on objects of interest and events that need attention and collect data to access actionable insights. Scenarios can be set up and tailored to specific monitoring needs with just a few clicks and multiple scenarios can run simultaneously. The application intelligently monitors the scene to determine if and when an event should be triggered when selected objects are detected.

This scalable, edge-based analytics processes and analyzes live video directly on the camera This improves data processing time and minimizes bandwidth and storage requirements. Furthermore, using the camera's event management system it integrates with AXIS Camera Station and all other major video management systems.

Simultaneous In-band Active & Passive Sonar (SInAPs) Goes Mobile

There is no doubt that as technology advances, whatever sector it may be in, not a week goes by without new and improved products launching onto the market. While this is very exciting, potential threats to our security are also evolving at the same pace.

Whilst developing this latest generation of our Sentinel Intruder Detection Sonar, our analysis of the rapidly evolving drone threat led us to the conclusion that it had to be more than just an incremental upgrade of the previous versions of Sentinel, the world's most deployed Intruder Detection Sonar. We should try, as part of this development, to take advantage of potential gains provided by passive processing but crucially without compromising the existing active performance. Subsequently we developed SInAPS®.

Simultaneous In-band Active and Passive Sonar, SInAPS, combines the existing active system with a new passive tracking capability which tracks the target by listening to the noise it is emitting. This is highly innovative and uses the same array for both active and passive processing simultaneously.

SInAPS has the unique advantages of:

- Retaining the processing gain of the Sentinel array, with over 30 dB higher than a single hydrophone sensor, and dramatically enhancing passive signal to noise ratio (SNR).
- Retaining the high bearing resolution associated with operating at higher frequencies with no need for a distributed sensor network.
- Guaranteeing spatially co-registered tracking between active and passive sub-systems from a point sensor.
- Avoiding the need for the system to be switched 'optimally' between active and passive operating modes.
- Finally, and crucially, it retains the performance of the system's active mode without being compromised.

HID and CERTIFY Health Deliver Advanced, AI-Powered Patient Verification Technology to the Healthcare Industry

HID has announced a new collaborative patient engagement and facial recognition offering designed to evolve healthcare operations and administer impactful, elevated patient service at every checkpoint.

HID combines its leading U.ARE.U™ Camera Identification System featuring highly accurate facial recognition capabilities with CERTIFY Care – a state-of-the-art patient engagement platform currently in use across major healthcare organizations. Key functionalities include patient onboarding, biometric authentication, patient communications, digital forms, appointment scheduling and management, and payment collection.

Webcams are not enough when it comes to reliable patient verification in healthcare today. The risk of misidentification is high – leading to potentially fatal results for patients and crippling repercussions across companies. HID's U.ARE.U Camera Identification System fuses AI with multispectral imaging (MSI) technology and modern machine learning algorithms to accurately identify and authenticate individuals. The CERTIFY Care platform integrates the U.ARE.U Camera technologies to deliver accurate patient authentication and identification while facilitating an excellent end-to-end patient experience from intake to claims payout. It's all anchored by the precision of face biometrics.

In addition to faster time to revenue, this technology pairing benefits healthcare practices by enabling:

- Positive patient identification

- Accurate medical records management and deduplication

- Medical fraud prevention and investigation

- Touchless, hygienic authentication

Milestone Systems announces Milestone Kite™ Camera to Cloud

Milestone Systems, a leading provider of video technology, announced the release of a new camera-to-cloud deployment option for its Milestone Kite video surveillance as a service (VSaaS) software. Known as Milestone Kite Camera to Cloud, the new option will offer even greater simplicity and cost-efficiency to customers.

As an alternative or expansion to gateway installations, Camera to Cloud builds on Milestone's focus on flexible and scalable solutions that support evolving needs.

Milestone Kite Camera to Cloud VSaaS works with a series of Axis cameras pre-installed with AI-based Axis Object Analytics. All computing, recording and video storage take place on the cameras, which connect directly to the Milestone Kite cloud. This can reduce bandwidth load and associated costs, as well as installation and maintenance costs.

"The combination of simplicity and cost efficiency makes Milestone Kite Camera to Cloud a highly practical choice for organizations with smaller or newly built locations, or simply those where having a gateway onsite would be impractical," says Jesper Just Jensen, VP Products at Milestone Systems.

Camera to Cloud is particularly suitable for businesses with multiple locations with a small number of cameras at each site. It is also beneficial for those with limited IT knowledge, bandwidth limitations or situations where installing on-site gateway hardware is not feasible.

Companies already using Milestone Kite with gateways can expand to new sites with Camera to Cloud. The new sites will be recognized and managed as part of the same Kite service as the gateway deployments.

This enhances the appeal of Milestone Kite as a suitable option for different budget and bandwidth situations, making Camera to Cloud a practical choice for businesses with multiple sites."

Mobile Access from Bosch uses smartphones instead of plastic cards

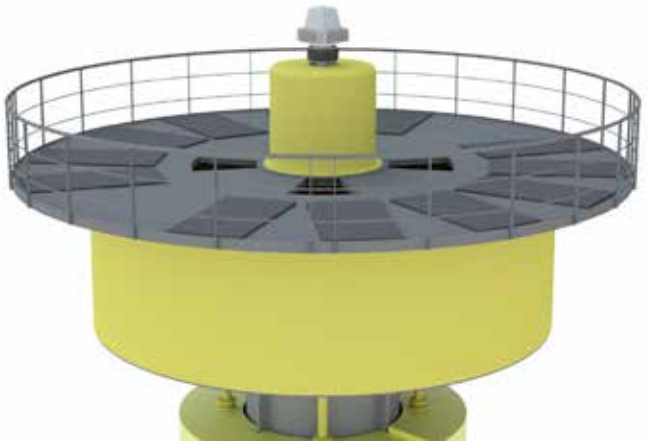
Thanks to Mobile Access, the new solution from Bosch, access to buildings and restricted areas can now be managed without additional identification media such as plastic cards.

Mobile Access is fully integrated into the tried-and-tested Access Management System from Bosch and offers numerous benefits in terms of efficiency, security, and convenience for building owners, employees, and visitors.

A few clicks are all it takes for authorized individuals, such as Facility Management or IT staff, to configure and create access authorizations in their local Access Management System. Visitor and employee data can then be managed with ease using an intuitive, browser-based interface. For example, authorization credentials can be sent remotely and easily as a link or a QR code to an app on the end users' mobile devices and can then be deleted again as necessary. "Most people always carry their smartphones with them everywhere they go. Storing authorization credentials on mobile devices has several advantages," explains Gregor Schlechtriem, Senior Vice President at Bosch Building Technologies, adding: "You provide both employees and visitors with a modern, easy-to-use, and sustainable solution that means they don't have to resort to additional forms of identification like plastic cards. Using the appropriate settings, they don't even have to take their smartphone out of their pocket. The app can run in the background once started, so the smartphone's home screen doesn't have to be unlocked to open doors." This solution also enhances accessibility, and is a major advantage for wheelchair users, for example, who are often unable to reach card reader machines.

DeTect Announces Development of Stabilized True3D™ Bird Radar for Offshore Wind Project Bird Surveys

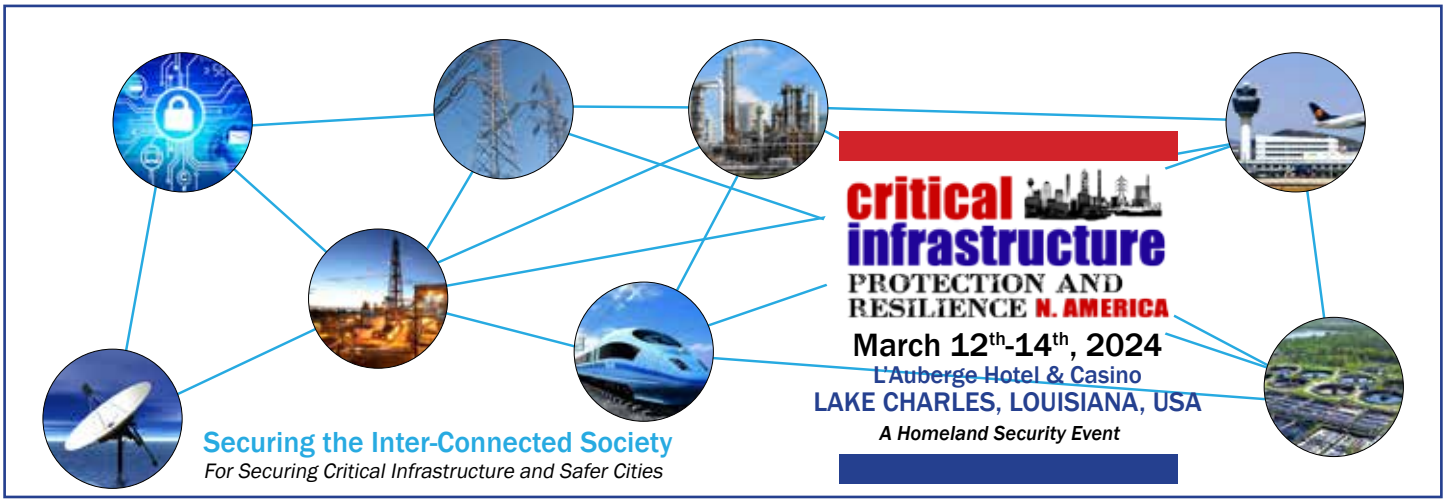
DeTect, Inc. announced it has developed a motion-stabilized True3D Bird Detection Radar (BDR) to support buoy and floating platform offshore wind farm project development and operation.



The MERLIN™ 7360s is based on DeTect's industry-proven MERLIN True3D bird radar technology and includes motion stabilization platform and software to compensate for wave and buoy movement. The system is currently in final testing at DeTect's Panama City, Florida headquarters before undergoing certification testing off the French coast in early 2024.

"The 7360s represents a breakthrough in offshore avian mortality risk assessment, monitoring and mitigation technology allowing wind farm developers and operators to conduct quantitative pre-construction risk assessment of proposed offshore wind projects and mitigate bird mortality in real-time", said Gary W. Andrews, DeTect's President and CEO.

The 7360 additionally includes DeTect's Artificial Intelligence (AI) target classification technology that automatically identifies birds and bats down to taxonomic (species) levels while collecting continuous high resolution data on biological activity 24-7, day and night. The system is compact, lightweight, low power and fully remote controllable, designed for extended unattended operation on metrological buoys and platforms. The 7360s will be commercially available by mid-2024.



ADVERTISING SALES

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

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

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

Sam Most
Rest of World
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

World Border Security Congress

24TH-26TH APRIL 2024
ISTANBUL, TURKEY

www.world-border-congress.com

Where East Meets West - Developing Border Strategies Through Co-operation and Technology

INVITATION TO ATTEND - REGISTER ONLINE TODAY

You are invited to attend the 2024 World Border Security Congress
Register online at www.world-border-congress.com/registration

Turkey is a transcontinental country, strategic positioned linking Europe, Asia and the Middle East, making it a perfect route for trade.

With a total border boundary of some 4,000 miles, about three-quarters is maritime, including coastlines along the Black Sea, the Aegean, and the Mediterranean, as well as the narrows that link the Black and Aegean seas.

The 'EU-Turkey deal', a 'statement of cooperation' between EU states and the Turkish Government, means Turkey can take any measures necessary to stop people travelling irregularly from Turkey to the Greek islands, and currenlty manages over 5 million migrants and refugees.

Turkey is a top destination for victims of human trafficking, as well a global trafficking hub for South American cocaine, fuelling rising demand for the drug in Eastern Europe and the Persian Gulf.

Many challenges face the region, which impacts globally, and therfore, an excellent place for the hosting of the next World Border Security Congress.

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.

We look forward to welcoming you to Istanbul, Turkey on 24th-26th April 2024 for the next gathering of border and migration management professionals.

www.world-border-congress.com

CONFIRMED SPEAKERS INCLUDE:

- AEAC Diane Sabatino, Acting Executive Assistant Commissioner (AEAC) for the Office of Field Operations (OFO), US CBP
- Amanda Read, National Operational lead, Safeguarding & Modern Slavery, UK Border Force
- Ana Cristina Jorge, Director of Operational Response Division of the European Border and Coast Guard Agency – Frontex
- Austin Gould, Assistant Administrator for Requirements and Capabilities Analysis, Transport Security Administratio
- Colleen Ryan, Border Advisor, Border Security & Management Unit, Transnational Threats Department (TNTD),OSCE
- Dr Maria Carmela Emanuele, Customs Officer -Chemist, Italian Customs and Monopolies Agency
- Emmanuel Oshoba, Deputy Comptroller of Customs, Nigeria Customs Service
- Guido Ferraro, Project Manager, Joint Research Centre, European Commission
- Iliuta Cumpanasu, Lead Evaluator, FRONTEX
- LTC Marcos Pérez-Mayor Rodríguez, Chief of Staff of the Border and Customs Police Command, Guardia Civil, Spain

Full Speakers at www.world-border-congress.com/speakers

for the international border management and security industry

Supported by:

Media Partners: