critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

SUMMER 2023
www.cip-association.org

FEATURE:
Beyond Physical Protection

FEATURE:
Hybrid Threats – A Comprehensive Resilience Ecosystem

FEATURE:
Using the EU Space Programme for disaster risk management in Hungary

THE CNI / CROWDED PLACES SECURITY DEBATE

critical infrastructure PROTECTION AND RESILIENCE EUROPE

3rd-5th October 2023

Prague, Czech Republic

www.cipre-expo.com

Co-Hosted by:

International Association of CIP Professionals

MINISTRY OF INDUSTRY AND TRADE OF THE CZECH REPUBLIC

Tomas Bata University in Zlín Faculty of Applied Informatics

VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF SAFETY ENGINEERING

INVITATION TO PARTICIPATE

Securing the Inter-Connected Society

Registration Open - Early Bird Delegate Fees apply

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

Learn more about the importance of the updated NIS2 Directive and implementing the upcoming CER Directive.

The European Commission has adopted a communication on Critical Infrastructure Protection in the fight against terrorism, enhancing European prevention, preparedness and response in the event of terrorist attacks involving critical infrastructures.

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

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

Join us in Prague, Czech Republic, for the next leading discussion on securing Europe.

Register online at www.cipre-expo.com.

Leading the debate for securing Europe's critical infrastructure

Confirmed Speakers include:

- Martin Sveda, Head of the Private Sector Regulation Unit National Cyber and Information Security Agency
- Lieutenant-General Vladimir Vlcek, Ph.D., MBA, Director General Fire Rescue Service of the Czech Republic
- Frédéric Petit, Ph.D., Project Officer European Commission Joint Research Centre, Italy
- Ing. Jindrich Sip MBA, Head of Business Continuity Management CEZ, a. s., Czech Republic
- Dr. Eng Adrian Victor Vevera, General Director National Institute for Research and Development, Informatics ICI Bucharest, Romania
- Frantisek Paulus, Director General Directorate of Fire Rescue Service, Population Protection Institute, Czech Republic
- Ivana Cesarec, Head of Critical Infrastructure and Cultural Heritage Department Ministry of the Interior, Civil Protection Directorate, Croatia
- Dr. Sandeep Pirbhulal, Senior Research Scientist Norwegian Computing Centre, Norway

See www.cipre-expo.com for speakers

Supporting Organisations:

Asociace kritické infrastruktury České republiky

EE-ISAC

TSIME

CoESS

PESI Plataforma Tecnológica Española de Seguridad Industrial

EU-CIP

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

Help2Protect

IET.tv

NS&RC

ISIO

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Space is the next cybersecurity frontier

U.S. officials are increasingly turning their attention to how best to keep spies and hackers out of the country's space systems — especially as private industry continues to play a bigger role in their development.

Driving the news: Intelligence officials issued a warning Friday that foreign spies could be targeting commercial space firms.

- The advisory — which came from the National Counterintelligence and Security Center, the FBI and the Air Force — says adversaries could target these companies to siphon intellectual property, collect sensitive data related to satellite payloads, or exploit supply chain dependences.

- However, the two-page advisory doesn't identify what inspired the warning or which countries are likely to be behind these attacks.

The big picture: U.S. officials have long worried about how to properly secure the growing space industry, especially as more private space companies take on missions of national significance.

- The space business — which is set to become a $1 trillion industry by 2030 — is about more than just the flashy, headline-grabbing trips that bring humans out of Earth's orbit.

- Many fields, including agriculture, health care, transportation and energy, rely on satellites to provide crucial GPS coordinates, relay critical communications, predict the weather and more.

Threat level: Securing these companies and their infrastructure is a multifaceted problem that involves keeping hackers not only out of satellites in orbit, but also out of base stations and internal company networks.

- Government officials' visibility into these networks has gotten cloudier as the industry privatizes — giving executives like Elon Musk, who founded SpaceX, an outsize role in national security.

- Meanwhile, U.S. prosecutors and companies have already identified suspected space-related espionage campaigns from Russian and Chinese nationals in recent years.

Catch up quick: Last week's U.S. advisory is just the latest in a recent string of cyber exercises focused on the space industry.

- A hacking team received $50,000 last week after it won the first-ever "capture the flag"-style hacking competition involving an actively orbiting satellite at the DEF CON conference in Las Vegas.

- The Office of the National Cyber Director has held White House forums and other meetings across the country this year focused on securing space systems.

- Former congressional policy advisers have also called on the Cybersecurity and Infrastructure Security Agency to designate space an official critical infrastructure sector — which could unlock new security resources and funding potential for the sector.

Zoom in: Much of Washington's interest in space security notched up after Russian hackers targeted American satellite company Viasat an hour before invading Ukraine in early 2022 — providing a vivid example of how consequential space-related hacks can be.

Details: Securing satellites and other physical space systems faces many of the same challenges as securing other critical infrastructure systems: You typically need physical access to the equipment to make software upgrades.

- Satellites especially are designed to orbit the Earth for years, and the tech stacks they rely on can easily become outdated or riddled with new security flaws during that time.

The bottom line: Many of the same nation-state espionage and hacking fears that plague much of the U.S.' critical infrastructure — from water systems to hospitals — are playing out in the Earth's orbit too.

Be smart: The intelligence community recommends that private space companies rely on security logs to detect anomalous activity, develop programs to detect insider employee threats, and create security plans specifically to protect companies' "crown jewels."

Author: Sam Sabin, Axios Codebook

DEVELOPING KNOWLEDGE BY ENHANCING COMMUNICATION, COOPERATION AND COORDNATION

In our increasingly interconnected, globalised and rapidly changing world our traditional notions of security, risk, resilience and crisis management are constantly being put to the test.

The last few years have seen us steeped in a period with significant challenges and a great deal of uncertainty. The world struggled with the impact of Coronavirus and then we witnessed Russia's aggression towards Ukraine and that war having a significant impact on global peace, security and the economy.

2023 started with the devastating earthquakes that hit Turkey and Syria causing tens of thousands of deaths and severe damage to the infrastructure of both countries. Alongside all of this we have the continual impact of climate change causing floods and fires and devastation. In fact, the UN Secretary General António Guterres, has recently stated that we have moved from the position of 'Global warming' to a position of 'Global Boiling'.

July 2023 was the hottest month ever recorded on our planet, although if you lived in the United Kingdom, you would never know it. Wildfires in Greece, other parts of Europe, in California and more recently in Hawaii are having an extreme impact, causing the loss of lives, necessitating mass evacuations of people, damaging property, infrastructure and transport networks.

The world is in a somewhat chaotic state and this is a crucial time for all within our communities and that includes those within our critical infrastructure and information sectors. The challenges that have to be addressed, both natural and man-made are increasing in complexity, frequency and magnitude.

To address those challenges there needs to be a continued drive to develop enhanced levels of communication, cooperation and coordination. This has to be a shared responsibility across all countries, all levels of government, private industry, non-governmental/nonprofit organisations and the public.

This is something that we see articulated in almost every major policy statement delivered by governments around the world. I personally believe, that across many countries, there is a genuine commitment to make this happen, notwithstanding the difficulties in achieving such a position. A prime example of this being the recently revised CONTEST (Counter Terrorism)

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.

strategy in the United Kingdom. This references the fact that not only is the threat from terrorism both enduring and evolving but also that it has become more diverse, dynamic and complex and therefore less predictable. The document clearly recognises the need for all to work together through developing partnerships at every level and across all sectors and in particular the need to deepen international partnerships for the strategy to succeed.

The International Association of Critical Infrastructure Protection Professionals (IACIPP) fully supports international endeavours in developing effective partnerships. We were formed in order to bring like minded individuals together. We provide a communication and information sharing platform through which we seek to:

- Create new partnerships
- Generate new collaboration opportunities
- Share good practises and insights from industry leaders/operators/ academics, law enforcement and government agencies
- Increase visibility and recognition of issues and learning.

The IACIPP also publishes the Critical Infrastructure Protection and Resilience News magazine which reaches an audience of 80,000 plus people. Alongside this we support two major conferences a year, one in Europe (CIPRE) and one in North America (CIPRNA).

So, in all this we hope to play some small part in developing connectivity by bringing people together through our activities and actions.

Our next event will be our Critical Infrastructure Protection & Resilience (Europe) conference which will take place in Prague between the 3rd and 5th of October this year. I am fortunate, to once again have the honour to Chair this event. The agenda has an amazing line up of speakers and looks set to be an event not to be missed. I look forward to seeing you there.

John Donlon QPM FSyI
Chairman IACIPP

The CNI / Crowded Places Security Debate

Sarah-Jane Prew, a security consultant from Arup, discusses the unique security challenges presented by sites that are both Critical National Infrastructure (CNI) and Publicly Accessible Locations (PALs) and offers some insight into how the sometimes opposing priorities can be managed.

Protecting Critical National Infrastructure (CNI) sites is a large part of the security profes-sion's role; preventing hostile intervention while assuring resilience to ensure that the sec-tor can keep the nation's critical services operational. As the name suggests, CNI is about critical services and infrastructure and therefore security is usually associated with protect-ing assets and information by keeping unauthorised people out.

However, what if that CNI site is also a Publicly Accessible Location (PAL) and exists for the very function of allowing people in? How do you maintain and protect the criticality of the asset and function while not being able to keep people out? And how do you deal with the fact that the presence of all those people creates a target in itself, and thus an addi-tional type of threat, one that aims to kill and injure crowds of people but in doing so, dis-rupts the very CNI function you were originally trying to protect?

Two CNI sectors typically fall into this category by definition …. transport and health. An airport and a hospital, for example, exist for the very purpose of 'allowing people in' and yet are often defined as CNI due to their resilience and criticality, therefore requiring the levels of security afforded by their status. Increasingly, other sectors are also opening up their facilities electively to the public - many offering public realm areas in their offices where people can enter freely and enjoy a coffee while others combine the occupation of CNI sites with other, less or non-critical, industries.

In these cases there needs to be a successful blend between protecting both the CNI and PALs elements but often the lines between then are confused. Whereas in the protection of CNI the primary focus is on the protection of the asset and function, in a PAL the focus is on protecting crowds of people. This relatively obvious statement, however, often leads to counter-intuitive responses in the implementation of security processes.

Typically this is seen where screening is placed further and further out, away from the core of an asset. In airports, for example, and often in publicly accessible government buildings, it is common to see screening just inside the doorway or even outside. What is this security design aiming to achieve?

The introduction of this additional screening is often implemented post an incident, such as an explosive device detonating in the check-in area of an airport. The instinctive reaction is to try to prevent that from happening again. Screening before entry to the building will min-imise the chances of that happening in the same place again. But will it minimise the chances of it happening elsewhere at the same site? No … if anything it offers the attack-er a more convenient solution and a more accessible target …. a queue outside a building, close to a glazed facade or entrance.

So what, in this instance, is the security policy trying to protect? If it is the asset then the policy may be on the correct lines …. but if it is the crowds of people that frequent the site then they are just moving the threat elsewhere and arguably making the new target an easier and more attractive one. Needless-to-say, whether the target is CNI or people, the ultimate result is the same - a loss of function ….. only the number of casualties varies with the addition of loss of life in the latter case.

Experience has taught us, in both the Manchester Arena incident and in the Paris Stade de France attacks that terrorists, even suicide bombers, can be easily deterred from push-ing through security lines into the hearts of sites but will instead maximise the easier op-portunities outside the perimeter, even if less crowded, to attack.

So why are we still seeing poor security design in so many of these sites? Is it just a lack of thought process or an unclear view of what to protect? Is it that the vulnerabilities are not sufficiently risk assessed so there is a lack of clear focus on where to concentrate re-source? Or is there sometimes a more complex issue that has something to do with con-flicting priorities? This can certainly happen sometimes if the sector is in a regulated space.

Aviation, for example, a sector that has been overseen by regulation since its conception, often struggles to have a clear ability to focus on the broad range of threats now facing it because the regulators' focus still tends to be very narrow - protecting the aircraft and the parts of the airport that are essential to ensuring this protection. Aviation security regula-tion is complex and often slow to respond to changes in threat

profile. This is especially evident in those soft target, landside, publicly accessible parts of the airport which are es-sentially non-regulated spaces.

Adding to this, there is a dichotomy around regulation and the acceptance of anything be-yond its requirements on the part of sites; while regulation enforces a standard of protec-tion, even accepting that it usually plays to the lowest common denominator of those who have to abide by it, it can be doubly challenging, in a regulated space, to gain engagement with and funding for the implementation of concepts that are beyond minimum require-ments.

Commerciality is another major factor that affects security decisions more often than is helpful when aiming to protect both CNI and PALs concurrently. Even where public access is inevitable, such as an airport or railway station, the fashion in some parts of the world is to maximise the public access throughout the site, in an effort to increase commercial re-turn.

Large scale airport cities, for example, where people visit for the experience itself - be-cause the site contains shopping malls with dining opportunities, integrated hotels, swim-ming pools, cinemas and even event spaces, are becoming increasingly popular - at a time when attacks on airports in recent years have been numerous and on crowds of people even more so.

An attack on crowds of people could happen anywhere, of course, but what architects and designers often forget is that if that attack happens within a CNI site, even if

it is not tar-geting the site itself but the people who have congregated there, the incident does not just close down the shopping mall or the cinema where the attack happened …. it shuts down the entire CNI asset that surrounds it. This is especially so in aviation because it is the larger, more significant airports - the ones more likely to be designated CNI - that tend to be the ones following this trend and offering more in the way of public amenities.

While the problem of combining CNI sites with PALs is challenging enough and the devel-opment of commercial ventures within CNI sites increases the associated problems, is-sues are compounded further when little thought is given to the security of the design of such developments because these are the exact areas of the site, especially in airports and railway stations, that are not necessarily considered under transport security regula-tions. This leaves security managers under pressure to develop and implement security regimes whilst enabling revenue-generating commercial activities.

Managing security design within CNI where large crowds of people are present clearly presents significant challenges. When the challenge is multi-faceted, an equally multi-faceted approach needs to be adopted to achieve the best chances of success. This in-volves taking a risk-based approach while working alongside a number of agencies and understanding the full range of threats and their inter-operabilities so a layered and intelli-gent process of security can be adopted.

The first step is to assess the risk to the site, from both the perspective of the site being CNI and a Publicly Accessible Location. Assessments need to be made as to the safety and security priorities and what measures need to be implemented to protect which as-sets.

From a design perspective, it is essential that security professionals are involved in any design projects from the start to undertake these risk assessments early enough in the process that the design itself can 'design out risk', therefore reducing the number of secu-rity

features that need to be added to minimise the risk and mitigate the effects of an at-tack. As well as providing the most robust security in the most aesthetically pleasing way, this is also the most cost and time effective way of ensuring good security.

Without early intervention and assessment of the whole site, security can be compromised due to prioritising the protection of one element over another, rather than addressing the site holistically. This will lead to push-back on developing further security due to lack of space, resource or time.

Take the example of positioning security screening further out to protect an inner asset …. This succeeds in reducing the risk to the inner asset but actually increases the risk to the individuals queuing to be screened by making them an easier target. If the two problems are not addressed together, then one will inevitably lose out, as the design of one in isola-tion is likely to compromise the security of the other.

While embedding security in the design is essential, it can't achieve everything and it is important to consider operational factors, especially for sites that attract large numbers of people. It is vital that all stakeholders are involved in security developments to ensure that their requirements are met and their operational needs incorporated. It is also essential that the multi-agency approach is adopted, which ensures that all those involved in man-aging security operations are brought together to ensure a fully co-ordinated strategy in terms of protection, detection, response, resilience and, if things do go wrong, recovery and business continuity.

Beyond the physical measures it is important to move the security perimeter out so there is vigilance far beyond the immediate vicinity of what you are aiming to protect, particularly when this is groups of people. For example, it is too late, at a screening point, to develop a suspicion about someone who may be targeting the crowds in that screening queue. By pushing the perimeter of surveillance out beyond this, operators can monitor the demo-graphic and behaviour of those approaching, giving time for an intervention if required.

In a time when pressure is on sites to reduce operational costs, this level of security oper-ation is often met with reluctance but complex security needs require layers of mitigation and this requires both physical and operational measures.

Ultimately, those areas that are not currently governed under regulation, especially when situated within sites that have areas and operations that are under a regulatory frame-work, would merit from having more published guidance. This would ideally show clear ar-eas of responsibility so organisations can assess their risks and priorities holistically, across the whole site, according to the risk presented, rather than a bias of focus and re-source from having regulatory requirements in one place and a lack of them in another.

The above considerations will give some solutions to the challenge of protecting those CNI sites that are also Publicly Accessible Locations (PALs); a question that is going to contin-ue to face the security industry as more CNI sites are allowing the public into their sites.

Beyond Physical Protection

Since 1996, the IAEA's International Physical Protection Advisory Service (IPPAS) has been helping countries to identify ways to strengthen the protection of nuclear materials and facilities.

How the International Physical Protection Advisory Service (IPPAS) facilitates the enhancement of computer security

For almost thirty years, the IAEA's International Physical Protection Advisory Service (IPPAS) has been used by countries for peer review to ensure the physical protection of all types of facilities where nuclear and other radioactive materials are used, including nuclear power plants and hospital radiotherapy units. However, owing to advances in technology, digital systems are now at the heart of operations for these facilities. This has led to many new nuclear security challenges.

In response to the real threat of cyberattacks on facilities, including nuclear facilities, information and computer security for physical protection was added to the scope of IPPAS in 2012. Since then, countries have increasingly requested this module as part of the IPPAS review, in order to support their work in counteracting cybersecurity threats.

As a core component of the IAEA's nuclear security

programme, IPPAS is an advisory service that reviews a country's existing practices against relevant international instruments and IAEA nuclear security guidance. It assists countries, upon request, in strengthening their national nuclear security regimes, systems and measures by providing advice on implementing international legal instruments.

"Twenty-seven years after the first IPPAS mission, the service has evolved to address modern challenges and needs," said Heather Looney, Head of the Nuclear Security of Materials and Facilities Section at the IAEA's Division of Nuclear Security. "Physical protection against the theft, sabotage or unauthorized use of nuclear and other radioactive material cannot be ensured without computer security measures. By inviting an IPPAS mission, countries can benefit from advice on what can be improved, and how," she added.

IPPAS follows a modular approach and offers five modules, which cover the following: a national review of the nuclear security regime for nuclear material and nuclear facilities; a review of security systems and measures at nuclear facilities; a review of the transport security for material; a review of the security of radioactive material, associated facilities and activities; and a review on information and computer security. In total, 97 IPPAS missions have been conducted to date since the first one in 1996, and 22 countries have requested the inclusion of the information and computer security module in the IPPAS review.

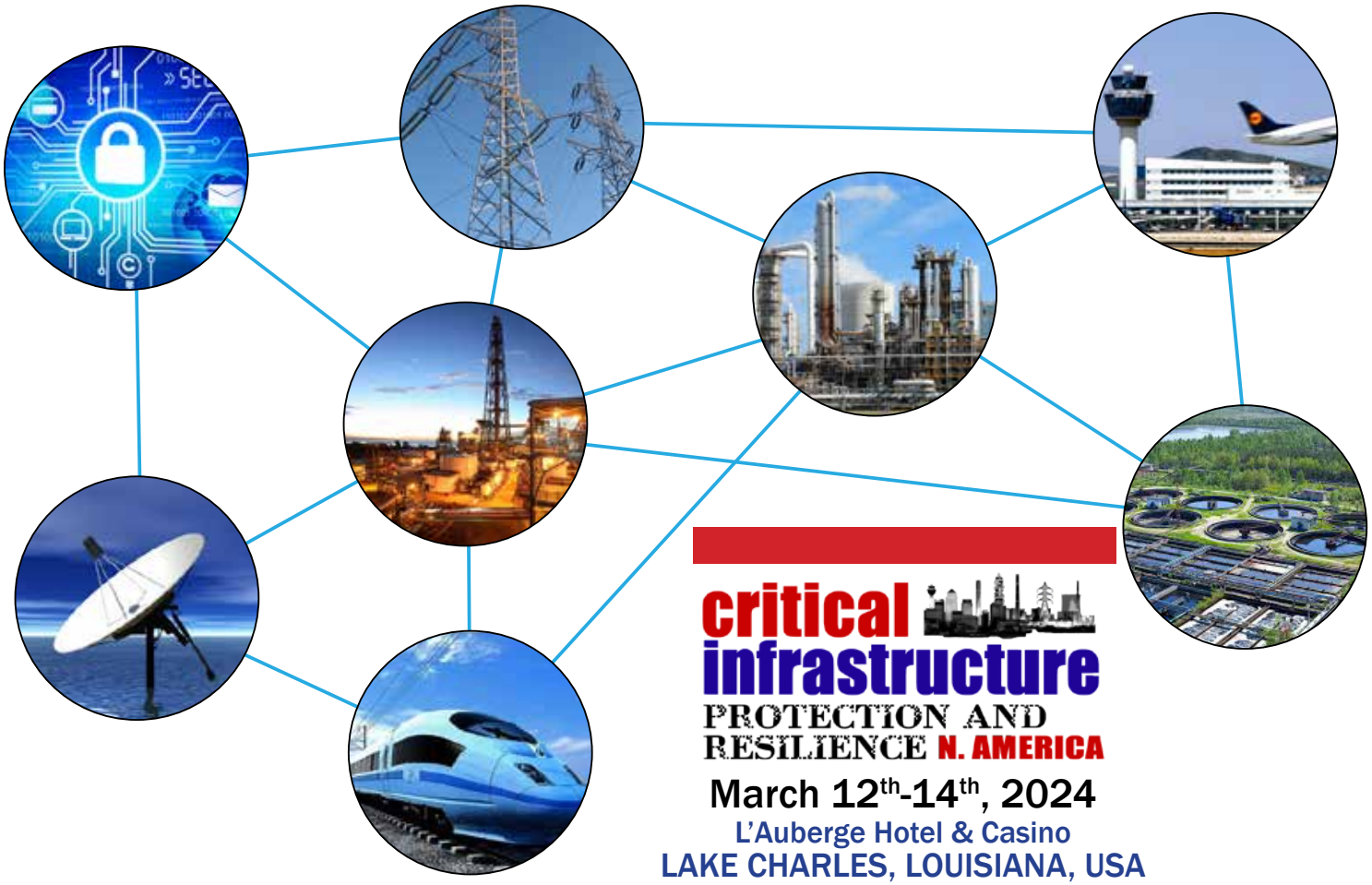
What should a country expect during the information and computer security assessment?

As a first step, an IPPAS team of international nuclear security experts examines how national policies relating to information and computer security programmes have been set up and managed. The team will then look at the legislative and regulatory framework by comparing the procedures and practices in place in the country with the obligations specified under the Convention on the Physical Protection of Nuclear Material and its 2005 Amendment, as well as with the guidance provided in relevant IAEA Nuclear Security Series publications. In this way, they are able to determine whether countries have the necessary policies and procedures in place to enable adequate computer security in critical nuclear and radiological facilities.

At the facility level, the computer security review will look at computer security management, computer security programme, access controls, defensive computer security architecture, and the detection of and response to computer security events. The team may also assess cross-cutting areas, such as risk management, graded approaches, nuclear security culture and human resource management.

Japan hosted an IPPAS mission and its follow-up mission in 2015 and 2018, respectively. "It was a valuable experience for Japan to review the current status of computer security measures and to promote their enhancement based on the reviewers' suggestions," said Hiroyuki Sugawara, Director for International Nuclear Security in the Division of Nuclear Security at Japan's Nuclear Regulation Authority (NRA). "In response to the IPPAS findings, we decided to strengthen the computer security measures and increase the number of inspectors with expertise in the field. In addition, the NRA incorporated computer security threats in its national threat assessment and required licensees to take robust computer security measures, as well as to enhance the content of their computer security plans by incorporating countermeasures against cyberattacks."

In France, following an IPPAS mission in 2018, the visibility of computer security was strengthened in the national nuclear security framework. "The IPPAS mission required a strong commitment from



critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 12th-14th, 2024

L'Auberge Hotel & Casino
LAKE CHARLES, LOUISIANA, USA

A Homeland Security Event

SAVE THE DATES

Securing the Inter-Connected Society

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

The 5th Critical Infrastructure Protection and Resilience North America brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing America's critical infrastructure.

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

Join us for the next gathering of operators and government establishments tasked with the regions Critical Infrastructure Protection and Resilience.

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

To discuss sponsorship opportunities contact:

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

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

Sam Most
(Mainland Europe, Turkey, Israel)
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

The premier discussion for securing America's critical infrastructure

Owned & Organised by:

Supporting Organisations:

Media Partners:

the various stakeholders giving the opportunity for France to consolidate its nuclear security regime and to stimulate its implementation," said Frédéric Boën, Computer Security Project Leader in the Ministry of Energy Transition, Defense and Security Directorate, Nuclear Security Office. "The staff dedicated to computer security was increased and regulatory guidelines were established in line with the international standards and the IAEA nuclear security guidance."

The IAEA has maintained the IPPAS Good Practices Database since 2016 to share the findings of such missions with the international nuclear security community, thus enhancing the impact of the assistance offered by the IAEA to countries around the world. "Maintaining this database and sharing such examples extends the benefits of IPPAS missions beyond the host country to the international nuclear security community, and multiplies the impact of the assistance offered by the IAEA to its Member States," said Looney.

The majority of the State-level good practices relate to nuclear security management, which provides the foundation for computer security and coordination. In addition, there are 40 good practices relating to computer security both at State and facility level that are accessible for IAEA Member States through designated points of contact.

The IAEA continues to support countries in enhancing their national nuclear security regimes; demand from countries to receive IPPAS missions in 2023 and in 2024 remains high.

TSA installs new security technology that enhance screening capabilities at West Virginia International Yeager Airport

The Transportation Security Administration (TSA) has installed two new state-of-the-art computed tomography (CT) checkpoint scanners that enhance screening capabilities of carry-on items brought to the checkpoint by passengers ticketed to fly out of West Virginia International Yeager Airport.

The new CT scanners screen carry-on items at the checkpoint by applying a sophisticated algorithm as they generate a 3-D image of the contents of carry-on bags. This new technology creates such a clear image of a bag's contents that the system can automatically detect explosives and other threat items by shooting hundreds of images with an X-ray camera spinning around the items to provide TSA officers with a 3-D view of the contents of a carry-on bag. A TSA officer can view the 3-D X-ray image on a monitor and manipulate the image to get a better view of the bag's contents, ultimately reducing the number of carry-on bags that need to be opened and manually inspected. However, if a bag requires further screening, a TSA officer will inspect it to ensure that a threat item is not contained inside.A computed tomography scanner.

In addition to enhanced security, the CT units improve the traveler's experience because passengers using these machines are permitted to leave their laptops and other electronic devices in their carry-on bags. Additionally, passengers screened in security lanes with CT units do not need to remove their travel-sized 3-1-1 liquids.

"Our officers' use of CT technology substantially improves our threat detection capability at the checkpoint," said John C. Allen, TSA's Federal Security Director for West Virginia. "Previously, our screening technology for carry-on bags used 2-D images. The CT technology applies advanced algorithms for the detection of explosives, including liquid explosives and other threat items."

With the new CT scanners, all carry-on items, including roller-bags, need to be placed into a bin for screening instead of being placed directly on the conveyor belt. The new scanners are more efficient for the passenger than the older advanced technology units, which provided TSA officers with only a 2-D image and required the passenger to remove, or divest, various items from their carry-on bags before being screened. Since the new CT scanners do not require divestiture of items from carry-on bags, it also saves time.

CT units have a slightly smaller entry tunnel and not all larger carry-on bags will fit into the units. TSA recommends that large carry-on items be checked with the airline.

Hybrid Threats – A Comprehensive Resilience Ecosystem

Hybrid threats constitute a combination of different types of tools, some expected and known, some unexpected and clandestine, applied to achieve an undeclared strategic objective, and without officially admitting to doing so. The common denominator for hybrid threat actors is their desire to undermine or harm democratically established governments, countries or alliances. By their very nature, hybrid threats constitute a risk to European values, governments, countries and individuals.

Their overarching aim is to constrain the freedom of manoeuvre of democracies in order to discredit its model compared to authoritarian regimes or gain other advantages over democracies.

In particular, hybrid threat actors may be characterised by their wish to:

• undermine and harm the integrity and functioning of

democracies by targeting vulnerabilities of different domains, creating new vulnerabilities through interference activity, exploiting potential weaknesses, creating ambiguity and undermining the trust of citizens in democratic institutions;

• manipulate established decision-making processes by blurring situational awareness, exploiting gaps in information flows, intimidating individuals and creating fear factors in target societies; and

• maximise impact by creating cascading effects, notably by tailoring attacks, combining elements from specific domains to overload even the best prepared systems, with unpredictable, negative consequences. These domains were outlined in a conceptual model which we, the European Commission's Joint Research Centre and the Helsinki-based European Centre of Excellence for Countering Hybrid Threats, published in 2020.

Today, Europe is facing growing and increasingly complex security challenges. Hybrid threats have become integral part of our security concerns; war has returned to Europe; instability is increasing in Europe's neighbourhood regions; there are attempts to manipulate election outcomes; and democracies increasingly are portrayed as weak governance systems. The possibility to spread disinformation rapidly and with great outreach via social media further exacerbates the potential impact of hybrid threats. Moreover, our increasing dependency on IT tools for our daily work, banking, health management as well as for

elections and governance, means that every European, Member State and company is at some risk of being impacted by hybrid threats. We should also be aware that the impact of hybrid threats is not simply restricted to the security domain but also links to defence. As seen in the Communication 'Commission contribution to European defence, it urgently calls for a major boost to European resilience and defence.

Hybrid threats have become increasingly common over the past 10-15 years, and we can fully expect them to grow both in frequency and impact in future. The problem of hybrid threats is however not one that can be solved just at national and/ or regional level: a concerted effort across Europe, involving all relevant partners, is crucial. For this reason we already proposed in 2020 a conceptual

9 Executive summary model that has proven a useful tool for policymakers when addressing hybrid threats.

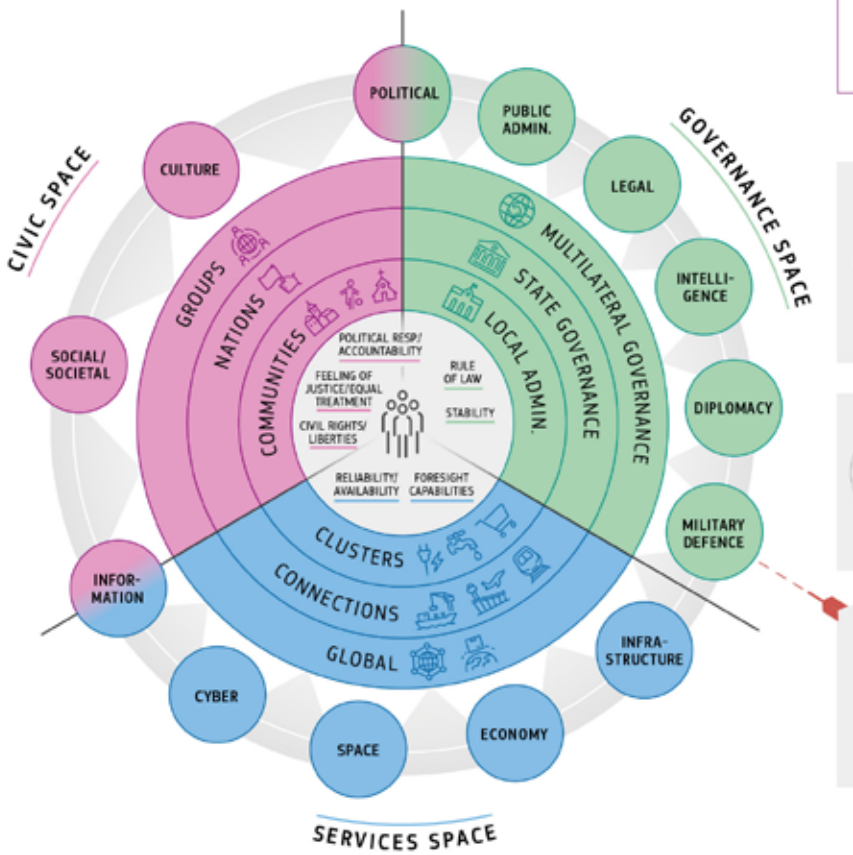
As outlined in recent EU policy initiatives such as the 'Communication on the EU Security Union Strategy'3 and 'A Strategic Compass for Security and Defence'4 we are seeing fast-moving developments and an increased level of sophistication in hybrid threats. Resilience against hybrid threats therefore needs to be designed and implemented at all levels, and has to consider resilience measures, not only from multiple domains' perspective but as a comprehensive ecosystem approach. In other words, developing resilience against hybrid threats necessitates looking beyond resilience in individual areas, building it systemically while considering dependencies and interdependencies between the different parts of society.

To address these issues, we in this report for the first time apply a systems-thinking approach to hybrid threats, with representation of society as a whole. Throughout the elaboration of the report and the underpinning scientific work, we have been in dialogue with Member States, notably

CORE — A COMPREHENSIVE RESILIENCE ECOSYSTEM

The comprehensive resilience ecosystem (CORE) model is a systemic representation of democratic society as a whole. It is used to analyse and ultimately counteract hybrid threats that seek to undermine and harm the integrity and functioning of democracies, change decision-making processes, and create cascading effects.

CORE MODEL — STRUCTURE



7 FOUNDATIONS OF DEMOCRATIC SOCIETIES

Hybrid threat actors aim to undermine them to achieve their goals. Resilience requires strong foundations, supported by trust.

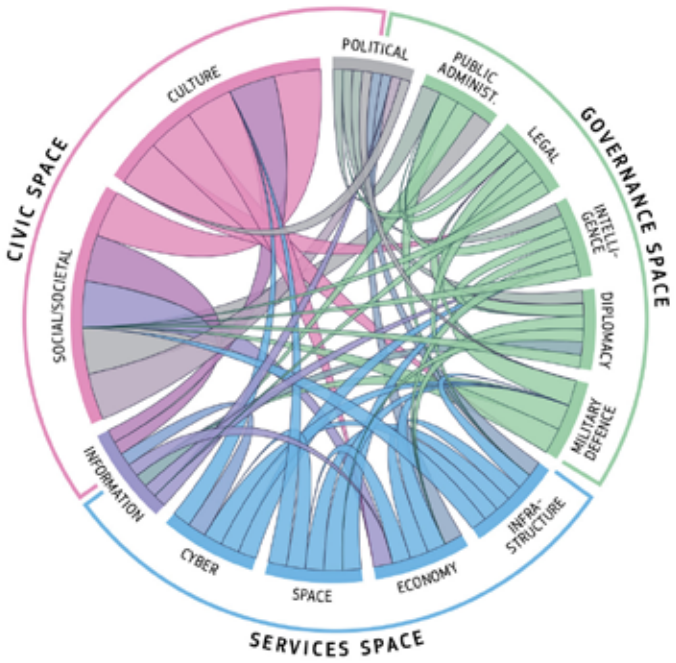
3 SPACES + 3 LAYERS

The spaces (Civic, Governance, Services) and layers represent the sectors and levels of society.

13 DOMAINS

Domains can act as shields against malicious activities or entry points for attacks.

RESILIENCE AND INTERCONNECTIONS BETWEEN DOMAINS



Resilience is key to counter hybrid threats and needs to be designed systemically.

Building resilience in domains individually is not optimal, since hybrid threats aim to create cascading effects and exploit interconnections.

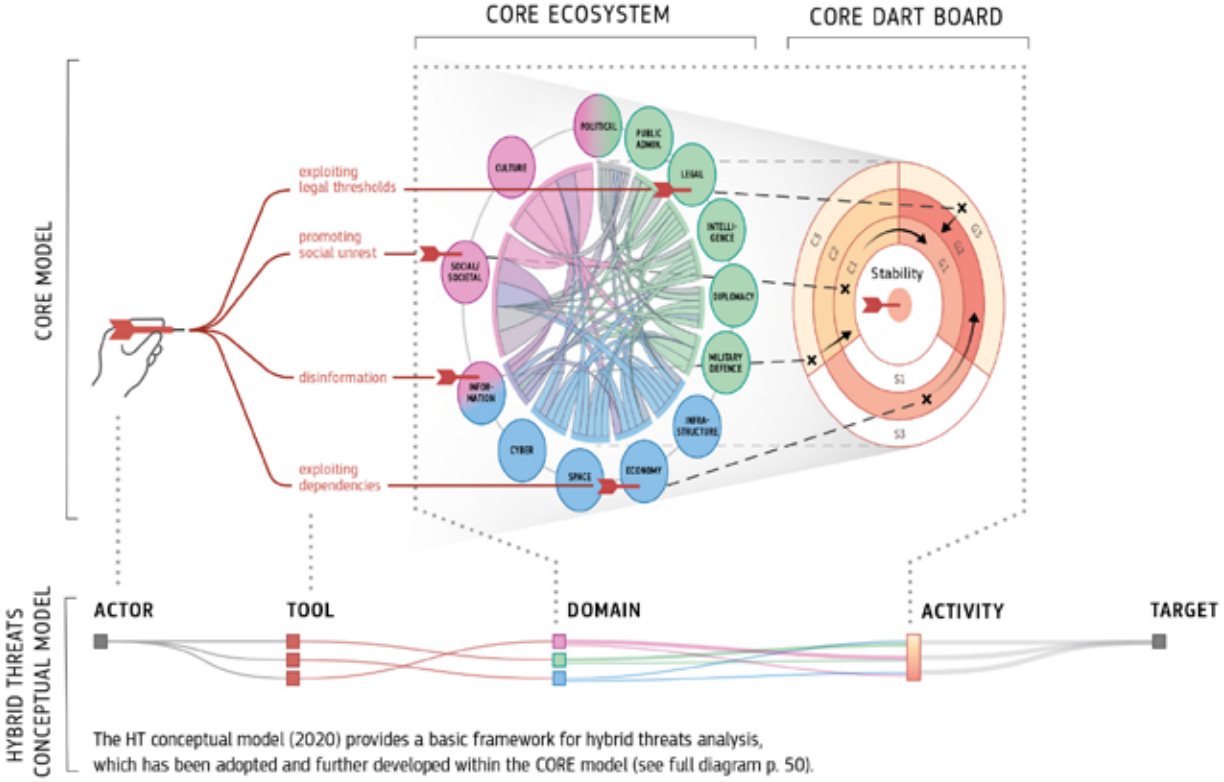
A **systemic approach** is necessary, **considering existing dependencies and interdependencies** in society.

Trust in the democratic process makes dependencies and interdependencies strong and healthy and supports the foundations of democratic systems. Hybrid threat actors seek to erode this trust.

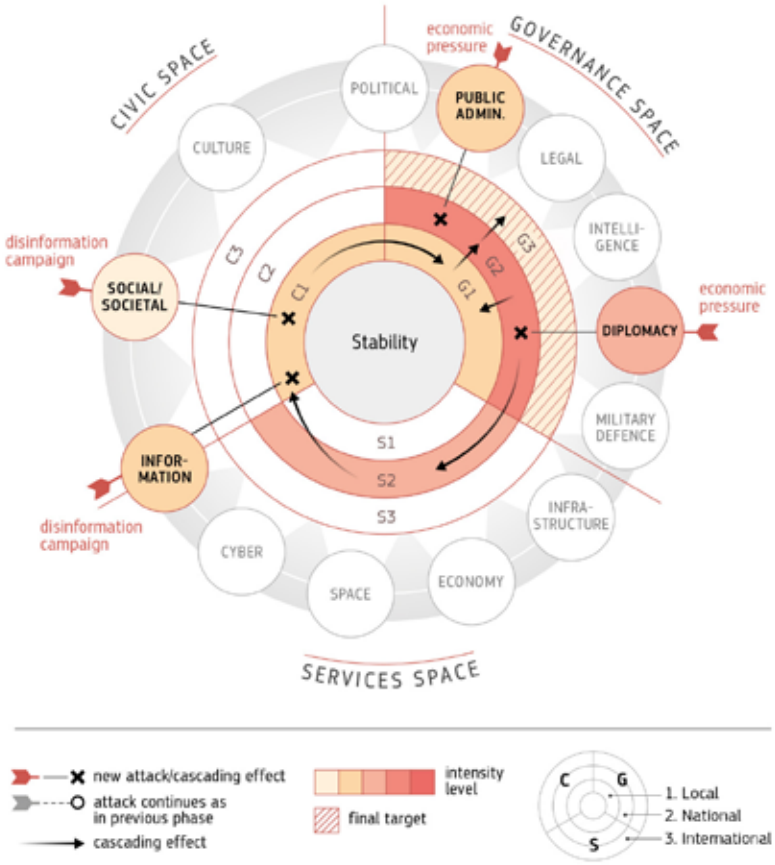
REPRESENTING THE IMPACT OF HYBRID THREATS

CORE can be used as a 'dart board' to map how actors use specific tools to attack different domains and create cascading effects to different spaces and layers.

It helps to analyse and understand impacts, developments/phases, and how intensely the spaces and layers are affected by hybrid threats and their dependencies.



The HT conceptual model (2020) provides a basic framework for hybrid threats analysis, which has been adopted and further developed within the CORE model (see full diagram p. 50).



CORE AS A STRATEGIC DESIGN BOARD

This ecosystem approach helps to spot early signals, support their analysis and identify potential response trajectories.

It can be used to:

- **design the right measures** to counter the primary and higher-order effects in all spaces and layers of the ecosystem
- build a cross-sectoral, **whole-of-society approach to resilience**
- serve as the **conceptual foundation to support policymaking** against hybrid threats

In essence, it helps decision-makers select which resources, tools and measures to mobilise at EU, Member State and operational levels.

via the Horizontal Working Party on Building Resilience and Countering Hybrid Threats of the Council of the European Union, as well as other key stakeholders. In concrete terms, we in this report propose a comprehensive resilience ecosystem (CORE) model to facilitate decision-making for policymakers. The novelty of the CORE model is how it allows policymakers to estimate how adversaries employ hybrid threats in order to alter democratic decision-making capabilities. It shows how the hybrid threat activity bit by bit challenges democratic systems by introducing different types of stress. It also allows monitoring the dependencies and possible cascading effects. This is important for the detection of hybrid threats. Foresight plays a crucial role in this process. The CORE model is based on the following elements, as also visualised in the following page:

1. Seven foundations of democratic systems lie at the heart of the ecosystem. The foundations are the ultimate goals that hybrid threat actors aim to undermine, while scoring some of their own strategic interests.

2. The domains from the conceptual model also are an integral part of the ecosystem. If resilience is well developed in the domains, they can act as shields against malicious activities. On the other hand, a lack of resilience in the domains can open entry points for hostile actors.

3. The ecosystem consists of three spaces – Civic, Governance and Services – which represent the three sectors of society.

4. The layers of the ecosystem represent the different 'levels' that exist in society – from the more local levels to international levels. The connections between the four types of elements represent the whole-of-society approach. Since elements are interconnected, resilience-building measures for one element will affect other elements, positively or negatively. Actors behind hybrid threats aim to exploit the various elements and their interconnectedness to maximise their impact. Therefore, policymakers need to understand the interdependencies between the various elements, in order to build resilience against hybrid threats and for early detection of malign activity.

This ecosystem model supports anticipation and foresight work in imagining developments, assessing the scale of risks and disruptions, and representing worst case scenarios. Used as a strategic design board, the CORE model can help identify the right measures to counter the effects of hybrid threats in all spaces and layers of the ecosystem. It can help to implement a holistic approach against hybrid threats and serve as a foundation for the creation of the EU Hybrid toolbox which was announced in 'A Strategic Compass for Security and Defence'.

The seven case studies presented in this report demonstrate the extent to which hybrid threat activity can undermine and weaken the foundations of a well-functioning democratic ecosystem.

Written in response to the above-mentioned EU policy initiatives, this report may therefore be considered a strategic manual for Member States and EU institutions on how to anticipate hybrid threats, evaluate their potential impact, and identify how to pre-empt or minimise their negative impact. Of particular value are the various case studies, the timeline outlining how hybrid threats have developed, and the cultural/linguistic comparisons. All of these contribute to a broad, multi-cultural perspective that lead to a deeper understanding of what hybrid threats constitute in this day and age, while offering tangible guidance on building

resilience and preparing for future challenges.

Looking ahead, the Russian invasion of Ukraine in particular highlights the need for further research on the following points:

• The Conceptual Model on hybrid threats can be further optimised by taking into account experiences from the ongoing war including the increasing role of disinformation by Russia, and how this to a large extent has been countered, not least by the Ukrainian president who has communicated well and continuously with his people and the rest of the world, being visible and transparent in showing what is going on, addressing fellow democracies to ask for support, and creating positive reactions to his country and people, successfully making Ukraine's cause the entire democratic world's cause.

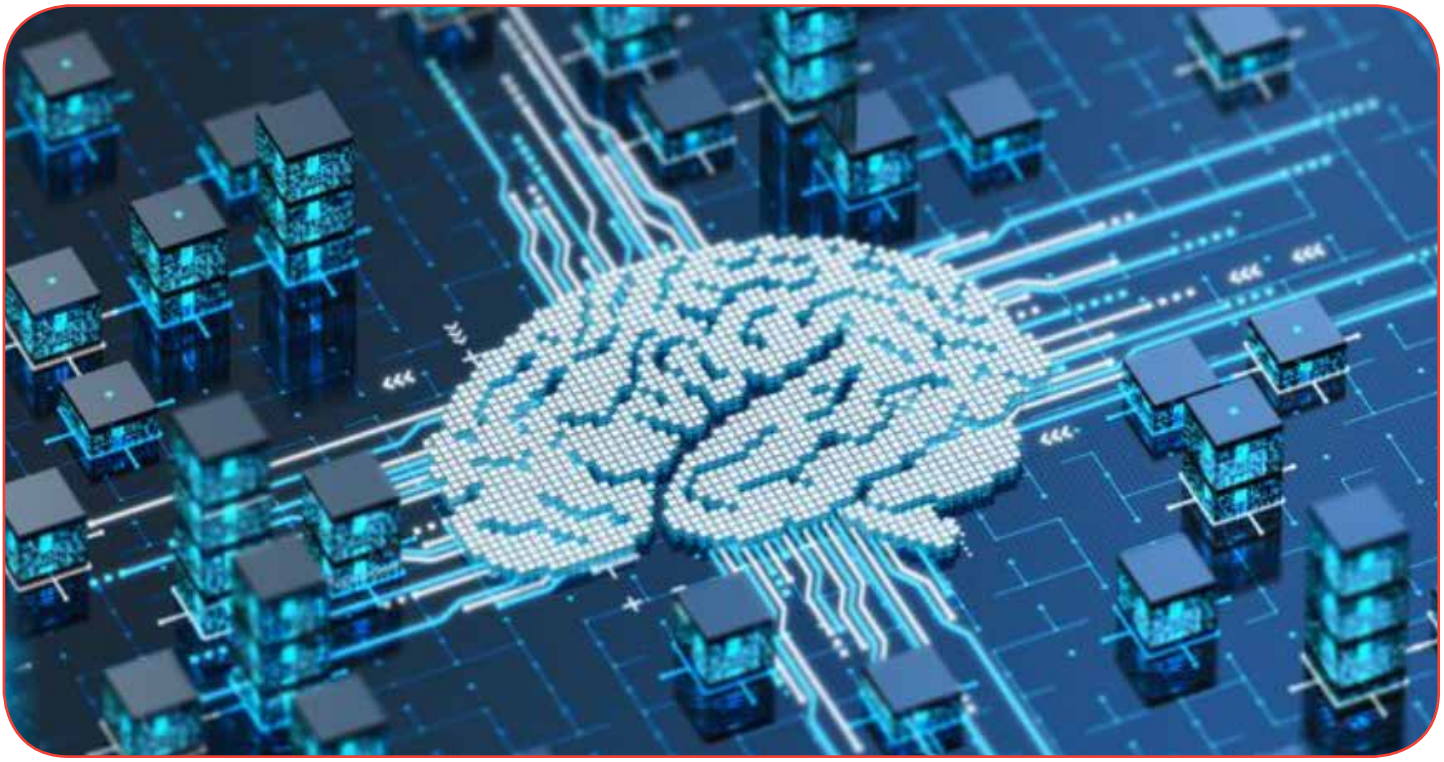
• The particular case of countries in an ongoing democratisation process could be explored further, as they already have the systemic vulnerabilities of democracies but not all the protection of established institutions, traditions, and processes of democracy.

• Seeing how Russia escalated from priming and destabilizing to actual coercion, crossing the threshold from hybrid threats to conventional war, it is essential to develop a better understand of the influence of culture, mind-set and values of hostile actors, to understand their thinking. That way we will be in a better position to understand, interpret and anticipate their strategic goals, and, crucially, to pre-empt of minimise their impact.

This report is a Science for Policy report by the Joint Research Centre (JRC), the European Commission's science and knowledge service, prepared together with the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE).

Jungwirth R., Smith H., Willkomm E., Savolainen J., Alonso Villota M., Lebrun M., Aho A., Giannopoulos G.,

Artificial Intelligence and Cybersecurity Research



ENISA Research and Innovation Brief

Artificial Intelligence (AI) is a typical dual-use technology, where malicious actors and innovators are constantly trying to best each other's work. This is a common situation with technologies used to prepare strategic intelligence and support decision making in critical areas. Malicious actors are learning how to make their attacks more efficient by using this technology to find and exploit vulnerabilities in ICT systems.

Taking one step further in clarifying this initial statement: with the help of AI, malicious actors can introduce new capabilities that can prolong or even expand cyber threat practises that have been in existence already for a long time. With AI, these capabilities are gradually becoming automated and harder to detect. This study explores some of these capabilities from a research perspective.

In this study, two dimensions of AI have been considered (categorisation explained in Section 4): (a) ensuring a secure and trustworthy AI and preventing its malicious use ('AI-as-a-crime-service' or 'AI to harm') and (b) the use of AI in cybersecurity ('AI use cases' or 'AI to protect').

The use cases of AI in cybersecurity are numerous and growing. Listing

them exhaustively is beyond the scope of this study, as research in this area is constantly evolving. However, we present examples of some of these use cases throughout the report to better explain ongoing research efforts in this technology and explore areas where further research is needed.

The aim of this study is to identify needs for research on AI for cybersecurity and on securing AI, as part of ENISA's work in fulfilling its mandate under Article 11 of the Cybersecurity Act1. This report is one of the outputs of this task. In it we present the results of the work carried out in 20212 and subsequently validated in 2022 and 2023 with stakeholders, experts and community members such as the ENISA AHWG on Artificial Intelligence3. ENISA will make its contribution through the identification of five key research needs that will be shared and discussed with stakeholders as proposals for future policy and funding initiatives at the level of the EU and Member States.

No prioritisation of research needs is presented in this report. ENISA conducts its annual prioritisation exercise taking into account the overall status of cybersecurity research and innovation in the EU, policy and funding initiatives for cybersecurity research and innovation in the Union and technical analysis on specific topics and technologies. The priorities for 2022 can be found in the ENISA Research and Innovation Brief Report.

Furthermore, in 2022, ENISA conducted a study reviewing the work of 44 research projects, programmes and initiatives on

Top 5 Resesrch Needs for AI and Cybersecurity

cybersecurity and AI, which were for the most part funded by the EU's framework programmes over the period 2014 to 2027. The

importance of this inventory relates to the specific role played by AI in the cybersecurity research field, given the continuous and intensifying interplay with other technology families. The fundamental question driving this study was whether investments in cybersecurity R&I on AI have enabled Europe to make progress in this area, especially those backed by EU funds. The findings of this study can also be found in the ENISA Research and Innovation Brief Report 2022.

While we recognise the immense potential in AI for innovation in cybersecurity and the many requirements needed to improve its security, we also acknowledge that there is still much work to be done to fully uncover and describe these requirements. This report is only an initial assessment of where we stand and where we need to look further in these two important facets of this technology.

Furthermore, according to the results of the ENISA study on EU-funded research projects on cybersecurity and AI mentioned earlier, the majority of the projects reviewed focused on machine learning techniques. This can be interpreted in two ways: as a sign that the market for such solutions is particularly appreciative of the potential benefits of ML compared to other fields of AI or that, for some reason, research and development in the other fields of AI is not being adequately considered by public funders despite their recognised potential. In this study, we also highlight the need to further explore the use of ML in cybersecurity but also to investigate other AI concepts.

ENISA has followed the steps outlined in the following list to identify the research needs presented in chapter 7.2 of this report.

- Identification from existing research papers of functions and use cases where AI is being used to support cybersecurity activities.
- Identification from existing research papers of areas where cybersecurity is needed to secure AI.
- Review of AI use cases.
- Analysis of open issues, challenges and gaps.

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

- Identification of areas where further knowledge is required.

These steps were carried out by experts who contributed to this report mainly through desk research, and the results were validated by members of the R&I community.

ENISA prepares these studies with the aim of using them as a tool to develop advice on cybersecurity R&I and present it to stakeholders. These stakeholders are the main target audience of this report and include members of the wider R&I community (academics, researchers and innovators), industry, the European Commission (EC), the European Cyber Security Competence Centre (ECCC) and the National Coordination Centres (NCCs).

Conclusions and Next Steps

AI is gaining attention in most quadrants of society and the economy, as it can impact people's daily lives and plays a key role in the ongoing digital transformation through its automated decision-making capabilities. AI is also seen as an important enabler of cybersecurity innovation for two main reasons: its ability to detect and respond to cyber threats and the need to secure AI-based applications.

The EU has long considered AI as a technology of strategic importance and refers to it in various policy and strategy documents. ENISA is contributing to these EU efforts with technical studies on cybersecurity and AI. For example, the cyber threat landscape for AI123 raised awareness on the opportunities and challenges of this technology. The Agency has already published two studies on this topic and this report will be the third publication aiming to provide a research and innovation perspective of cybersecurity and AI. In preparing these studies, the Agency is supported by the R&I community and has established an ad-hoc working group124 with experts and stakeholders from different fields and domains.

This study makes recommendations to address some of the challenges through research and identifies key areas to guide stakeholders driving cybersecurity research and development on AI and cybersecurity. These recommendations constitute ENISA's advice, in particular to the EC and ECCC, using its prerogative as an observer on the Governing Board and advisor to the Centre. The findings were used to produce an assessment of the current state of cybersecurity research and innovation in the EU and contribute to the analysis of research and innovation priorities for 2022, presented in a separate report.

In this context and as next steps, ENISA will:

1. present and discuss the research and innovation priorities identified in 2022 with members of the ECCC Governing Board and NCCs;
2. develop a roadmap and establish an observatory for cybersecurity R&I where AI is a key technology; and
3. continue identifying R&I needs and priorities as part of ENISA's mandate (Article 11 of the CSA).

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.

EDITORS

Corina Pascu (ENISA), Marco Barros Lourenco (ENISA)

AUTHORS

Dr. Stavros NTALAMPIRAS, University of Milan, I; Dr. Gianluca MISURACA, Co-Founder and

VP, Inspiring Futures, ES; Dr. Pierre Rossel, President at Inspiring Futures CH

Zero Trust a cybersecurity Imperative

A current cybersecurity initiative in the United States is Zero Trust (ZT). According to the National Institute of Standards and Technology (NIST), Special Publication (SP) 800-207 ZT is characterized as "… the term for an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources…" (NIST, 2020). In other words, device access to networks or cloud environments is authenticated before a session to an enterprise resource is established. This cybersecurity process changes how access is granted to cyber resources. In current operations, devices are assessing networks and clouds by attempting to authenticate at the network boundary. The network, through directory services, authenticates the device. So, an adversary could run bot scripts to gain unauthorized access to the network. The concept of ZT was first mentioned in 1994. In his 1994 doctoral dissertation, Stephen Marsh is credited with the first use of the term Zero Trust. In this work, Marsh discusses the concept of trust in a global community with very limited physical boundaries (Marsh, 1994). In 2013 The Cloud Security Alliance (CSA) developed the "Software Defined Perimeter (SDP) protocol" (CSA, 2022). SDP is designed to provide on-demand, dynamically provisioned, air-gapped networks. Air-gapped networks are trusted networks that are isolated from all unsecured networks and allow them to mitigate network-based attacks. The SDP protocol is based on workflows invented by the United States (U. S.) Department of Defense (DoD) and used by some U. S. Federal Agencies. In February 2014, CSA sponsored the SDP Hackathon to prove the cybersecurity protection SDP provides. More than 10 billion packets were fired at the SDP from around the world, and no attacker broke through even the first of five layers of security controls specified by the SDP architecture. Hackers from all over the world participated in the hackathon. Notable entrants signed on from Argentina, Brazil, Chile, China, Hong Kong, Hungary, Korea, Romania, Russia, the UK, and the U. S. (Hackathon, 2014).

Within the 2020 NIST publication SP 800-207, SDP was named an emerging technology to implement a zero-trust architecture (ZTA) (NIST, 2020, p. 48). In 2021 President Biden, in an executive order, directed all executive agencies to implement a ZTA. In response to this federal directive, the U. S. Department of Defense, the U. S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA), and the President's National Security Telecommunications Advisory Committee provided formal zero trust implementation governance (Biden, 2021).

In the U. S., the private sector owns and operates a majority of our nation's critical infrastructure, and partnerships between the public and private sectors that foster trust and effective coordination are essential to maintaining critical infrastructure security and resilience (CISA 2023). Operational technology (OT) systems are prevalent in various critical infrastructure sectors. In 2022, NIST updated its publication on industrial control systems to include a Guide to Operational Technology (OT) Security. Since U.S. critical infrastructures often comprise interconnected and mutually dependent systems, OT plays a crucial role in their operation (NIST, 2022). The guide features 12 different OT topologies that offer owners and operators fundamental frameworks for implementing security measures.

Dr. Martin is a Professor of Practice at Capitol Technology University. His work is in the functional areas of Critical Infrastructure and Operations Technology System Security.

The Cloud Security Alliance Research is an industry-driven initiative that is impartial to vendors and seeks consensus. The Zero Trust Advancement Center is dedicated to creating tools and resources that aid in the implementation of zero trust. Implementing SDP in a Zero Trust model can provide protection to organizations against new attack techniques in conventional network models. Additionally, SDP implementation can improve the security stance of businesses dealing with the challenges of adapting to constantly expanding and widely dispersed attack surfaces. If you wish to join the research working group, please visit the following website: https://cloudsecurityalliance.org/research/.

When it comes to safeguarding crucial infrastructure cyber resources, there are numerous techniques at our disposal. One such method is the implementation of a zero-trust cybersecurity model, which holds great promise in terms of security protocol. If you are responsible for critical infrastructure environments, exploring the benefits of adopting a zero-trust approach to bolster your security posture would be wise.

Resilience in action

by Robert Hall

A new book, Building Resilient Futures, looks at what resilience means at times of crisis as well as the in-between periods. The author considers the application of resilience principles to challenging national and organisational situations as they affect the critical infrastructure (CI). While most of the CI is provided by private organisations, it is for public use and as a result has a lower risk tolerance than other private-sector entities. This makes resilience an important factor in recovery.

Introduction

Like strategy and crisis, resilience is a much over-used word. Yet, it is the word that from its Latin roots (resilire) indicates a bouncing back or recoil from distortion or adversity. Its significance has progressed from applications in physics and engineering, through ecology and the environment, to today when it is preceded with a wide range of adjectives such as personal, organisational, societal, infrastructural, economic, national, etc.

While definitions also widely vary, the most succinct for the purpose of this article is the ability to 'anticipate, absorb and adapt to change' – essentially, to survive and thrive. This interpretation can include key activities like foresight, preparation, response, recovery and regeneration. By incorporating change, it means that bouncing back is an insufficient description as the status quo ante cannot be realised. Rather, it is a case

of bouncing forward to a new or different state that, hopefully, will allow better coping mechanisms for future distortions or adversities.

Learning lessons

Let's see this interpretation in action. Perhaps the most pertinent example of resilience in action today is Ukraine. The Ukrainian nation has shown remarkable resistance and resilience in the face of devastating attacks on its population and CI. Large parts of the CI has been destroyed. Bouncing back to the 'old' Ukraine in no longer possible but the prospect of a 'new' Ukraine emerging from the ashes is motivating.

In a recent Ukrainian book called How Nations are Reborn: The Experience of East Asia, the author (Sergiy Korsunsky) draws on lessons of building resilience and particularly from the Japanese who have come through a series of national disasters affecting their CI, from bombing with atomic weapons, meltdowns of nuclear-power plants, major earthquakes, tsunamis and typhoons, to bouncing forward to become a modern industrial state.[1]

The author makes three important points. The first is that the CI is worthless unless communities return to use it. This statement reinforces the message that resilience is ultimately about people. It is people who will generate recovery, usually at ground level, and while having the right infrastructure is important it cannot guarantee regeneration if people and communities feel unsafe. Interestingly, evidence stemming from the earthquake and tsunami that struck Fukushima in 2011 showed conclusively that communities with deeper reservoirs of social capital had higher survival

rates and faster recovery times.[2] By way of contrast, an earthquake in Christchurch in the same year saw a population loss in the rebuilt main urban area: this resulted in the city dropping from being the second-most populous area in New Zealand to third.

The next point is the importance of seizing the opportunity when it arises. This reinforces the message of bouncing forward and the cliché 'building back better'. In the Ukrainians' case, the rebuild is estimated to cost around $411billion+ over a decade. It will be the largest reconstruction of civil infrastructure in Europe since the Second World War. It will present opportunities for transforming parts of the old system into more modern and efficient ones, that will hopefully also have an improved level of redundancy (spare capacity). Efficiency and redundancy can sometimes be uneasy bedfellows and need to be reconciled; both are important in resilience.

The third point is that while money is important the real task is about preparation and planning i.e. anticipation. It is about being proactively protected.[3] The author makes the point that when the war concludes there will be little time for planning so it needs to start now. Lessons learnt from others can greatly help. In Japan, underground electrical substations are a feature that could help Ukrainians avoid disruptions from drone attacks and provide some redundancy. Water drawn from wells proved valuable after the Kobe earthquake in 1995 when the water grid was severely disrupted, while fire foam has been one way of using less water when hydrants are out: all lessons for Ukraine. Such alternatives need to be considered early on and not in isolation as cascading consequences can have a devastating impact on a wide range of services.

Being agile

Preparation and planning for resilience apply across the board to any major disruption. But resilience is not just for disasters or emergencies. It can also apply in between the stresses and shocks. Yet, it still requires the application of agility and adaptation to realise the opportunities.

Take the example of Canary Wharf in London. The Wharf is a massive infrastructure estate built over the past three decades that, alongside the City of London, constitutes one of the main financial centres in the

UK and the world. Finance is one of the UK's designated 13 CI sectors. But change is upon the area.

As hybrid working has reduced the occupancy for many clients, they are seeking smaller footprints in other or modified buildings while undergoing organisational change as a result. This means that Canary Wharf Management is repurposing office space into residential dwellings.[4] Of the 2.4 million square feet currently under construction, three quarters is now earmarked for homes. In turn, this has introduced more shops and leisure facilities, making it an increasingly popular destination, bringing fresh infrastructural demands. A new, third rail connection to the island has, for instance, given both inhabitants and visitors added resilience in travel options. Here is an example of bouncing forward driven by change where both resilience and sustainability combine.

Cause and effect

At the national level, the UK government's Integrated Review and Resilience Framework make much of resilience, including a re-examination of the national risk assessment process as it applies to the CI.[5] The latest, unclassified National Risk Register was published in August.[6]

Traditionally, risk has focused on the panoply of threats facing a company or community measured against the vulnerabilities of those organisations. Enterprise risk management (ERM) has largely been about the operationalisation of risk registers, labelled in red, amber or green, with impact and likelihood managed to the nth degree. This is a mechanistic, quantitative, and siloed approach, and largely backwards facing based on historical probabilities. However, the current period of rapid change means that many modern threats do not have precedence, and certainly do not fit traditionally probabilistic models. Just look at the frequency of flooding when a one-in-a-hundred-year event can now be every few years in some places.

This means we should be analysing consequences and recovery (resilience) as well as causes and vulnerabilities (risks). If we cannot forecast the next major risk then at least we should prepare some generic solutions to deal with the common consequences. Often, different risks can demand similar responses – dealing with a flood or terrorist attack, for example, requires alternative safe locations and compatible communication channels. Clearly, prevention is better than cure when foreseen risks can be avoided or mitigated but with an increasing number of unknown risks then there is little opportunity to have a prevention plan for every emergency. Hence, the threat-agnostic, resilience approach i.e. enterprise resilience management.

Resilient futures

The rapid advance of technology is sure to give resilience a push in a positive direction. The expansion of AI, robotics and quantum technologies, for instance, is significant not only individually but also as a combined set of systems and derived services that support the socio-economic and infrastructural necessities for the future of humankind and our environment. This is even before the merger of infotech and biotech takes us to a whole new level.

But in the final analysis, it is the shocks and stresses on people and communities that will be felt acutely. The so-called 'resilience dividend' will need to focus on ways to help alleviate those stresses at the local level, while combining measures to mitigate the shocks and reimagine new circumstances. Those measures need to be transferred from top to bottom yet actioned from bottom to top. Resilience must marry with sustainability for us to endure and build a brighter, more resilient future.

Building Resilient Futures is available in paperback or e-format from Austin Macauley Publishers Ltd (ISBN 9781035812622). The author, Robert Hall, is currently writing a sequel looking at Natural Resilience: How the natural world can help us understand the key elements of resilience.

An Interview with EU-CIP Project

Ben Lane, CIPRE event manager, met with Emilia Gugliandolo, Senior Researcher, Engineering Ingegneria Informatica S.p.A, Italy, and Project Co-ordinator at EU-CIP

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

In this direction, the partners have already established the European Cluster for Securing Critical infrastructures (ECSCI), which brings together more than twenty-two projects that collaborate in CI Resilience.

Emilia Gugliandolo, Senior Researcher, Engineering Ingegneria Informatica S.p.A, Italy and Project Co-ordinator at EU-CIP

EU-CIP will leverage the capacity, organization, community, and achievements of the ECSCI cluster towards establishing an EU-wide knowledge network with advanced analytical and innovation support capabilities.

Ben Lane (BL): Please describe the ultimate purpose and goals of the

EU-CIP project.

Emilia Gugliandolo (EG): The EU-CIP project is a Coordination and Support Action (CSA) funded by the European Commission under the call topic SSRI (Strengthened Security Research and Innovation). It is a three-year funded project. It started in October 2022 and runs until September 2025. The EU-CIP consortium has twenty partners, including the coordinators of recent European projects, dealing with critical infrastructure and resilient infrastructure that are part of the European Cluster for Securing Critical Infrastructures (ECSCI) that is a knowledge network on resilient infrastructures.

So, the project is a natural evolution of this cluster.

To understand the surrounding landscape, we must consider that innovation and policy development for resilience infrastructure and critical infrastructure protection is a complex process that involves many stakeholders and must analyze a rich set of data and information from various sources. So, some of the main challenges that European policymakers and innovators have to deal with is the need of reducing information fragmentation, in terms of security technologies, policy, standards and so on, and also overseeing the continuous and structured analysis and boosting evidence-based policy-making to ensure a unique ecosystem to engage all relevant stakeholders in this landscape.

The main goal of the EU-CIP is to establish a novel pan-European knowledge network for resilience infrastructure, which will enable policymakers to shape and produce data-driven evidence, while boosting the innovation capacity of critical infrastructures operators, authorities, innovators including small and medium enterprise and startups. And this network will produce insights and foresight on critical infrastructure protection, research, and innovation activities, to help policymaker's operators, innovators in their innovation development activities. In particular, the consortium will base its work on three main pillars:

Pillar one is EU-CIP's ANALYSIS to enhance Europe's analytical capability regarding research outcomes, technologies, and policies and to foster data-driven evidence-based policy and innovation development. So, the EU-CIP project continuously collects and analyzes raw data and information towards producing foresight, insights, and knowledge. The information collected is focused on security research activities and outcomes, security solutions and technologies, security and infrastructure resilience policies, standards and so on.

Pillar two is EU-CIP AMPLIFY to maximize the impact of the research and innovation activities in Europe, through innovation support and solution validation services. So, EU-CIP will provide innovation support services to innovators, such as small medium enterprises and startups to support them in identifying unique selling points, business plans and to commercialize their products. Finally, we will offer a test bed for experimentation with standard-based solution and certification projects.

Pillar three is the EU-CIP ECOSYSTEM that will establish a knowledge hub and create a vibrant ecosystem of interested stakeholders. So, there will be

a pool of different knowledge assets that will be integrated in the knowledge hub. This hub will be a unique point of access to all the resources produced in EU-CIP, in particular a directory of policies and standards, directory of technologies, research outcomes, research and innovation projects, training material, white papers and so on. Also, we will establish Europe's largest community and ecosystem around the analytical services and innovation support services.

BL: In the past you talked about KPIs and how you measure success. Can you provide an overview of how you are measuring the success of this project?

EG: Community-building KPIs, production of support resources, and access to these knowledge resources are especially important for us. In the EU-CIP, we have a key indicator framework that will provide the means for monitoring the activities, the achievement, the performance, and the success of the project. We will have various kinds of indicators; some indicators are linked to the project goals and the objectives to evaluate the extent to

which the project has met the stated objectives and targets.

Then we will have some project performance KPIs around structuring and monitoring the analytical capability of the project, in particular, our KPI related to the scheduled performance, scope performance, quality performance, risk management. And then, we will have another set of indicators known as impact indicators, which are fundamental to assess who is using the results, and their purpose. This indicator demonstrates the usage and appreciation of results by user.

So, by using a combination of these indicators, we can obtain insight into the satisfaction and the value that we will provide to the user. For example, we have a quantitative indicator for the number of people registered in the Knowledge Hub, the engagement in terms of download of material, and participation and satisfaction of the experience.

All these indicators and the KPI framework will help us to assess the success of the project. And these indicators will be regularly monitored.

BL: The project is funded until 2025, so what happens then? What is the next stage?

EG: EU-CIP is expected to continue its operation and activities because the project completion does not imply the termination of our activity. It marks only the end of its initial funding period. So, key outcomes of the EU-CIP project, like the Knowledge Hub will be taken on by a critical infrastructure partner, to maintain it and offer a continuous information & insights to the community.

So, all the knowledge resources, all the deliverables, such as our reports, our white papers, sectorial studies, roadmaps will be disseminated. The project team may continue to update and maintain the online observatory and the Knowledge Hub of the EU-CIP.

Also, we must consider the policy impact and the implementation because the project policy recommendations and roadmaps can potentially influence policymaking and the decision-making processes at the European, national, and regional level. So, we must consider this aspect along with collaboration and follow-up initiatives, knowledge transfer and capacity building, and self-financing models.

BL: How will the exploitation stage of this project develop in the future? And, is there space for other organizations to still join the consortium?

EG: EU-CIP collaborating organizations and partners will benefit by establishing a strong brand name in the community, exploiting individual assets of the project, such as training, innovation, support, consulting services and reinforcing research and innovation projects. But also, there will be training in commercialization to gain a better understanding of the commercial partners, their activities and to provide them support.

In general, the consortium is closed, but EU-CIP is open to the engagement of supporting critical infrastructure operators, vendor solution providers, policymakers, and research project research initiatives.

We already have established the ECSCI cluster, so, we are open to this type of collaboration and involvement of other organizations.

BL: Thank you and we look forward to hearing you speak at CIPRE 2023 in Prague, in the session: EU Horizon Projects Overview session, Thursday October 5th, 2023.

IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs

IBM Security released its annual Cost of a Data Breach Report, showing the global average cost of a data breach reached $4.45 million in 2023 – an all-time high for the report and a 15% increase over the last 3 years. Detection and escalation costs jumped 42% over this same time frame, representing the highest portion of breach costs, and indicating a shift towards more complex breach investigations.

According to the 2023 IBM report, businesses are divided in how they plan to handle the increasing cost and frequency of data breaches. The study found that while 95% of studied organizations have experienced more than one breach, breached organizations were more likely to pass incident costs onto consumers (57%) than to increase security investments (51%).

The 2023 Cost of a Data Breach Report is based on in-depth analysis of real-world data breaches experienced by 553 organizations globally between March 2022 and March 2023. The research, sponsored and analyzed by IBM Security, was conducted by Ponemon Institute and has been published for 18 consecutive years. Some key findings in the 2023 IBM report include:

- AI Picks Up Speed – AI and automation had the biggest impact on speed of breach identification and containment for studied organizations. Organizations with extensive use of both AI and automation experienced a data breach lifecycle that was 108 days shorter compared to studied organizations that have not

deployed these technologies (214 days versus 322 days).

- The Cost of Silence – Ransomware victims in the study that involved law enforcement saved $470,000 in average costs of a breach compared to those that chose not to involve law enforcement. Despite these potential savings, 37% of ransomware victims studied did not involve law enforcement in a ransomware attack.

- Detection Gaps – Only one third of studied breaches were detected by an organization's own security team, compared to 27% that were disclosed by an attacker. Data breaches disclosed by the attacker cost nearly $1 million more on average compared to studied organizations that identified the breach themselves.

"Time is the new currency in cybersecurity both for the defenders and the attackers. As the report shows, early detection and fast response can significantly reduce the impact of a breach," said Chris McCurdy, General Manager, Worldwide IBM Security Services. "Security teams must focus on where adversaries are the most successful and concentrate their efforts on stopping them before they achieve their goals. Investments in threat detection and response approaches that accelerate defenders speed and efficiency – such as AI and automation – are crucial to shifting this balance."

Every Second Costs

According to the 2023 report, studied organizations that fully deploy security AI and automation saw 108-day shorter breach lifecycles on average compared to organizations not deploying these technologies – and experienced significantly lower incident costs. In fact, studied organizations that deployed security AI and automation extensively saw, on average, nearly $1.8 million lower data breach costs than organizations that didn't deploy these technologies – the biggest cost saver identified in the report.

At the same time, adversaries have reduced the average time to complete a ransomware attack. And with nearly 40% of studied organizations not yet deploying security AI and automation, there is still considerable opportunity for organizations to boost detection and response speeds.

Ransomware 'Discount Code'

Some studied organizations remain apprehensive to engage law enforcement during a ransomware attack due to the perception that it will only complicate the situation. For the first time this year, the IBM report looked closer at this issue and found evidence to the contrary. Participating organizations that did not involve law enforcement experienced breach lifecycles that were 33-days longer on average than those that did involve law enforcement – and that silence came with a price. Ransomware victims studied that didn't bring in law enforcement paid on average $470,000 higher breach costs than those that did.

Despite ongoing efforts by law enforcement to collaborate with ransomware victims, 37% of respondents still opted not to bring them in. Add to that, nearly half (47%) of studied ransomware victims reportedly paid the ransom. It's clear that organizations should abandon these misconceptions around ransomware. Paying a ransom, and avoiding law enforcement, may only

drive-up incident costs, and slow the response.

Security Teams Rarely Discover Breaches Themselves

Threat detection and response has seen some progress. According to IBM's 2023 Threat Intelligence Index, defenders were able to halt a higher proportion of ransomware attacks last year. However, adversaries are still finding ways to slip through the cracks of defense. The report found that only one in three studied breaches were detected by the organization's own security teams or tools, while 27% of such breaches were disclosed by an attacker, and 40% were disclosed by a neutral third party such as law enforcement.

Responding organizations that discovered the breach themselves experienced nearly $1 million less in breach costs than those disclosed by an attacker ($5.23 million vs. $4.3 million). Breaches disclosed by an attacker also had a lifecycle nearly 80 days longer (320 vs. 241) compared to those who identified the breach internally. The significant cost and time savings that come with early detection show that investing in these strategies can pay off in the long run.

Additional findings in the 2023 IBM report include:

- Breaching Data Across Environments – Nearly 40% of data breaches studied resulted in the loss of data across multiple environments including public cloud, private cloud, and on-prem—showing that attackers were able to compromise multiple environments while avoiding detection. Data breaches studied that impacted multiple environments also led to higher breach costs ($4.75 million on average).

- Costs of Healthcare Breaches Continue to Soar – The average costs of a studied breach in healthcare reached nearly $11 million in 2023 – a 53% price increase since 2020. Cybercriminals have started making stolen data more accessible to downstream victims, according to the 2023 X-Force Threat Intelligence Report. With medical records as leverage, threat actors amplify pressure on breached organizations to pay a ransom. In fact, across all industries studied, customer personally identifiable information was the most commonly breached record type and the costliest.

- The DevSecOps Advantage – Studied organizations across all industries with a high level of DevSecOps saw a global average cost of a data breach nearly $1.7 million lower than those studied with a low level/no use of a DevSecOps approach.

- Critical Infrastructure Breach Costs Break $5 Million – Critical infrastructure organizations studied experienced a 4.5% jump in the average costs of a breach compared to last year – increasing from $4.82 million to $5.04 million – $590K higher than the global average.

New Research Reveals Critical Infrastructure Employees Are More Likely to Detect and Report Phishing and Malicious Emails

Hoxhunt, the market leader in security behavior change, released the findings of its latest research, the 'Human Cyber-Risk Report: Critical Infrastructure'. This report, which examined human risk in the critical infrastructure sector, analyzed over 15 million phishing simulations and real email attacks reported in 2022 by 1.6 million people participating in security behavior change programs. The research highlights that critical infrastructure employees are comparatively more engaged in organizational security, as their phishing reporting and miss rates indicate.

The report revealed that 66 percent of active participants in security behavior training programs at critical infrastructure organizations detect and report at least one real malicious email attack within a year of commencing training. Resilience velocity, the speed at which an organization reaches its highest level of actual threat detection behavior, is also 20 percent higher in the critical infrastructure sector, with organizational threat detection rates reaching high points at 10 months, compared to the 12-month average in most other industries.

Phishing simulation success rates, the act of reporting a simulation and not skipping or failing it, in critical infrastructure is 61 percent higher than the global average after 12 months. In addition, resilience ratios, success rate versus failure rate, is 51 percent higher in critical infrastructure - 10.9 for critical infrastructure compared to the 7.2 global industry average.

The report also reveals that critical infrastructure employees are most likely to fall victim to spoofed internal organizational communications. While this is the most effective type of phishing attack across most sectors, Hoxhunt's study found that these types of attacks induce an 11.4 percent higher failure rate in the critical infrastructure sector compared to global averages.

"Over the past several years, attacks on critical infrastructure have become all too common, leaving fuel pumps and store shelves empty," said Mika Aalto, CEO and co-founder of Hoxhunt. "In response, critical infrastructure organizations and their employees are exponentially more aware and cautious of malicious activity. This higher state of caution has spurred many security and risk leaders to move away from traditional security awareness programs and choose new innovations like Security Behavior Change products to achieve true risk reduction."

The research also highlights that communication, marketing, and business development departments are most likely to be victims of phishing attacks. The most resilient departments are finance, sales, and legal. These results track with global averages except for the high performance of sales, whose success in critical infrastructure is greater than the global average.

Using the EU Space Programme for disaster risk management in Hungary

The recent severe droughts and extremely high temperatures in Hungary, led rivers and lakes to dry up, negatively impacting the country's economy and ecosystem. With that in mind, EUSPA, together with the Ministry of Foreign Affairs and Trade of Hungary and Eurisy, co-organised a workshop on Satellite-based Services for Disaster Risk Management. Held in Budapest, the workshop brought together national and regional stakeholders to discuss how satellite-based services can support both disaster risk management and search and rescue operations.

Dr. Orsolya Ferencz, Ministerial Commissioner for Space Research at the Ministry of Foreign Affairs and Trade, presented an overview of Hungary's space strategy and outlined its implementation milestones. Speaking about the workshop, Dr Ferencz stated, "This gathering is important in addressing the challenges we face in emergency situations. By leveraging innovative tools and satellite technologies, we can make evidence-based decisions and better respond to disasters."

Visualising with Copernicus

Copernicus, the EU Earth Observation programme provides up to date, near real-time optical information about disasters such as wildfires and floods.

More precisely, the Copernicus Emergency Management Service (Copernicus EMS) uses data from a range of satellites and ground-based sensors to provide information about the location, extent, and behaviour of fires and floods. This information helps emergency responders make informed decisions regarding where to direct resources and in the case

of fires, how to contain the blaze. The service is provided free of charge to all users.

But there's more. Wildfires are a significant source of air pollution which poses a threat to human, animal, and plant populations.

When a disaster such as a wildfire strikes a region, it is important to have access to precise and up-to-date information for the delivery of an effective disaster management response. The Copernicus Atmosphere Monitoring Service (CAMS) can monitor emissions which can, in turn, be used in smoke forecasts. These forecasts are used in air quality apps to help people limit their exposure to pollution, and by policymakers and local authorities to manage the impact of fires.

Secure and reliable positioning with Galileo and EGNOS

Galileo, the EU global navigation satellite system and EGNOS the EU's regional navigation system have revolutionised various sectors of the European economy such as agriculture and transportation. But their contribution goes even further by helping to save lives.

Take for example the European 112-emergency number. As of March 2022, it became mandatory for all mobile phones sold in the European Single Market to be Galileo enabled. When someone places an emergency call, the emergency responder will receive their location information with an accuracy down to just a few metres. The improved accuracy has a major impact in terms of response times, ultimately allowing for quicker intervention in emergency situations where every second counts – resulting in more lives being saved. The ability for 112 to communicate a caller's location automatically to emergency services is possible

thanks Advanced Mobile Location (AML) system which is already available in Hungary.

Likewise, in case medical assistance is needed, helicopter operators and pilots can rely on EGNOS to land safely, especially when visibility is reduced due to fire smoke or fog. Additionally, services like the Galileo High Accuracy and OSNMA services ensure that drones deliver accurate mapping as well as assistance to inaccessible areas due to natural disasters such as earthquakes.

Communicating with GOVSATCOM and IRIS2 programmes

GOVSATCOM and IRIS2 will provide robustly protected communication, filling the gap for secure communication alongside Galileo and Copernicus. These solutions enable secure and cost-efficient communication for critical missions, operations, and infrastructure. EUSPA, in collaboration with Member States and other entities, oversees the procurement, operations, and user coordination of the secure ground segment (GOVSATCOM Hubs).

The power of synergy

Rodrigo da Costa, Executive Director of EUSPA, provided the European perspective on the integrative use of components from the European Space Programme. "Galileo, EGNOS, Copernicus, are powerful tools individually, but an exponential achievement is reached when used in synergy. Soon, the addition of GOVSATCOM and IRIS² will add an extra layer of efficiency in the management of disasters by providing secured and uninterrupted satellite communications to EU Member States. The Emergency Management and Disaster Response sector is one of the key sectors where this synergy is saving lives". "As an agency focused on meeting user needs, EUSPA closely monitors this market and actively develops and delivers new space-enabled services to address its requirements" he stated.

European Union Agency for the Space Programme (EUSPA).
www.euspa.europa.eu

An Interview with TIEMS

Ben Lane, CIPRE event manager, met Harald Drager, The International Emergency Management Society (TIEMS) President

Ben Lane (BL): Hello Harald. Can you give us a little bit of information about yourself, why you are here?

Harald Drager (HD): My name is Harald Drager. I was born and raised in Norway. I received an engineering education and worked with Det Norske Veritas for 15 years. I started my own company, and we specialized in emergency management issues on communication and evacuation. Based on that, I met a group in the US who dealt with emergency management, and we agreed to start TIEMS International Emergency Management Society. This was in 1993. I took over as president in 2002 and since then it has developed into an international organization.

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

BL: Let's look at TIEMS itself and the first point I was going to ask you is the ultimate goals and the ultimate aims of the society.

HD: We have made up what I call a vision statement; and we say that

TIEMS inspires to be the leading organization for international emergency management professional development. And we have a very big mission, namely that TIEMS is a global forum for emergency management and disaster risk reduction that builds capacity to prepare for, respond to and recover from disasters and climate change impacts. And we work to achieve this mission through exchange of information, innovation and good practices in education, training and certification and research development activities. TIEMS is about education, experience and communication.

BL: You talk about creating a "safer world". And that struck me as interesting because it's a big statement. Can you qualify that statement.

HD: TIEMS prepares the world for emergencies. We are a global forum for education, training, certification, and policy for emergency and disaster management. We do not respond to emergencies: we ensure that others are ready to respond. This is important internationally because some parts of the world have limited support for preparation.

As the international community discovers and develops new technologies, methodologies, and best practices, we offer conferences, ongoing forums, and training courses that rapidly and continuously spread the knowledge to every corner of the community. As policy makers grow to understand the need for preparation and the support TIEMS provides, we expect to influence policy choices that strengthen cooperation among regional communities before a disaster

strikes.

I see too little education, too little thinking ahead, and too little political will to fix problems before they happen. Also, the media likes to dramatize results, but often they over dramatize events, and this leads people to think that warnings are all hype.

Communication often fails in emergencies, and we may seem to "never learn" by repeating errors over again. Improving global communication focusing on and agreeing on a common global language, knowledge and understanding of international emergency management and disaster response through education training and certification is in my opinion an important measure.

BL: Can you explain a little bit about the TIEMS connections with other bodies worldwide?

HD: Well, we have been doing this for 30 years, so we are getting more and more, let's say, proficient. We are focused on our international conference and workshops, which we do every year. We move around the world because the local context is very important. For example, this year we are in South Africa and the South African chapter of TIEMS are responsible for the conference.

We also run webinars where we ask civil protection departments from around the world to attend and speak. We explore how they do their emergency management and civil protection. We do research and development activities. We have also established an international certification and we explore new emerging technologies such as artificial intelligence, to understand how these technologies can be used in emergency management.

BL: How is TIEMS funded?

HD: We are a not-for-profit NGO. We are a voluntary organization so everybody working for the organization is not paid, they do it on a voluntary basis. We generate income from membership fees and paid-for research.

BL: Tell us a bit more about the importance of the chapters and the regional focus and why that was set up and how that is beneficial.

HD: We started out in Washington DC and, we moved the annual conference between Europe and North America. But when I took over as president, my goal was to make this an international organization to address the different cultural aspects when we do emergency management. If you go to Africa, they might be primitive in some of their approaches, but some of their approaches could be useful in other parts of the world.

BL: Can you provide a recent case study that shows the impact and the outcomes that you are particularly happy about?

HD: TIEMS was invited by the World Bank to participate in a global study of Civil Protection Worldwide.

The aim of the study was:

Investigate the State of Civil Protection in the World: Typologies, Good Practices and Economic Returns" to deepen the overall knowledge on civil protection, understand good practices, challenges and lessons-learnt, and to build consensus within the DRM community on this important area for disaster risk management and resilience.

TIEMS contributed with a report on the following countries, China, Australia and Ukraine. I think the final report was very enlightening and showed how civil protection practice was worldwide and what economic resources was available for civil protection in different countries, and how it in many cases was a limitation factor for efficient emergency management in many countries. Unfortunately, the report was never published by the World Bank for unknown reasons.

BL: Thank you. That's great. You are going to be attending CIPRE 2023 in Prague in October.

HD: Yes. I look forward for that.

BL: We are looking forward to seeing you there. You're coming with a colleague from the Czech Republic, I gather?

HD: Yeah, he lives there so it's good for him to be there as well.

BL: You are in the crisis management session, I believe, and we'll hear more about the work of TIEMS, which will be interesting. Thank you, Harold, and see you soon.

HD: Thank you.

ABOUT TIEMS

- TIEMS was founded in Washington, USA in 1993, and is today registered as an international, independent, not for profit NGO in Belgium, see Certificate

- TIEMS is a global forum for education, training and certification in emergency and disaster management.

- TIEMS international expert network comprises users, planners, researchers, industry, managers, response personnel, practitioners, social scientists, and other interested parties within emergency and disaster management.

- Within its network TIEMS stimulates to the exchange of information on the use of innovative methods and technologies within emergency and disaster management to improve society's ability to avoid, mitigate, respond to, and recover from natural and technological disasters.

- TIEMS works locally through its worldwide chapters which provide a regional focus for TIEMS activities.

- TIEMS activities comprise international conferences, workshops and exhibitions, research and technology development projects, task force groups of experts from TIEMS international group of experts, and TIEMS academy providing international education, training and certification programs.

- TIEMS offers membership, sponsorship and partnership.

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 AND RESILIENCE EUROPE

3rd-5th October 2023
Prague, Czech Republic
www.cipre-expo.com

Securing the Inter-Connected Society

Preliminary Conference Programme

Your invitation and guide to the premier discussion

UN Member States need "to share information [...] to prevent, protect, mitigate, investigate, respond to and recover from damage from terrorist attacks on critical infrastructure facilities, including through joint training, and use or establishment of relevant communication or emergency warning networks."

Co-Hosted by:

International Association of CIP Professionals

MINISTRY OF INDUSTRY AND TRADE OF THE CZECH REPUBLIC

Tomas Bata University in Zlin, Faculty of Applied Informatics

VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF SAFETY ENGINEERING

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Supporting Organisations:

Media Partners:

CIPRE – Where CIIP/Cyber and Physical Security Meet

Attacks on critical infrastructure sites are now a fact of life not simply a potential threat. Power stations, chemical plants, nuclear facilities are routinely targeted by cyber-attacks, the most successful so far being the Ukraine power outage that caused 225,000 customers to lose electricity. Last year an activist landed a UAV carrying small traces of radiation on the roof of the Japanese Premier's office and this year a UAV collided with a aircraft at London's Heathrow airport. And of course the terrible attacks on the metro and airport in Brussels. This is just the start of what we can expect to be the repeated targeting of our critical infrastructure. The potential effects not only in terms of loss of life but also in terms of damage to infrastructure, economic disruption and costs, can be enormous.

Once again widespread flooding across Europe in 2015 caused even bigger outages of power and for longer periods than cyber-attacks and the damage to lives, property and businesses was larger still, emphasising the need for planning and preparation on European scale.

We must be prepared!

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

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

Why the Need for Such a Discussion?

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

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

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

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

Attend CIPRE 2023 to learn about the importance of the updated NIS2 Directive…

An important discussion will centre around the EU cybersecurity rules introduced in 2016 and updated by the NIS2 Directive that came into force in 2023. It modernised the existing legal framework to keep up with increased digitisation and an evolving cybersecurity threat landscape. By expanding the scope of the cybersecurity rules to new sectors and entities, it further improves the resilience and incident response capacities of public and private entities, competent authorities and the EU as a whole.

Also learn about the importance of the new directive on the Resilience of Critical Entities…

The Directive on the Resilience of Critical Entities entered into force on 16 January 2023. Member States have until 17 October 2024 to adopt national legislation to transpose the Directive.

The Directive aims to strengthen the resilience of critical entities against a range of threats, including natural hazards, terrorist attacks, insider threats, or sabotage, as well as public health emergencies.

Follow us:

Critical Infrastructure Protection / Physical Security

Drone's, Insider threats, Vehicle Borne IED's, Suicide Bombers and Active Shooters are just some of the myriad of known threats facing CNI operators in 2019. Identifying ways of detecting, defeating and mitigating against those threats and building-in resilience are crucial organisation or CNI operator.

Critical Information Infrastructure Protection / Cyber Security

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

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

Why Attend?

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

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

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

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

For conference or registration queries please contact:
Neil Walker
Events Director
T: +44 (0) 7725 318601
E: neilw@torchmarketing.co.uk

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

Who Should Attend

Critical Infrastructure Protection and Resilience Europe is for:

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

Schedule of Events

Tuesday 3rd October 2023

3.00pm - 3.30pm - Ministerial Opening Keynote

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

4.00pm-5:30pm - Session 1: Interdependencies and Cascading Effects across the CI Communities

5:45pm - Networking Reception

Wednesday 4th October 2023

Track One

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

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

11:15am - 12:30pm - Session 3a: Power & Energy Sector Symposium

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

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

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

4:15pm - 5:30pm - Session 5a: Transport Sector Symposium

Track Two

9:00am-10:30am - Session 2b: Crisis Management, Coordination & Communication

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

11:15am - 12:30pm - Session 3b: Government, Defence & Space Sector Symposium

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

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

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

4:15pm - 5:30pm - Session 5b: CBRNE Sector Symposium

Thursday 5th October 2023

Track One

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

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

11:15am - 12:30pm - Session 7a: The Insider Threat

Track Two

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

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

11:15am - 12:30pm - Session 7b: Business Continuity Management

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

2pm-3:30pm - Session 8: EU Horizon Projects Overviews

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

HOW TO REGISTER

1. Online at **www.cipre-expo.com.**
2. Complete the Registration Form at the back of this booklet and email to: **cipre@torchmarketing.co.uk.**
3. Complete the Registration Form at the back of this booklet and fax to +44 (0) 872 111 3210.
4. Complete the Registration Form at the back of this booklet and mail to:
   CIPRE, Torch Marketing, 200 Ware Road, Hoddesdon, Herts EN11 9EY, United Kingdom.

EARLY BIRD DISCOUNT - deadline 3rd September 2023

Register yourself and your colleagues as conference delegates by 3rd September 2023 and save with the Early Bird Discount.

Discounts for Members of Supporting Associations

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

- Association of Critical Infrastructure of Czech Republic (AKICR)
- National Security & Resilience Consortium (NS&RC)
- International Association of CIP Professionals (IACIPP)
- Confederation of European Security Services (CoESS)
- Institute of Engineering & Technology (IET)
- Security Partners Forum (SPF)

Check the Registration Form at the back of this booklet for full details.

On-Site Registration Hours

Tuesday 3rd October	1.00pm to 5.00pm
Wednesday 4th October	8.30am to 5.00pm
Thursday 5th October	8.30am to 2.00pm

Tuesday 3rd October

Conference Programme

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

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

Ing. Jozef Síkela, Minister of Industry and Trade, Czech Republic

LG Vladimir Vicek, General director of the Fire and Rescue System, Prevention and Civil Emergency Preparedness, Czech Republic

Adrian Victor Vevera, General Director, National Institute for Research and Development, Informatics ICI Bucharest, Romania

---

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

4:00pm-5:30pm - Plenary Session 1: Interdependencies and Cascading Effects across the CI Communities

It is the interoperability between independent critical national infrastructures that is the catalyst for multiple failures in the so called cascade effect. As more infrastructure becomes increasingly interdependent, how do we identify the weaknesses to enhance resilience across industries to prevent and/or mitigate the effects of a natural disaster or man-made attack? How should the CI community build situational awareness to mitigate the cascading effect across infrastructures.

Chris Rodriguez, Director of Homeland Security and Emergency Management for Washington DC, USA

Cyber-Physical Security and Critical Infrastructure - Catherine Piana, Secretary General, CoESS

Frederic Petit, Project Officer, European Commission, Joint Research Centre

Update on Directive on the Resilience of Critical Entities - Alessandro Lazari, Senior Key Account Manager, F24

Martin Hromada, Security Research Project Manager, Tomas Bata University, Czech Republic

---

5:45pm-7:30pm - Networking Reception

**invited*

Wednesday 4th October

Track One

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

The ever changing nature of threats, whether natural, through climate change, or man-made through terrorism activities and insider threats, and coupled together with the latest challenges with cyber attacks from many directions, creates the need to continually review and update policies, practices and technologies to meet these growing demands. But what are those emerging threats, both physical and cyber, and how can we identify, monitor and manage their levels of potential damage?

Global threats and local threats to Cis - Lina Kolesnikova, Security Expert

Daniel Golston, Associate Programme Officer, Action Against Terrorism Unit, OSCE

Hybrid Threats Against CI - Senior Representative, European Commision Joint Research Centre*

TBC

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

11:15am - 12:30pm - Session 3a: Power & Energy Sector Symposium

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

Ing. Jindrich Sip MBA, Head of Business Continuity Management, CEZ, Czech Republic

Senior Representative, EUTC*

Modeling resilience of German offshore energy infrastructures - Arto Niemi, Research Team Leader, DLR Institute for the Protection of Maritime Infrastructures

TBC

Track Two

9:00am-10:30am - Session 2b: Crisis Management, Coordination & Communication

Planning and preparation is the key to ensuring that CI and venue operators have the right equipment, processes and procedures in place to respond in the event of an emergency. Coordination and information sharing is essential for situational awareness and can improve the planning process. How do we better coordinate and co-operate to enhance protection and resilience.

Fitting national CIP legislation to new EU CER framework in a view of prospect for better coordination and management - Ivana Cesarec, Head of CI and Cultural Heritage Dept, Civil Protection, Croatia

Harald Drager, President & Jaroslav Pejcoch, Secretary to TIEMS

Javier Larraneta, Secretary General, PESI

Markus Epner, Head of Academy, F24 AG, Germany

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

11:15am - 12:30pm - Session 3b: Government, Defence & Space Sector Symposium

As we rely more and more heavily on satellites for communications, navigation, observation and security/ defence, the requirement to ensure that space based systems are both secure and resilient becomes more urgent. Government networks and systems need to lead security and resilience across agencies and departments for confidence throughout the CI sectors and communities. What impact does the Government, Defence and Space based systems have as a growing role in CI resilience.

Eugen-Liviu Militaru, Senior Security Officer, Head of the Protective Security and Continuity Sector, eu-LISA

Building the cybersecurity of the eGovernment cloud - Ondrej Nekovar, CISO, Chief Deception Officer, State Treasury Shared Services Centre, the Ministry of Finance

Roya Ayazi, Secretary General, NEREUS

Erica Bustinza, Program Director, USAID Critical Infrastructure Digitization and Resilience Program (CIDR) at DAI Center for Digital Acceleration*

12:30pm - Delegate Networking Lunch

Wednesday 4th October

Track One

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

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

Paolo Grassia, Director of Public Policy for Cybersecurity, ETNO

Senior Representative, National Cyber and Information Security Agency, Czech Republic

Senior Representative, EUTC*

TBC

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

4:15pm - 5:30pm - Session 5a: Transport Sector Symposium

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

John Laene, Strategic Asvisor, RAILPOL

International cooperation for a better future of transport and traffic - Jana Pelešková, Chief Commissioner, Police Presidium of the Czech Republic, directorate of traffic police

Enhancing Port Security and Resilience: Towards a Holistic Approach for Real-time Performance Monitoring and Threat Mitigation - Babette Tecklenburg, Researcher, Institute for the protection of maritime infrastructures, German Aerospace Center (DLR)

Fusion Threat Intelligence: Concept, Practice, and Future Use in the Transport Sector - Natasia Kalajdziovski, Senior Fusion Threat Intelligence Analyst, SecAlliance

Track Two

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

Securing the digital infrastructure. Information technology is responsible for such a large portion of our workforce, business operations and access to information and data, Critical Information Infrastructure Protection (CIIP) through cybersecurity and network security, is vital to protect information assets. Recent ransomware attacks and other threats, such as Malware, Stuxnet, etc and the continued cyber threats and intrusions, means we have to be more vigilant to protect our information assets.

Martin Švéda, Head of the Private Sector Regulation Unit, National Cyber and Information Security Agency (NÚKIB)

Get ready for the transformative effect of blockchain on critical infrastructures - Adrian Victor Vevera, General Director, National Institute for Research and Development, Informatics ICI Bucharest, Romania

Human Factor Control to protect industrial companies against phishing attacks - Mohammed Al-Ghamdi, Information Security Analyst, Saudi Aramco

International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance) - Dr. Sandeep Pirbhulal, Senior Research Scientist, Norwegian Computing Centre, Norway

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

4:15pm - 5:30pm - Session 5b: CBRNE Sector Symposium

Sectors such as Chemicals, Nuclear and Water/Wastewater are as much at threat from an attack as a threat they pose that could include CBRNE agents in terrorist attacks against CI. The convergence of biological and cyber sector issues also characterises an evolving frontier in health security, and mitigation of such attacks is as much of a consideration as post attack resilience.

ERNCIP Chemical and Biological (CB) Risks to Drinking Water Thematic Group - Frederic Petit, Project Officer, European Commission, Joint Research Centre

Thomas Fojtik, Director, T.G. Masaryk Water Research Institute, Czech Republic

František Paulus, Director of Population Protection Institute, Czech Republic

Thursday 5th October

Track One

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

What are some of the latest and future technologies, from ground surveillance, space based or cyber technology, to predict or detect the wide range of potential threats to CNI.

How Unified Physical Security Solutions Help You Thrive in Evolving Times - Jakub Kozak, Regional Sales Manager, Genetec

Seyit Ali Kaya Regional Manager, Eastern Europe, Central Asia, and Türkiye, Iris ID Systems

Communication Systems & Technologies Engineer, European Space Agency*

TBC

10.30am-11:15am - Networking Coffee Break

11:15am - 12:30pm - Session 7a: The Insider Threat

An insider threat is a perceived danger to your company that originates from individuals who work there, such as current or former employees, contractors, or business partners, who have inside knowledge of the company's security procedures, data, and computer systems. The main objectives of malevolent insider threats are espionage, fraud, intellectual property theft, and sabotage, for monetary, private, or malicious purposes, they wilfully misuse their priviledged access to steal information or damage systems. Here we take a deeper dive into the range of threats and how to mitigate and counter these.

John Donlon, Chairman, International Association of CIP Professionals

Peter Nilsson, Head of AIRPOL

Sarah-Jane Prew, Senior Security Consultant, Arup UK

Catherine Piana, Managing Director, Help2Protect, Belgium

Track Two

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

Being prepared for the changing threat environment can benefit greatly in mitigating its impact on infrastructure and the broader community, ensuring resilience, safety and security. How can we counter these emerging physical and cyber threats to minimise loss of service and financial impact?

Designing Security for when CNI and Crowded Places meet - Sarah-Jane Prew, Senior Security Consultant, Arup UK

Person-Centric Artificial Intelligence for Critical Infrastructure Surveillance - Amr el Rahwan, International Security Expert, TPASCO (Terrorism Prevention & Anti Social Crime Organization)

Addressing Consequence within Operational Risk - Ollie Gagnon, Strategic Advisor, Critical Infrastructure Security and Resilience, Idaho National Laboratory, USA

What you don't measure you don't know! - Peter Braun, Sales Manager, Telespazio Germany

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

11:15am - 12:30pm - Session 7b: Business Continuity Management

How to we develop and plan the best resilience strategies within our CI community? Through discpline in information sharing and making infrastructure preparedness personal, we can help to build resilience into our infrastructures that benefit the whole community.

A Serious Game for Coordinated Business Continuity Planning - Boris Petrenj, Senior Researcher, Politecnico di Milano, Italy

Marco Buldrini, Head of Major Risks Unit, NIER Ingegneria S.p.A., Italy

Stefano A. Fulgi, Head of Internal Audit, F.I.S. Fabbrica Italiana Sintetici S.p.A., Italy

TBC

12:30pm - Delegate Networking Lunch

Thursday 5th October

2:00pm-3:30pm - Plenary Session 8: EU Horizon Projects Overviews

A deeper look at the current range of Horizon Europe Critical Infrastructure Protection & Resilience projects and research programmes across Europe that are designed to enhance critical infrastructures and understandings for adapting policies and adopting best practices.

SATIE Project - Tim Stelkens-Kobsch, Project Manager, DLR, Germany

EU-CIP Project - Emilia Gugliandolo, Project Coordinator, ENG, Italy

Sunrise Project - Tomáš Trpišovský, Institut mikroelektronických aplikací s.r.o. (IMA)

CyberSEAS Project - Ilja David, OT Cyber Resilience & Cyber Security Architect, KPCS CZ

PARADeS Project - Roman Schotten, Research Assistant, University of Applied Science Magdeburg Stendal

---

3.30pm - Conference Close

John Donlon QPM, FSI, Conference Chairman

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

Early Bird Deadline - 3rd September 2023

Networking Reception

Tuesday 3rd October
5.45pm - 7:30pm

In cooperation with the The Ministry of Industry and Trade, Tomas Bata University in Zlin and Technical University of Ostrava, we invite you to joins us at the end of the day for the Networking Reception, which will see the CNI security industry management professionals and delegates gather for a more informal reception.

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

The Networking Reception is free to attend and will take place in the Grandium Hotel, just a few short steps from the Ministry of Trade & Industry Building, Policta Prisoners 931.

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

We look forward to welcoming you.

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

Accommodation

Event HQ Hotel

Grandium Hotel
Politických vězňů 913/12 (Political Prisoners 913/12)
Prague

Critical Infrastructure Protection & Resilience Europe event HQ hotel for the 2023 event is the Grandium Hotel Prague, just 100m from the event venue of the Ministry of Trade & Industry Buildings, Political Prisoners 931.

www.hotel-grandium.cz/en

Additional / Alternative Hotels

Additional hotels all within a 2 minute walk of the venue:

Esplanade Hotel Prague
Washingtonova 1600/19
www.esplanade.cz

Falkensteiner Hotel Prague
Opletalova 1402/21
www.falkensteiner.com/hotel-prague

Occidental Praha Wilson hotel
Václavské nám. 110 00/812/59
www.barcelo.com/en-gb/occidental-praha-wilson

Boutique Hotel Jalta
Václavské náměstí 45/818
www.hoteljalta.com/en

Sponsors and Supporters:

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience Europe 2023.

Co-Hosted by:

International Association of CIP Professionals

MINISTRY OF INDUSTRY AND TRADE OF THE CZECH REPUBLIC

Tomas Bata University in Zlín
Faculty of Applied Informatics

VSB TECHNICAL UNIVERSITY OF OSTRAVA | FACULTY OF SAFETY ENGINEERING

Bronze Sponsor:

Genetec™

Lanyard Sponsor::

SecAlliance

Supporting Organisations:

TECHNOLOGICKÁ PLATFORMA ENERGETICKÁ BEZPEČNOST ČR

Asociace kritické infrastruktury České republiky

STIME

CoESS

PESI
PLATAFORMA TECNOLÓGICA ESPAÑOLA DE SEGURIDAD INDUSTRIAL

EU-CIP

Help2Protect

IET.tv

NS&RC

ISIO
ISIO - International Security Industry Organization

Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

Media Supporters:

TSI TRANSPORT SECURITY INTERNATIONAL
READ LATEST ISSUE TSI-MAG.COM/CURRENT

critical infrastructure PROTECTION AND RESILIENCE EUROPE

3rd-5th October 2023
Prague, Czech Republic
www.cipre-expo.com

DELEGATE REGISTRATION FORM

EARLY BIRD SAVINGS
Book your delegate place by 3rd September 2023 and save with the Early Bird rate

REGISTRATION IS SIMPLE
1. Register online at www.cipre-expo.com/onlinereg
2. Complete this form and email to: cipre@torchmarketing.co.uk
3. Complete this form and fax to +44 (0) 872 111 3210
4. Complete this form and mail to: CIPRE 2021, Torch Marketing, 200 Ware Road, Hoddesdon, Herts EN11 9EY, UK.

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

Title: _____ First Name: _____

Surname: _____

Job Title: _____

Company: _____

E-mail: _____

Address: _____

Street: _____

Town/City: _____

County/State: _____

Post/Zip Code: _____

Country: _____

Direct Tel: (+) _____

Mobile: (+) _____

Passport No (for security clearance) _____

Signature : _____ Date: _____

(I agree to the Terms and Conditions of Booking)

PARTICIPATION FEES

GOVERNMENT, MILITARY AND PUBLIC SECTOR/AGENCY
Individual Full Delegate
(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and 2 lunches, plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)
- ☐ Paid before 3rd September 2023 ..... €195
- ☐ Paid on or after 3rd September 2023 ..... €295

OPERATORS OF INFRASTRUCTURE
Individual Full Delegate
(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and 2 lunches plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)
- ☐ Paid before 3rd September 2023 ..... €195
- ☐ Paid on or after 3rd September 2023 ..... €295

COMMERCIAL ORGANISATIONS
Individual Full Delegate
(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and lunch plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)
- ☐ Paid before 3rd September 2023 ..... €395
- ☐ Paid on or after 3rd September 2023 ..... €595

Individual Day Delegate
(includes participation on one day, coffee breaks and lunch on the day plus ONE YEAR BASIC MEMBERSHIP of IACIPP)
- ☐ Paid before 3rd September 2023 ..... €250
- ☐ Paid on or after 3rd September 2023 ..... €350

Attending on: ☐ 3rd Oct ☐ 4th Oct ☐ 5th Oct

Sponsor Full Delegate
(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and lunch plus ONE YEAR PREMIUM MEMBERSHIP of IACIPP)
- ☐ Paid before 3rd September 2023 ..... €195
- ☐ Paid on or after 3rd September 2023 ..... €295

Student Full Delegate
(includes 3 day participation, conference proceedings, keynote, networking reception, coffee breaks and lunch) - Student ID required
- ☐ Paid before 3rd October 2023 ..... €195

Terms and Conditions of Booking

Payment: Payments must be made with the order. Entry to the conference will not be permitted unless payment has been made in full prior to 3rd October 2023.
Substitutions/Name Changes: You can amend/change a delegate prior to the even start by notifying us in writing. Two or more delegates may not 'share' a place at an event. Please ensure separate bookings for each delegate. Torch Marketing Co. Ltd. reserve the right to refuse entry.
Cancellation: If you wish to cancel your attendance to the event and you are unable to send a substitute, then we will refund/credit 50% of the due fee less a £100 administration charge, providing that cancellation is made in writing and received before 3rd September 2023. Regretfully cancellation after this time cannot be accepted. If we have to cancel the event for any reason, then we will make a full refund immediately, but disclaim any further liability.
Alterations: It may become necessary for us to make alterations to the content, speakers or timing of the event compared to the advertised programme.
Data Protection: Torch Marketing Co. Ltd. gathers personal data in accordance with the UK Data Protection Act 1998 and we may use this to contact you by telephone, fax, post or email to tell you about other products and services.
Please tick if you do not wish to be contacted in future by:
☐ Email ☐ Post ☐ Phone ☐ Fax

PAYMENT DETAILS
(METHOD OF PAYMENT - Conference fees are subject to Czech VAT at 21%.)

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

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

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

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

Card No: _____

Valid From ____ / ____ Expiry Date ____ / ____

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

Cardholder's Name: _____

Signature: _____ Date: _____

I agree to the Terms and Conditions of Booking.

Complete this form and fax to +44 (0) 872 111 3210 or email to cipre@torchmarketing.co.uk

Ransomware Accounts for 54% of Cybersecurity Threats

The European Union Agency for Cybersecurity (ENISA) releases today its first cyber threat landscape for the health sector. The report found that ransomware accounts for 54% of cybersecurity threats in the health sector.

The comprehensive analysis maps and studies cyberattacks, identifying prime threats, actors, impacts, and trends for a period of over 2 years, providing valuable insights for the healthcare community and policy makers. The analysis is based on a total of 215 publicly reported incidents in the EU and neighbouring countries.

The report reveals a concerning reality of the challenges faced by the EU health sector during the reporting period.

- Widespread incidents. The European health sector experienced a significant number of incidents, with healthcare providers accounting for 53% of the total incidents. Hospitals, in particular, bore the brunt, with 42% of incidents reported. Additionally, health authorities, bodies and agencies (14%), and the pharmaceutical industry (9%) were targeted.

- Ransomware and data breaches. Ransomware emerged as one of the primary threats in the health sector (54% of incidents). This trend is seen as likely

to continue. Only 27% of surveyed organisations in the health sector have a dedicated ransomware defence programme. Driven by financial gain, cybercriminals extort both health organisations and patients, threatening to disclose data, personal or sensitive in nature. Patient data, including electronic health records, were the most targeted assets (30%). Alarmingly, nearly half of all incidents (46%) aimed to steal or leak health organisations' data.

- Impact and lessons learned by the COVID-19 Pandemic. It is essential to note that the reporting period coincided with a significant portion of the COVID-19 pandemic era, during which the healthcare sector became a prime target for attackers. Financially motivated threat actors, driven by the value of patient data, were responsible for the majority of attacks (53%). The pandemic saw multiple instances of data leakage from COVID-19-related systems and testing laboratories in various EU countries. Insiders and poor security practices, including misconfigurations, were identified as primary causes of these leaks. The incidents serve as a stark reminder of the importance of robust cybersecurity practices, particularly in times of urgent operational needs.

- Vulnerabilities in Healthcare Systems. Attacks on healthcare supply chains and service providers resulted in disruptions or losses to health organisations (7%). Such types of attacks are expected to remain significant in the future, given the risks posed by vulnerabilities in healthcare systems and medical devices. A recent study by ENISA revealed that healthcare organisations reported the highest number of security incidents related to vulnerabilities in software or hardware, with 80% of respondents citing vulnerabilities as the cause of more than 61% of their security incidents.

- Geopolitical Developments and DDoS Attacks. Geopolitical developments and hacktivist activity led to a surge in Distributed Denial of Service (DDoS) attacks by pro-Russian hacktivist groups against hospitals and health authorities in early 2023, accounting for 9% of total incidents. While this trend is expected to continue, the actual impact of these attacks remains relatively low.

- The incidents examined in the report had significant consequences for health organisations, primarily resulting in breaches or theft of data (43%) disrupted healthcare services (22%) and disrupted services not related to healthcare (26%). The report also highlights the financial losses incurred, with the median cost of a major security incident in the health sector estimated at €300,000 according to the ENISA NIS Investment 2022 study.

- Patient safety emerges as a paramount concern for the health community, given potential delays in triage and treatment caused by cyber incidents.

Take the First Steps Towards Better Cybersecurity

Every day, organizations across our country are impacted by cyber intrusions, many of which affect the delivery of essential services. Security professionals and business leaders alike recognize the need to protect their customers, employees, and enterprises against this threat, which raises a simple but challenging question: where to start?

We know that no organization can adopt every possible cybersecurity measure or solution, but every organization can do something. We also know that some cybersecurity measures are more effective than others in addressing the types of attacks that occur with the greatest frequency and impact. There's no shortage of guidance, best practices, and standards, but we've heard from countless partners about a challenge in prioritization.

To address this gap, President Biden's National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems required Cybersecurity and Infrastructure Security Agency (CISA) to work with industry and interagency partners to develop a set of voluntary Cross-Sector Cybersecurity Performance Goals (CPGs). We first introduced the CPGs in December 2022 and updated them this March based on initial stakeholder feedback. The CPGs were developed for entities of all sizes and across all sectors and meant to enable rigorous prioritization because being secure shouldn't mean breaking the budget. In addition, the CPGs can help organizations evaluate their current cyber posture while guiding them on how to achieve a strong cybersecurity foundation for their organization.

We believe that if every organization incorporates fundamental cybersecurity practices that they can materially reduce the risk of intrusions, no matter what sector or what size. As the nation's Cyber Defense Agency, our goal at CISA is to make it easier for every organization to prioritize the most important cybersecurity practices. We also want to be sure they are clear, easy-to-understand, and when—implemented—lay out tangible steps organizations can take to reduce the risk of cyberattacks and the damage they can wreak.

Organized according to the Cybersecurity Framework, the CPGs reflect some of the best thinking gleaned from across the cybersecurity community and draw from extensive input from experts across sectors, public and private, domestic and international.

Evolving CDM to Transform Government Cybersecurity Operations and Enable CISA's Approach to Interactive Cyber Defense

In recent weeks, a federal agency identified an active exploit targeting their network. The agency quickly shared cyber threat intelligence with our team at the Cybersecurity and Infrastructure Security Agency (CISA). Though the agency quickly mitigated the threat, CISA used our Continuous Diagnostics and Mitigation (CDM) Federal Dashboard and quickly detected several other vulnerable systems in the federal government related to this exploit. Within minutes, we leveraged this host-level visibility into federal agency infrastructure to confirm potential risks, alert affected agencies, and actively track mitigation – preventing an active exploit from causing widespread harm across agency systems and impacting essential services upon which Americans depend.

A New Era for CDM

The capabilities of CDM today are in stark contrast to those of just a few years ago. Previously, Federal Civilian Executive Branch (FCEB) operators and CISA counterparts lacked sufficient operational visibility – insight into what devices, software, and users were operating within the environment – to effectively mitigate risks prior to a breach. Operators had no automated way to share valuable intelligence with other federal agencies; it was all manual data calls. Now, because of the CDM program, agencies and CISA can respond to cyber threats in a coordinated and expedited fashion by sharing data between dedicated CDM Agency Dashboards and CISA's CDM Federal Dashboard.

CDM Agency Dashboards visualize cyber risk information collected from sensors and tools deployed within agencies' environments. Each Agency Dashboard shares data with our Federal Dashboard, giving CISA an integrated view of the dynamic state of the federal enterprise's unclassified domain, positioning cyber operators across the federal government to more effectively collaborate when responding to a cyber threat.

Genetec and Axis Communications transform physical access control with introduction of Axis Powered by Genetec

Genetec Inc. has announced a new collaboration with Axis Communications that delivered Axis Powered by Genetec, the industry's first enterprise-level access control offering combining Genetec access control software with Axis network door controllers in a single easy-to-deploy, all-in-one offering.

With inventory available globally and offered exclusively through the Genetec™ Certified network of channel partners, Axis Powered by Genetec combines the Genetec Synergis™ access control software with the AXIS A1210 and AXIS A1610 network door controllers.

Axis Powered by Genetec combines hardware and software in one unit, which simplifies the installation process, reduces maintenance, and brings built-in cybersecurity features at both the hardware and software levels. The open platform solution expands the Genetec ecosystem of non-proprietary systems while providing customers with more flexibility to scale as their physical security needs evolve.

Integrators will benefit from easy-to-deploy hardware pre-loaded with the industry's most innovative access control software, removing friction associated with traditional software/hardware integrations. Devices in the Axis Powered by Genetec program benefit from continuous delivery of product and firmware improvements, new features, and important cybersecurity updates – all from two of the industry's leading innovators.

XProtect 2023 R2 release further boosts operational efficiencies

Milestone Systems announces its latest product update, XProtect 2023 R2, a software upgrade designed to meet the evolving demands of Video Management Software (VMS) users.

Following the successful 2023 R1 update earlier this year, the R2 release brings significant advancements, featuring Adaptive Playback, Video Restrictions, the introduction of Adaptive View for Exports, a new Rapid REVIEW enhanced installer, and improvements in XProtect Management Server Failover capabilities.

In the new R2 update, Adaptive Playback enables the Smart Client to switch seamlessly between high and low-resolution streams. This adaptive streaming capacity helps reduce the system load, lessens the load on viewing clients, thereby offering a smoother viewing experience. The reduced system load further allows for additional cameras to be connected.

The R2 release also introduces the Sharing a Camera Link feature, allowing to share links to live video streams between users of the Mobile Client. This can greatly improve the efficiency of field security personnel by allowing them to share a specific live stream with a colleague, particularly useful in high-stress scenarios.

Building on the focus to improve the user experience, the R2 update offers an Adaptive View for exported video projects. This new viewing mode in the Smart Client Player adjusts the camera layout based on the number of cameras playing simultaneously to maximize view size. This feature aids users in better managing their video exports.

With this R2 update, XProtect now offers Video Restrictions, a functionality designed to provide additional security provisions. It allows operators to limit access to certain video sequences, including video, audio, and device metadata, to authorized personnel only.

LenelS2 Releases Updates to Flagship OnGuard Platform

LenelS2, the global leader in advanced security systems and services, has released the latest version of its flagship access control and alarm monitoring system, OnGuard ® Version 8.2

This new version empowers users to take advantage of a range of new value-added features and enhancements, prioritizing the optimization of their security profiles, boosting operational efficiency, and delivering a more customizable and intuitive user experience. LenelS2 is a part of Carrier Global Corporation (NYSE: CARR), global leader in intelligent climate and energy solutions.

OnGuard v8.2 offers new override functionality to access doors in "locked" mode. This feature enables first-responders to navigate through locked doors when necessary. By simply setting a badge attribute, this override feature can help facilitate a timely response, supporting the safety and well-being of those in need during critical situations. This feature is designed to support first responders during site-wide lockdowns, such as those at schools and campuses or at manufacturing and chemical facilities.

As part of LenelS2's digital transformation, OnGuard v8.2 has increased its capability with Amazon Web Services (AWS) and Microsoft Azure to include Amazon RDS cloud database support, additional Azure SQL support, and the addition of cloud platforms to its compatibility charts. Customers now have more resources to leverage the OnGuard platform's Infrastructure-as-a-Service capabilities through self-managed hosting as an alternative to LenelS2's upcoming OnGuard Cloud service.

"These new OnGuard Version 8.2 features not only boost our customers' security profiles and improve operational efficiency - they'll also enable emergency management personnel to respond to critical situations without delay due to not having access" said Stephen Russo, VP of Product Management at LenelS2. "These and upcoming OnGuard releases deliver on our customers' needs today and into the future."

Identiv's Access Control Solutions Granted FedRAMP Marketplace Authorization

Identiv, global digital security and identification leader in the Internet of Things (IoT), announced that its cloud-based Hirsch Velocity security management software, Velocity Vision video management system (VMS), and Hirsch Mx Controller products have been granted Federal Risk and Authorization Management Program (FedRAMP) Marketplace Authorization following a rigorous, multi-year assessment process.

FedRAMP is a U.S. government-wide program that promotes the adoption of secure cloud services across the U.S. federal government by providing a standardized approach to security and risk assessment for cloud technologies and federal agencies. The FedRAMP Program Management Office (PMO) maintains the FedRAMP Marketplace, a searchable and sortable database of Authorized Cloud Service Offerings (CSOs), federal agencies using FedRAMP Authorized CSOs, and FedRAMP recognized auditors (3PAOs). By deploying FedRAMP Authorized CSOs, federal agencies can leverage standardized security authorizations on a government-wide scale, thereby accelerating the adoption of cloud computing services.

Identiv's Hirsch Velocity, Velocity Vision VMS, and Hirsch Mx Controller products are industry-leading physical access control solutions, trusted and used by government agencies and commercial organizations worldwide. FedRAMP Authorization indicates that Identiv's cloud-based access control products have met the strict FedRAMP security requirements to provide secure, reliable access control in U.S. federal government environments.

"We are proud that our end-to-end Velocity, Velocity Vision, and Mx Controller solution has secured FedRAMP Marketplace Authorization," said Steve Humphreys, Identiv CEO. "This designation validates the strength of our physical security platforms and our commitment to provide the highest level of security to our customers."

In addition to the FedRAMP Authorized designation, Identiv's end-to-end Velocity, Velocity Vision, and Mx Controller access control solution has been certified as Federal Identity, Credential, and Access Management (FICAM)-compliant, ensuring that it meets the highest standards of identity and access management for federal agencies.

Final Report on 24th Annual MEMS Industry Commrcialization Report Published

Roger Grace, President of Roger Grace Associates, the world's leading marketing consultancy specializing in sensors and MEMS has announced the publishing of its complimentary and extensive Final Report for its popular 24th. annual MEMS Industry Commercialization Report Card Study.

The 2022 MEMS Industry Commercialization Report Card Study showed the unprecedented increase in virtually of all of 14 subject (a.k.a. critical success factor) grades. The aggregated grade increased from C+ to B- from the previous year and thus demonstrated the resilience of MEMS Industry participants to significantly mitigate the negative effects of Covid which continued to exist into the current Report Card Study year of 2022. The Final Report of this unique, highly regarded and one-of-a-kind Study provides over 75 extensive and actionable verbatims that were received from the 43 highly experienced MEMS industry respondents. The initial and ongoing intent and objective in the creation of the Report Card has been to share with the international MEMS community the barriers a.k.a. critical success factors in the creation of a successful MEMS industry and to help guide participants with valuable inputs as to how to better succeed based on past performance.

A sample of some of the subjects' more significant results showed:

Infrastructure… supply chain problems which have been severe in the previous Report Card, appear to have been mitigated to a great degree and organizations are adopting novel approaches including attempting to develop local suppliers for critical parts. Grade improved one level from B- to B.

Venture Capital Attraction… the increase in grade level by three was the most significant change of an individual grade in the history of the report card. Several organizations continue to receive major infusions in series funding. Grade improved three levels from C- to B-.

Industry Association … MEMS and Sensors Industry Group (MSIG) has come up to speed and is providing the industry with valuable informational programs. Grade improved two levels from C+ to B.

Spanish EU Council Presidency: CoESS and APROSER make proposals for a future-oriented, more resilient, European Union

On 01 July 2023, Spain took over the rotating Presidency of the Council of the EU. It will thereby be responsible to lead the work in Brussels on important matters such as negotiations on the EU Artificial Intelligence (AI) Act and initiatives in the context of the EU Year on Skills.

In a Joint Statement, CoESS and APROSER declare the commitment of the European security industry to support the efforts of the Spanish Presidency on a large range of matters impacting not only the security services, but public security overall.

The timing of the Spanish Presidency comes at a particularly decisive stage. First, EU lawmakers will have to find agreement on a large range of open dossiers before the European elections in 2024, notably the EU AI Act. At the same time, European businesses and societies are confronted with a range of challenges, such as labour shortages and increasing threats to the protection of Critical Infrastructure and supply chains – to name only a few.

In their Joint Statement, the representatives of the European and Spanish private security industry, CoESS and APROSER, confirm their commitment to support the Spanish Presidency in its efforts to build a more future-oriented and resilient EU and make respective proposals for the way forward. These are grouped along four key messages:

- Recognising the value of private security services to European citizens and economy

- Adapt legislation to realities in a changing security landscape

- Public security empowered through qualified workers

- Enforce the provision of high-quality security services to European citizens

Important recommendations include the hosting of a private security roundtable in Brussels, principles of human-centred AI and legal certainty in the context of the future EU AI Act, and a call for a revision of the EU Public Procurement Directives.

ADVERTISING SALES

Jina Lawrencec
UK & ROW
E: jinal@torchmarketing.co.uk
T: +44 (0) 7958 234750

Sam Most
Mainland Europe & Turkey
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

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

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

SAVE THE DATES

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

for the international border management and security industry

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

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

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

Supported by:

European Association of Airport and Seaport Police
AFRICAN UNION
ISIO
NSCRC

Media Partners:

World Border Security Network
BORDER SECURITY REPORT
World Security-index.com