critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

SUMMER 2022
www.cip-association.org

FEATURE:
Redefining Critical Infrastructure

FEATURE:
Quo Vadis Homine? TOC structure in a Continue Digital evolution

FEATURE:
Introducing the first CIP standard for private security

THE IMPORTANCE OF EMBEDDING SECURITY INTO THE DESIGN OF CNI

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event

Collaborating and Cooperating for Greater Security

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

Invitation to Exhibit

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

The 4th 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 in Baton Rouge, Louisiana 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 exhibiting and sponsorship opportunities contact:

Ray Beauchamp
(Americas)
E: rayb@torchmarketing.co.uk
T: +1 559-310-0330

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

Supporting Organisations:

Media Partners:

WELCOME TO CRITICAL INFRASTRUCTURE PROTECTION AND RESILIENCE

Honoured Guests –Ladies and Gentlemen - Good Afternoon – Bună ziua and welcome to the lovely city of Bucharest and this our 7th Infrastructure Protection and Resilience conference here in Europe and our first live event since we were in Milan in 2019.

What a strange time it has been since then, an unbelievable couple of years for everyone both Personally and Professionally, struggling with the enormous impact of Coronavirus and now we find ourselves waking up to the sights of a most regrettable and dreadful war between Russia and Ukraine and the knock-on effect that will have on the rest of the world and the impact on Global Peace and Security.

This is a critical time for all within the CNI sectors, both Natural and Man-Made Disasters are here to stay.

The range of Attack Vectors that we face are vast and vulnerabilities will continue to grow, as those who wish to cause us harm advance their methods and discover ever more exploitable weaknesses.

The current Geopolitical situation, the Threats and Risks, whether Malicious or Natural are obviously matters that will be subject of much debate over the next few days.

We are delighted that for this event we are partnered together with our good friends from:

The National Institute for Research & Development in Informatics – (ICI Bucharest) under the coordination of – The General Secretariat of the Government - and we are extremely grateful for the support they have provided to us.

critical infrastructure PROTECTION AND RESILIENCE EUROPE

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.

I am John Donlon and it is my privilege to be your Conference Chair for the next few days.

My background is in Policing in the UK. I was a Police Officer for 34 years the last 10 years of which was within the world of National Security and Counter Terrorism.

Within this I had the National Police Lead for a wide range of security issues which included, the Protection and Resilience of our National Infrastructure and I am currently the Chairman of IACIPP, The International Association of Critical Infrastructure Protection Professionals

We have an exciting line up of topics and speakers over the next few days where we will seek to explore the:

• Continuing Complexities -

• The current and future threats and hazards -and the

• Innovations in place - around the protection and resilience of our Critical National Infrastructure and Information

The conference aims to deliver, discussion, debate and a wide range of presentations on the variety of challenges that we all face in seeking to ensure we deliver the essential services so vital to the well-being of our nations.

The risk environment affecting our Infrastructure continues to be complex, challenging and uncertain.

Threats, vulnerabilities and consequences have all evolved at a pace and as mentioned the current conflict in Ukraine and the increased posturing of Russian State Actors around Cyber-Attacks is central to all of our considerations.

As technology makes the world smaller, we all become increasingly impacted by world events.

As urbanization increases, we march towards a more interconnected and networked society, globally.

Infrastructure that has long been subject to the dangers associated with physical threats and natural disasters are now facing a significant level of exposure to cyber risks.

Cyber space has become central to our economies and societies.

Science and Technology continues to transform the way we live our lives and to a great extent shape some of the threats we face, as we see:

• An ever-accelerating pace of innovation

• An exponential growth in data leading to information challenges

• More complexity as differing technologies converge or enable each other and

• More automation of processes ultimately including Artificial Intelligence.

So, whilst Cyber space fosters open markets and brings amazing new opportunities this very openness can make us more vulnerable to those who want to cause us harm.

Our endeavours to deal with the range of challenges across both the Physical and Cyber spectrums must continue to develop. This has to be considered alongside the devastating impact that adverse weather conditions can cause to our society. As we all know, the number of natural events and disasters are increasing all over the world, as are their effects and impact on people, the environment and lifestyle.

Our world is unpredictable and is changing at an incredible pace. So, our efforts to deal with the range of challenges we face must continually evolve.

There is, therefore, a constant need to review-develop and update

Policies, practices, procedures and technologies to meet these growing and changing demands.

The community involved in managing those challenges, both here in Europe and Internationally is wide-ranging and is comprised of partnerships among:

• Owners and Operators

• National, Regional and Local Government Entities

• Academia and other Key Stakeholders.

Managing those challenges needs an integrated approach, across this extensive community to:

• Identify – Deter – Detect – Disrupt - Plan and Prepare for the current and future - threats and hazards……

• To Reduce vulnerabilities of Critical Assets - Systems - and Networks – and to –

• Mitigate the potential consequences of incidents or adverse events that do occur.

The success of any integrated approach depends on leveraging the full range of capabilities, expertise and experience across the Infrastructure community and its associated stakeholders.

This in turn requires the:

• Efficient and effective sharing of relevant information among partners - to build - Situational Awareness and to enable effective risk-informed decision making – And -

• Integration within National System - Across –

Prevention,

Protection,

Mitigation,

Response - and

Recovery.

Tackling these issues - becomes much simpler - when we approach them together, collectively.

And the fact that we are all here, tends to suggest that we understand the power of cooperation, connectivity, collaboration and communication across the Infrastructure Community.

We all have more to learn and we all have something we can pass onto others and a forum like this is the ideal place for:

• New learning

• Making New Professional Friendships

• Developing New Ideas – and –

• Understanding exactly what is being done at an International level.

In conclusion I do hope that you find the conference to be a great event, to be of real value to you, both personally and professionally and that you all have a great time here in Bucharest.

John Donlon QPM FSyI
CIPRE Conference Chair

ADVERTISING SALES

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

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: +1-559-310-0330

The Importance of Embedding Security into the Design of CNI

From Critical Infrastructure Protection & Resilience Europe, Bucharest, June 2022, Sarah-Jane Prew, Senior Security Consultant, Arup

Embedding security early into any capital infrastructure project is essential to achieve a good security outcome, and security managers need to have an awareness of the design process. Sarah-Jane Prew, Senior Security Consultant at Arup offers such an insight, explains the benefits of including security early and discusses some of the challenges.

Early engagement

One of the biggest challenges facing any security manager when it comes to design projects is the engagement of the security department into a project at an early enough phase to influence the design. It is not uncommon for the security manager to be made

aware of the existence of projects only when external consultants engage with them to seek their input, or a member of the project steam asks their advice on some technical issue, usually at a very late stage of the design.

The reasons for this are many but usually stem from lack of awareness; lack of awareness on the part of those planning and implementing the project that security needs to be considered; lack of awareness by the security manager that the project is even happening; lack of awareness of what security is and understanding it only as the addition of CCTV cameras and access control once the design is complete, and lack of awareness of how security by design can assist in providing the most robust security in the most cost-effective way.

People are often unaware at how early a stage the security team should be engaged and that is, right at the beginning. Whether a new build project or a development of an existing site, the changes will influence the risk picture and result in new vulnerabilities that will need to be understood and mitigated against.

Bringing it right back to basics

Making the very first decision about what a development should be or where it should be located, without security input to assess the risks of such a decision, will leave the project facing the consequences of that choice for ever more. At best, costly and often unaesthetic measures will need to be employed which will usually only achieve part of what could have been accomplished in the design at no extra cost or time to the project, and at worst, major security vulnerabilities will be 'baked in' to the design with catastrophic implications for the project.

It is critical that any decisions about the project are risk-based and that this understanding and assessment of risk is ongoing throughout every stage of the design and build. This must take into account the current threat and risk picture and any changes to the project scope. All too frequently the project proceeds in tandem with the threat and risk piece being carried out, rather than waiting for the report and basing developments on the results and a proper understanding of risk tolerance, without which security will be playing catch up and will never be fully embedded to best effect.

The positive impacts of embedding security at the outset

Examples of where understanding risk and embedding security into the design can really impact include the ability to:

- use road layout and landscaping to keep traffic from an asset to prevent the need for additional Hostile Vehicle Mitigation (HVM) measures and blast hardening of the asset;

- understand the strengths required by a structure to resist blast or to hold heavier laminated glass windows and their retention systems before these structures are designed and in some cases even built;

- understand the secondary fragmentation properties of fixtures and fittings so the appropriate products can be procured the first time round;

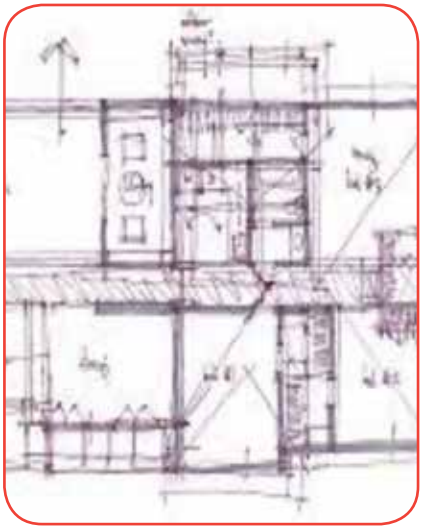
- future-proof – if there is a future requirement, for example, to install counter UAV systems on the roof of the building, the necessary roof strengths, access and connectivity need to be designed in at the build stage.

When security is designed into the project at the outset, it provides the opportunity for risk-based, proportionate and cost-effective security measures to be unobtrusively embedded into the design, achieving security outcomes in line with the client's risk tolerance, and enhancing passenger or user experience.

Influencing Security Culture.

Without the right corporate security culture security managers should never assume that they will be informed of projects that design teams consider require no security input and therefore have a responsibility to keep abreast with all capital projects taking place at their site. Engaging with capital infrastructure projects and design teams should be a critical part of every security manager's role. This will also enhance an awareness of security which can only contribute to a positive security culture.

This is the only way they can start to influence the culture of security by design and maintain control of what is being developed and its security implications.



Redefining Critical Infrastructure

Lina Kolesnikova, security expert, looks at what the impact of the Covid-19 pandemic has done on infrastructure and how we may need to review what is considered critical infrastructure.

The Next Normal

What is our "next"?

In January 2021 consulting company McKinsey introduced a term "The Next Normal", which had to replace the old-fashioned "New Normality".

"Next" is a good turn in this definition. On the one side, it is based on the assumption that there was "before" and there will be "after. On the other side, 'next' does not mean it is the end, it highlights the fact that the "next new normal" will exist until the next 'something' which will come and will create a basis for the "next after next normal".

What will be part of this next normality? Of course, some decisions which have been taken during the pandemic, will be, in full or partly the part of this.

We may constate that we have seen the responses to the Covid-19 pandemic are simply the amplification of the dynamic that drives other social and ecological crises: the prioritization of one type of value over others ("the doctrine of the more pressing question") and more presence of state, state institutions.

Modern crises are often: creeping, slow-moving and hard to detect (demographic, climate change), transboundary, high-scale, have twilight zone between crisis and risks (deep

uncertainty that threat can be transferred into the crisis, no urgency) and have significant geopolitical implications.

While there are multiple directions and facets of the next new normality, we suggest considering the Critical Infrastructure, what this might become in the post-covid era or other trigger events (flooding in Western Europe, Ukraine,) and what are the impacts and changes would be.

Critical Infrastructure AS IS

The primary function of critical infrastructure is to provide essential services to society

The current scope of the Critical Infrastructure usually includes the following sectors:

- Energy supply
- Transportation
- Water control (dams, etc.)
- Water supply and water waste management
- Food and agriculture
- Commercial facilities
- Critical manufacturing
- Government facilities
- Defence
- Chemical
- Nuclear industry
- Financial services
- Healthcare
- Emergency services
- Communications
- Information technologies

Different countries have different definitions of their Critical Infrastructures (e.g.tourism, historical buildings and monuments etc).

Covid pandemic clearly has shown that the Critical Infrastructure might need re-definition to cope with new experienced type and magnitude of threats realising.

Impacts

The virus and lockdown crisis forced people to do things differently. Among main impacts are those related to work and education organisation, governmental services, one's life and socialisation, travel, supply, and health services.

Work:

- Remote work, flexible hours, video conferencing and remote meetings have become normal with organisations and companies having expanded the work-at-home opportunities. Supporting infrastructure have grown and matured dramatically. Businesses and organisations are widely using online meeting and video conferencing technologies which came out of the pandemic time as one of big winners. Expansion of online meetings will inevitably lead to a cut back on travel.

- Re-purposing of the offices. In place of being a space with equipped workplaces, many offices will be changing its "reason to be".

- More automation. Many organizations have started their digital transformation journeys prior to the pandemic. The pandemic turned journeys to a goal to become a reality, mightily accelerating changes and getting organisations digitally maturing so that digitalisation is no longer a process and a future goal, but the reality.

Government services:

- Role of government. Governments have arisen public debt to smoothen the impacts of the crisis. Such raise of the debt will have lasting impact on the recovery and further economic growth on one side, while current extended expenditure will unlikely decrease to meet where they were before the crisis, as governments have shown that they can spend, and current or future recipients will demand assistance again and again.

- E-government. It was impossible, for health safety reasons, to deliver common face-to-face services. Making governmental services available remotely has pushed itself high on the agenda and it seems there is no intent to introduce much of the face-to-face services back. Digital service provision is now here.

- Government regulations will be reassessed. If regulatory reforms facilitating telemedicine and provision of healthcare and other services across state boundaries and increasing the speed of developing life-saving drugs made sense during the COVID-19 crisis, why not make the reforms permanent?

Communication:

- Reduced capability of governments to maintain credibility

- Impact of social network and big IT policies/filtering or denying posts. Fake news and other/alternative views

- Communication channels have to stand much higher loads

Trade and supply services:

- International trade and travel will be increasingly restricted

- Supply chains shortening and localising/regionalising

- Stock management; in particular, in what concerns the minimum emergency supplies (food, healthcare materials)

- Further raise of electronic payments and e-commerce and remote commerce

- ATM machines decline raising concerns of the cash availability in remote locations

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

- Raise of gas/electricity prices

- Fertilisers prices increase. Food security concerns

Health services:

- The next pandemic won't be nearly as bad, as states and societies get better informed and prepared

- More telemedicine. Some doctors and patients have discovered that online doctor visits work well compared to face-to-face visits

Covid pandemic (and other events) have shown several main tendencies:

- Shortage of workforce (ageing, educational gap, outsourcing, generations "Z etc", offices fear)

- Growing reliance on specialised information systems, their compatibility and reliability (health information systems, covidsafe/ greenpass etc).

- Cyber security

- More and more services and situations shall be handled in a contactless or remote way, avoiding close face-to-face interactions at all or nearly all cost. Digital service delivery is now a norm wherever is feasible. Single-use equipment.

- Some industries and individual suppliers had to adapt and to adopt to a "mobilisation-style" definition of their produces, re-purposing their production lines. Banks who continued providing financial services while also playing a role of main agents channelling governmental assistance to those in the need. Beverage factories who, in place of producing alcohol or parfum, got themselves organised or contracted by authorities to produce sanitisers. Same comes for the clothes industry, where many players start producing masks at

the time of the harsh deficit. Re-purposing might open new business lines for the companies now and in the future, and, might become somehow mandated for some industries which shown up as critical.

- Ability to scale certain capabilities (research, test labs, delivery services, social assistance), while re-using existing channels as support

- New comers to the Critical Infrastructures Club, without being prepared for associated way of thinking and operating; states often don't know how to deal with such new comers, usually, in the non-regulated markets

- Wide use of direct and indirect supra-national decisions directly impacting Critical Infrastructures (sanctions)

Critical Infrastructure TO BE

The experience of the Covid pandemic brings us to increasing the scope of the Critical Infrastructure, notably, with the following sectors:

- Education. Apart of developing and making accessible more diverse and developed remote education, this sector should be considered from the point of view of developing qualified human capital which can be reachable in case of a need. Shortage in medical and other personnel were manifesting at multiple countries during the Covid crisis

- Science, research and test labs. This sector was at the front line meeting the need to find proper actions, methods, recommendations and materials to confront the crisis. Together with Education, this sector should also be considered from the point of view of developing reachable human capital, when in need

- Waste management. Some countries did better than others, but experience has shown that this sector is critical, especially, in case of a sanitary crisis

- Last-mile delivery services. Given lockdown is one of the most effective methods in controlling sanitary crises, food and medicine distribution and, especially, its last-mile sector, is critical to feasibility of maximising the effect of such methods

- Information channels reaching wide population. With the raise of digital media and social networks, the traditional channels such as TV or radio, went dramatically down in their ability to reach wide population. This is especially a case for younger generations which are often the most difficult to manage during the prolonged or continuous crisis. The information channels do not need to be all state

owned or localised, but rather they should be cooperative and operating in the state-defined framework of rules and policies. Notable experiences during the time of Covid crisis provided evidence that big private IT companies apply their own rules and policies, which can lead to the state actor information being restricted or even outright banned based on their (private IT companies') ethical or political views. Such compartmentalisation of policies and rules applied to the critical sector, coupled with commercially driven AI algorithms, can lead to barbarisation by promoting fake news and segmentation of societies during the time when prompt communication and cooperative unity are critical.

- Individual protection and new protocols shall be developed and adopted which could stand the raised sanitary requirements with no disruption to the supply chains and several critical sectors as whole (e.g., food, transportation, last-mile delivery, water supply and waste management, emergency services, …). For example, for all various reasons, there were cases during the pandemic crisis when emergency services simply did not arrive when called upon. While lack of capacity is often the "excusable" reason, the event of non-arriving when the responders have no protection and do not have proper protocols in place, is a risk which can and shall be remediated

- Transportation and food sectors shall integrate with the last-mile delivery services

- Remote work and lockdowns are used widely during sanitary crises. This leads to a need of developing burn-out management methods and practices going beyond regular primary and secondary victims (e.g. emergency responders). This naturally applies to multiple sectors – traditional ones like law enforcement, healthcare and emergency services, but also critical manufacturing, food and public services, students and the mass of remote workers, last-mile delivery agents and, in general, all those who are on the first line of confronting a crisis

- Telemedicine should be furthered and, in particular, a legal framework shall be developed allowing more remote services to be delivered, in function, of the individual and society situation

- Critical manufacturing should be able to respond to the need of producing single-use products at large scale. Given evidenced and possible border and transportation restrictions, more attention should be paid to localising, or at least, regionalising supplies. This might lead to consider lowering dependence on inter-regional and even intra-regional supplies, as pandemic clearly has shown the problem of operational span across borders and cross-border access of personnel and deliveries. There are two main methods for critical manufacturing to respond – sufficient stock management covering peak demands in critical products or localised supply chain which can feed the critical manufacturing to quickly produce necessary products. These two methods can be used independently or in combination

  o Here raises an important political problem too. Producing more of the single-use products directly contradicts the climate agenda. Therefore, the political not only economical or sanitary balance shall be found, and waste management and recycling will likely become critical in this balance

- Communication by governmental services or command centres is often a weak spot due to its complexity and the fact that command centres are often operate in the situations of uncertainty and stress. However, all efforts need to be put in place so that qualified personnel deals with analysis and communication preparation so that large impacts get effectively communicated and highlighted (e.g., that certain governmental financial assistance may impact the tax situation of benefiting individuals in the future). Letting people be uninformed, not setting or managing expectations, open the door for all negative surprises and reactions afterwards

- Massive further digitalisation and improvements so that more operations can be conducted contactless (e.g., postal or food delivery) up to fully remote when feasible

- Finally, not to be forgotten, the time of crisis makes the cyber-attacks more dangerous. Often, certain companies or organisation suddenly become critical to national welfare, and it changes the implications of cyberattacks on them. Threat actors are moving extremely fast, being motivated by monetary, political, economic or another impetus to achieve their malicious goals. When certain company or organisation becomes critical but is not properly prepared, it opens the society and the country towards potentially devastating effects. NIS/NIS2 frameworks might need to expand towards wider sectors.

Conclusion

The pandemic has re-confirmed that the physical reality is real and critical, and that globalisation while beneficial economically, is not necessarily the answer to all needs. It also stressed the fact that the digital reality is an indispensable instrument in enabling and assisting our physical reality. Therefore, digital reality in broader sense shall now become as critical consideration as any other physical reality sector could be.

World Border Security Congress

25TH-27TH APRIL 2023

SKOPJE, NORTH MACEDONIA (BALKANS)

www.world-border-congress.com

Developing Border Strategies Through Co-operation and Technology

Co-Hosted and Supported by:

SAVE THE DATES

The Republic of North Macedonia is a landlocked country in the Southeastern region of Europe known as the Balkans. It gained independence in 1991 as one of the successor states of Yugoslavia.

In March 2020, North Macedonia acceded to NATO, becoming the 30th member state and accession process to join the European Union remains ongoing.

Ranked as the fourth "best reformatory state" out of 178 countries ranked by the World Bank in 2009, North Macedonia has undergone considerable economic reform since independence. North Macedonia has witnessed steady, though slow, economic growth and has implemented policies focused on attracting foreign investment and promoting the development of small and medium-sized enterprises (SMEs).

The country has a rich and diverse history and Skopje, the capital has been inhabited since at least 4000 BC; remains of Neolithic settlements have been found within the old Kale Fortress that overlooks the vibrant modern city centre.

By virtue of its position North Macedonia sits on the Balkan route for illegal migration into the European Union and therefore faces border challenges that require a collective, collaborative, and holistic response, making it the ideal place for the next meeting of the 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 Skopje, North Macedonia on 27th-29th April 2023 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: +1 559-319-0330

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

Supported by:

Media Partners:

Quo Vadis Homine?

TOC structure in a Continue Digital evolution

From Critical Infrastructure Protection & Resilience Europe, Bucharest, June 2022, Mihail Cunescu, Operational Manager at RASIROM

A slightly twisted biblical phrase. The question posed by Saint Peter to Christ, during the flight from Nero's Rome.

This is also the question which was pestering me for a good period of time now. And under this umbrella there are a plethora of other questions. In which direction we are running, what are we doing, if what we are doing is good or not, who can tell us what are the consequences from our actions or indifference? What I can do to better myself, what should I do to help others, how I can increase the quality of life for everybody? How am I situated in relation with the technological advance?

I just hope that my life is in an equilibrium, that what I take from the society to fulfill my needs is at least smaller than what I give back. But how to measure this? Until now was not possible, today and in the near future is a certainty.

Each one of us is a simple cog in a huge planetary machine. How aware is this cog? How we can educate the cog in order to have a

performant machine, society?

This crowded human environment has nowadays a big quantity of technology integrated and the impact of technology in our life is tremendous. The speed of any process nowadays it's a few times faster than twenty years ago. Individually we know how to deal with this segment of our life, but collectively are we able to use the technology for bettering our society?

Everybody is talking about our reality, that our needs are changing due to the impact of technologies. We have terms like Augmented Reality to bring us at a glance a lot of information, IoT to integrate artificial intelligence and communication in any tool created by man, public and local Cloud to access Services and Storage Space, SaaS (software as a service) to open an entire virtual world which is superimposed on a real one. All of these creations on a very large distribution and availability it's increasing the awareness and level of education on a big part of human society.

How good are we perceiving what happens with us or around us? How good are we at understanding the Process? This is the big question, how to understand the process?

We have a lot of methods to do this, but all of them are using tools to sample or read in real time key parameters in order to compose the image of the process. If you want to recreate an analogic signal, with great accuracy, from a digital coding than you better have a great resolution in sampling. This means that you have to use the appropriate sensors, in meaningful places and read data in real time or with a frequency high enough to reach your purpose.

Then after gathering all of data from those sensors, you should interpret them in order to compose an image. How accurate is this image depends entirely on sensor quality and if you use the correct algorithms to compose it.

Now this tool should be applied in a continuous cycle, checking each time if the data from your sensors is enough, if you have to create new sensors for other sets of data or the sample places are enough or if all the dimensions were treated or not.

The problem seems to be that the process is everchanging rapidly due to the technological advance. Now there is also an issue related with the speed of process. That means the model used for the process study should be a dynamical and fast one. And for this we will look in AI direction.

I work in a company with a business core oriented toward technical security, implementing Operational Centers (Security and Network) for institutions. We create these Operational Centers in order to deal with the security and functional issues on organizational and technical level. Nowadays a physical security OC gather flows of data from sensors which are distributed al over a zone of interest, doesn't matter if are temperature, control access, video cameras, smoke detectors, data traffic or computer agent sensors. If a few years ago, we had simple Operational Centers with a few types of sensors and a significant human presence, now we have mini-Data Centers or big ones attached to any SOC, in order to deal with integrated systems and big flows of data gathered form multiple sensors platforms. Also, there are a lot of applications in an integrated environment and a lot of automatizations. The development of IoT and the possibility to transform the sensor in an intelligent one, the leap done in communications, quality and quantity of manipulated data, the possibility to create a sensing mesh in order to samples in real time any small process increased a lot the visibility over the process.

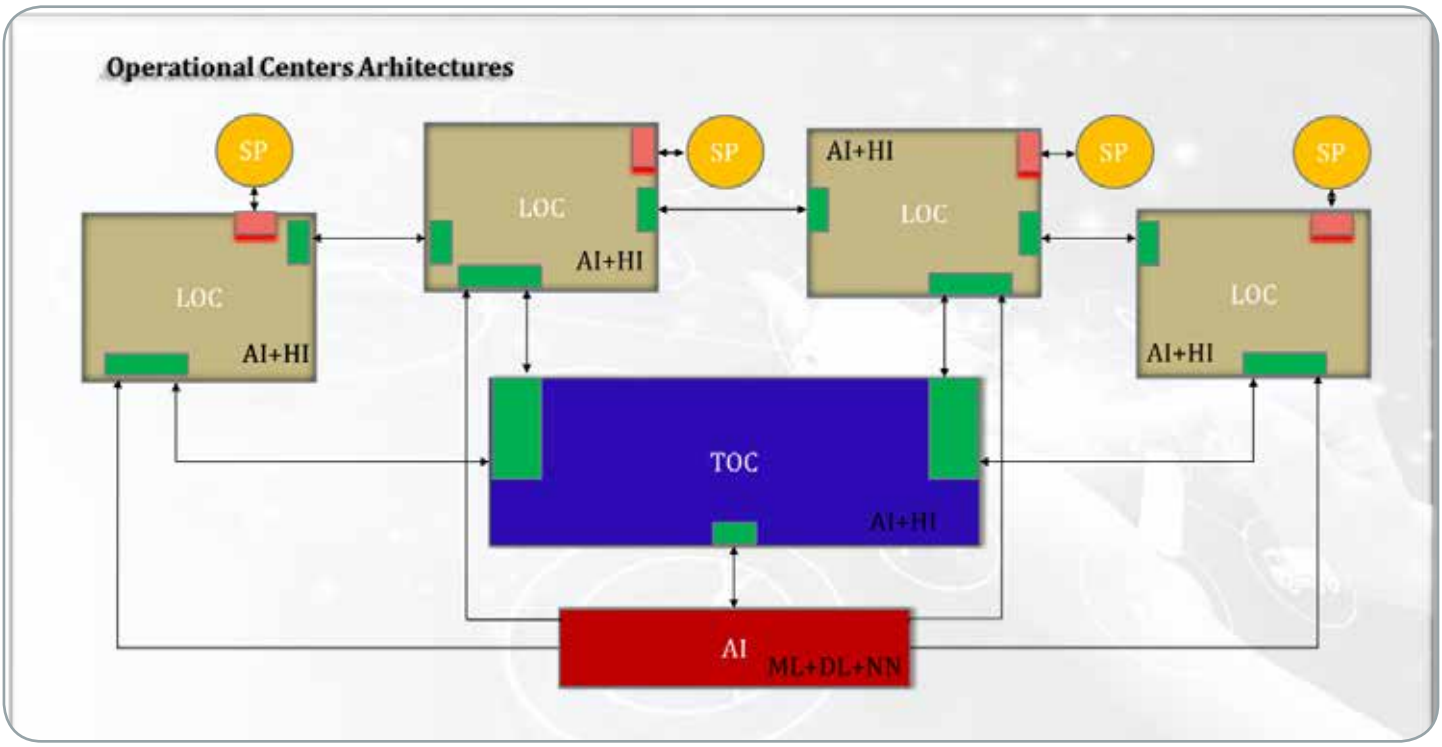
The technology is making leaps each year and we have an interesting time trying to stay in sync with all we have to implement in order to fulfil the clients and reality requirements.

We have nowadays a lot of applications and automatization at our hand to create more services to came in front of the user and give him the possibility to fulfill his needs. But what are his real needs? Who is doing the process analysis? And until you finish one with a team of specialists and implement the changes or the project it's possible to realize that is already obsolete.

The solutions seem to lean more and more on one hand on AI for speed and on the other one on increasing the efficiency of sensors platforms.

In order to be able to sample the process how oft is needed and in so many layers are visible for us, we have to create specialized sensors. The technology is all around us, we have only to grab and adapt it to serve our purpose.

Starting with Wi-Fi communications and the IoT any tool created by man can be transformed in a sensor or receive de functionality of one. More than that, the sensor from a thin client_ fat server architecture is able to transform in a fat client_ thin server one. More than this we have M2M structures which literally means 'Machine to Machine'. It based on interaction of devices and machines that are connected to the internet and to each other. These physical objects integrate computing capabilities that enable them to capture data about the world around them and share this



with other connected devices, creating an intelligent mesh of iSensors.

The machines can communicate and share information without the need for human interaction. Some processes that are time-consuming are automated.

A good example is Smart Asset Tracking application installed in my car which use any registered phone to show the GPS position, status of the car parameters, any numbers of identification data and history of driving. Or the sensors in the equipment detecting errors or issues in functionality and are able to send a warning asking for predictive or corrective maintenance.

In beta testing phase of product development and then in field, a connected equipment can send back information about its state or any numbers of parameters used to study the production environment and make correction if necessary or give advices.

The sensors used in our systems are from three types: fixed, mobile and combined.

The fixed one were until now the majority of used sensors in our projects. Wall mounted cameras, movement and fire detectors, temperature and air quality sensors, computers sensors combined with an agent software, etc.

In the last years we started to use also mobile ones. Cars and other vehicles augmented with IoTs, UGV, UAV.

And like a novelty the client requirements are bringing any number of combinations between the fix sensors and mobile one. Even "off grid" iSensors positioned in inaccessible places far away in nature, powered by solar energy, can upload the stored data on moving receivers mounted on trains, vehicles, UGVs or UAVs.

The Unmanned Aerial Vehicles are starting to play a bigger role due to the increase of autonomy, communication range and payload. The number of sensors available for these mobile platforms and applications are starting to increase fast, covering some black spots in sensing capability.

Together with the UGV, there is a bright future in activities like surveillance and SAR. A good example is the combination of UGV and UAV used in long patrol missions in case of natural calamities, earthquakes.

But the star seems to be the BYOD. On the very beginning was meaning the practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes. But nowadays the model has crossed the border of organizations, and a lot of private companies are providing services for everybody using the sensors integrated in their mobile phone in a collaborative structure. The most discussed subject regarding the integration of these terminals on a network was the security issues. But with the cybersecurity measures and policies integrated in any client software which is connected to an OC, this mobile sensor platform can be used in acquiring any type of data.

The complexity starts when an OC have to deal with multiple systems, with a spread sensors architecture, with a complex communication layer and a different behavior for each surveilled object.

The security layer and the functionality one should work flowless together in order to maintain the process alive.

We are using the AIs to discover and learn the normal behavior on any object in the process and take actions if it's showing any anomalies.

The AI should be part of any Business Analysis needed for a new process or a transforming one and after implementation should continue the work in the background, to keep the functionalities up to date and to deal swift with any issue which may appear.

A good example of Operational Center structure can be a distributed one with Local Operational centers with any numbers of sensor connected to the them.

All of them interconnected and connected in a Technical Operational Center which integrate multiple functionalities and has a supervising role. The TOC is able to substitute part of a Local OC functions or ask others LOC to do this in case of a malfunction.

The TOC will gather all the information received from LOCs and put together a big picture.

Is assisted and supported by an AI. On this layer we have all the subsets from AI, Machine Learning, Deep learning and Neural Networks.

The layer is dedicated for:

• Future predictions.

• Classifications.

• Exploring key insights in data mining.

• Helping in development of applications and use cases.

This structure has a Data Information Knowledge Wisdom model used for understanding the process. The Local Operational Center use sensor platforms to gather the data and has the Command-and-Control function. Data evolve in enhanced information. Actions are taken at this level after established policies and procedures.

The Technical Operational Center gather all information made available by LOCs, create live populated Data Base, make correlations between different sets and types of data, elaborate algorithms for virtual Proof of Concepts. Support LOCs if needed.

The AI Data Center include a Machine Learning model with its subsets Deep Learning and Neural Nets. It's using the gathered information to create virtual POCs, make tests with available entry data and predictions about the process.

The results from the AI will follow a model like Deming circle (PDSA) in order to optimize any modifications implemented at LOC and TOC level and to understand any variation in process.

The predictability offered by AI will be used to increase the speed of decisions at TOC and LOC levels. This layer can be scaled to address the customer needs, with a minimal AI or in a SaaS available service.

But the big winner of this informational flow it will be the user with the BYOD platform sensor because he will receive the enhanced information, the big picture and the best approach in order to take the best educated decision.

Working in a collaborative environment the user will be able to access a set of information, created and personalized for him. He will have access to real time data intelligence, access to maps or applications populated with real time information, will receive real time notification from both fixed and mobile sensors, will be able to follow any happening changes, will have access to historical operational data.

Our main goal is twofold. To integrate and develop the AI on a scalable structure, to increase the predictability and the reaction speed to the fast process variation or new required functionalities and to develop the sensor platform in order to bring so many sets of data are required giving back to users enhanced information in prepared and customized form.

The final results it will be an increasing level of education and awareness in population.

We will have a better understanding of the process and a tool to show our actions impact in real time.

Introducing the first CIP standard for private security

Catherine Piana, Chairperson of TC439 and Director General of CoESS

Critical Infrastructure Protection is an increasingly complex challenge, and the threats have intensified with Covid19 and the war in Ukraine, increasing both the cyber and physical threats from insiders, criminal organisations and hostile Nation States. This is all the more reason to only employ private security companies that meet the quality criteria that will reassure you that your Infrastructure is well protected.

National legislation generally covers guarding and surveillance activities but it doesn't (or insufficiently) address the quality criteria that companies should meet in order to perform services in CI. The new standard EN 17483-1:2021 seeks to close this gap. It is a certifiable standard that specifies service requirements for quality in organisation, processes, personnel and management.

It provides recommendations on all important aspects when delivering services in CI, such as:

– Criteria that the provider must meet, for example regarding management structure, HR, Health and Safety, Operational and financial capacity, corporate governance and IT security;

– Requirements regarding contracts, including liabilities, cooperation with other parties, subcontractors, and leased workers;

– Requirements for staff, for example terms and conditions of employment, security screening, recruitment and selection, training;

– Service delivery aspects, and service level agreements.

EN 17483-1 is the foundation for a complete standard system for CIP, on which several "vertical" standards will be built. At present several sector-specific standards are being prepared to build on the general requirements standard, namely for the security of airports and aviation, port and maritime, and the production and transmission of energy.

EN 17483-1 can be used for any type of CI and it guides public and private buyers through different key quality criteria to consider when selecting a quality provider of civilian private security services. It also enables contracting parties to issue clear and detailed specifications of their requirements to prospective tenderers, thus generating a higher quality response.

Organisations in charge of security within CI can benefit of the use of the standard, as follows:

— Operators of Critical Infrastructure when selecting private security services to protect their organisation: it helps them select companies that are trustworthy and professional;

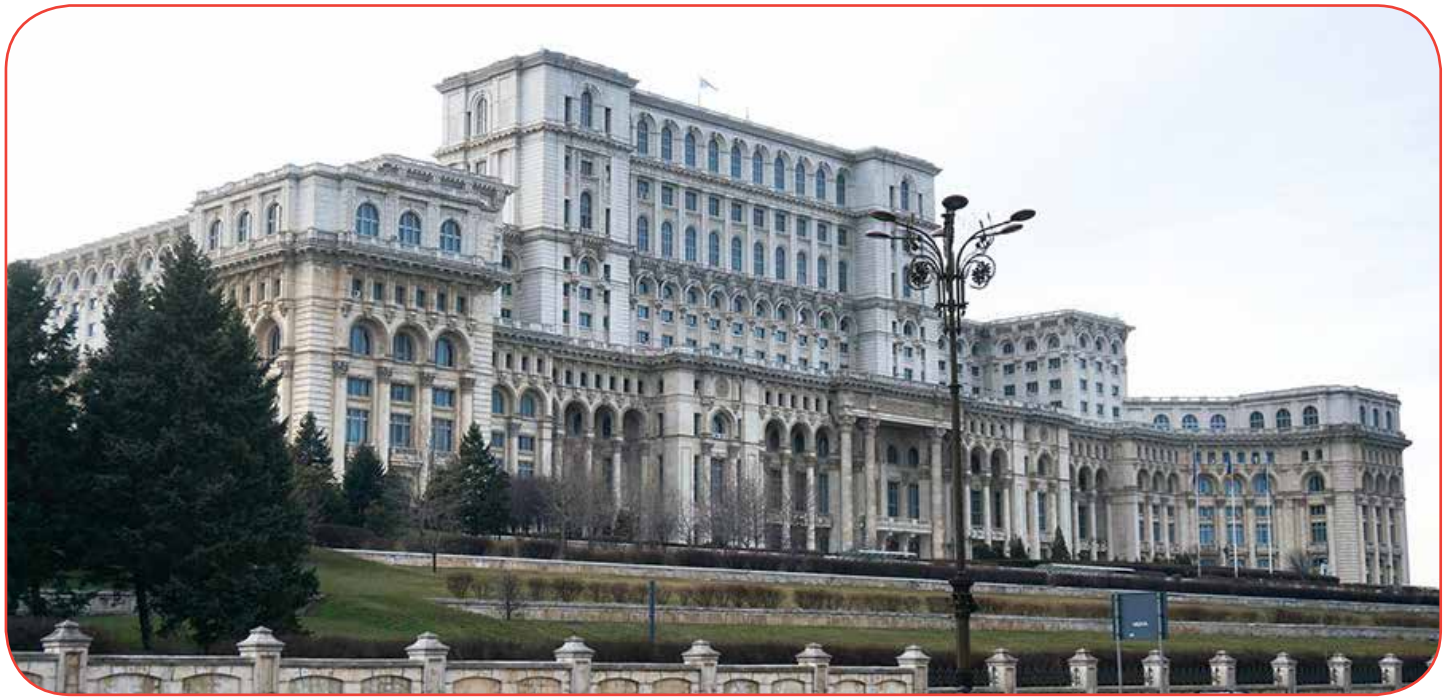
— Private Security Companies: being certified to EN 17483-1 (and in the future to the sectoral standards) is a clear demonstration that they are committed to meeting high quality criteria;

— Any interested parties who are directly or indirectly involved in or affected by a procurement process within CI.

The standard was developed by an international cross-sector expert technical committee within the official European Standards Body, CEN, including a representation of Trade Unions (ETUC). It therefore takes into consideration the Trade Union's requests for a safe, just and motivating working environment, which is key in a labour-intensive industry such as security services.

For any further information about the standard, please contact your National Standards body, where you will be able to purchase it.

Closing Comments from Critical Infrastructure Protection & Resilience Europe



Before we all head off home, or back to work for some of us, I just wanted to close the conference with a few comments.

It has been fantastic to be back at a live CIPRE event here in the beautiful city of Bucharest with so many talented, professional and charming people. The networking opportunities at events such as these are priceless and I always go away having learned something new and worthwhile. So, for example, who knew there was such a word as 'Fusionism'….I didn't and I am still not exactly sure what it means but it is the word of the week for me.

I do hope that everyone has found the last few days to have been informative, enjoyable and of real value. We have had some excellent presentations by some very distinguished and experienced professionals and some great discussions across a whole range of infrastructure and information issues.

We have been fortunate to have been able to host the event in this most magnificent building and to have had fabulous support from Victor and Carmen and the whole team here at the National Institute for Research and Development in Informatics – ICI Bucharest.

It has also been our first joint enterprise bringing together CIPRE alongside the Romanian Critical Infrastructure Forum under their banner line 'Collaboration is the key

critical infrastructure PROTECTION AND RESILIENCE EUROPE

for connecting the dots' and I am glad to say it has been an enormous success.

We had a great start on Tuesday with the keynote session comprising of a host of senior government representatives who clearly set out the infrastructure and information challenges they are dealing with. These included:

• The focus on citizens as the beneficiaries of services and how delivery can be continually improved

• The protection of data as a major government issue – and –

• The continued development of Public Private Partnerships.

And Public Private Partnerships continued as a theme across the conference. We heard from several speakers about the challenge to establish effective cooperation and coordination between the State and Private Companies, whilst maintaining a proper balance between Public and Private interests. There were then some great examples of this from the presenters on AIRPOL and RAILPOL.

The conference covered a whole range of topics:

• Exploring the evolving business and societal needs, in particular in light of the current geopolitical situation

• The significant complexity and levels of fragmentation across the infrastructure environment – and then in terms of –

• Cyber challenges, the level of complacency that still exists, in particular around financial investment, the costs versus common sense conundrum and the issue of getting organisational leadership buy in.

Cyber was as expected a constant theme throughout the event. We heard from the Director of the Romanian National Cyber Security Directorate who told us that he expected 50% of infrastructure at a national level in Romania is likely to be subject to some form of Cyber attack within the next 12 months and that 25% of those attacks will be conducted by State actors, although he didn't articulate which States they would be. However, there are no prizes for guessing who the most likely candidates would be…Russia – China – Iran and North Korea, maybe!

Cyber policies, standards and best practices also attracted significant attention with the audience extremely keen to understand the progress being made across these areas on an international level.

A number of speakers referenced the resilience gaps within international cyber systems and the need to build greater resilience through the constant – Scanning – Checking and Testing of those systems.

Resilience as a definition was also referred to in a few differing ways. I personally think a simple definition is always best, such as the following which was mentioned in a couple of presentations: 'Resilience is being prepared for uncertainty and unknown incidents, the goal being the absorption of such incidents and the ability for a fast recovery'.

The depth and breadth of resilience across our critical infrastructure during the pandemic was of great interest to all, as were the lessons learned during that difficult time. There were both presentations and discussions on how the pandemic affected the functioning of those vital services and shifted our thinking, during what was described as a 'creeping crisis' and how this led us all to start considering what the next new normality might look like.

There were many other topics covered, including:

• Mitigating Major Threats

• Emerging Threats to both Infrastructure and Information Systems

• Critical Infrastructure Interdependencies and

• Artificial Intelligence, Machine Learning, Automation and Security in the Digitalisation of Critical Infrastructure.

As with any good conference there is a great deal to be gained through the questions asked and discussions that follow and this was certainly the case here at CIPRE. The audience were both engaged and knowledgeable and didn't shy away from challenging our speakers

nor did they miss the opportunity to follow up on issues during the coffee/lunch breaks.

As I said on day one of the event, the world is an unpredictable place and is constantly changing. In that context one of the best quotes that was raised through a presentation was one from Douglas Engelbart, who was an Engineer and Inventor who stated, 'In 20 or 30 years, you'll be able to hold in your hand as much computing knowledge as exists now in the whole city, or even the whole world'. Which I think ably reflects the pace of change we are seeing across the globe.

The protection and resilience of our infrastructure and information requires us all to constantly change, adapt and innovate and one of my favourite quotes of all time, from Albert Einstein, sums that up for me, when he stated – 'We cannot solve our problems with the same thinking we used when we created them'.

We have to be aware that what was needed yesterday may not be what we need for today or for tomorrow.

So, in finishing, I do hope that you all have had a great time here and that you go away:

- Having learned something new
- Having made new professional contacts who may be able to assist you in some way in the future – and importantly –
- Having made new friends

I would like to thank ICI Bucharest for joining us in putting together this first partnership event and for hosting us here at the beautiful Palace of the Parliament.

I would also like to thank our sponsors:

- Paulo Alto Network and
- Vector Synergy

The caterers and all the staff here in the Palace.

The AV guys for keeping things running smoothly, and of course all the great speakers for giving us their time and sharing their expertise. But most of all I want to thank all of you for your attendance and your active participation which has made this conference such a worthwhile and great event.

Our next conference, Critical Infrastructure and Resilience North America will take place in Baton Rouge, Louisiana in the United States on 7th-9th March next year.

I hope to see some of you there.

John Donlon QPM FSyI
Chairman CIPRE

We wish to thank the following organisations for their support and contribution to Critical Infrastructure Protection & Resilience Europe 2022.

Co-Hosted by:

International Association of CIP Professionals

The National Institute for Research & Development in Informatics (ICI Bucharest), under the coordination of the General Secretariat of the Government.

Supporting Organisations:

Accelerating Critical Infrastructure Security in The Energy Sector

by Chuck Brooks, President, Brooks Consulting International

Critical energy infrastructure has been under siege by threat actors. The May 7, 2021, cyberattack against Colonial Pipeline is illustrative of the growing impact of cyberthreats on the energy sector and the need to prioritize cyber-defenses.

"Senators Maggie Hassan (D-N.H.) and Ben Sasse (R-Neb.) recently introduced legislation called The National Risk Management Act that is intended to protect critical infrastructure from cyber-attacks and other national security threats."

The recent announcement of The Department of Energy's (DOE) '100-day Plan to Accelerate Cybersecurity Detection, Mitigation, and Response Capabilities Across Electric Utilities' calls attention to the importance of securing the nation's power grid. DOE will be working in coordination with The Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to address "persistent and sophisticated threats" to the nation's electric grid,

including a "voluntary industry effort" to deploy technologies to secure Industrial Control Systems (ICS) and Operational Technology (OT).

"The initiative modernizes cybersecurity defenses and:

• Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities.

• Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real-time situational awareness and response capabilities in critical ICS and OT networks.

• Reinforces and enhances the cybersecurity posture of critical infrastructure Information Technology (IT) networks; and

• Includes a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems."

The initiative is one of the first cybersecurity actions from the new Administration. It is a continuing effort built on past Administration Executive Orders and activities dedicated toward bolstering critical infrastructure protection. Across other government institutions, including Congress, securing critical infrastructure has been a priority topic. Senators Maggie Hassan (D-N.H.) and Ben Sasse (R-Neb.) recently introduced legislation called The National Risk Management Act that is intended to protect critical infrastructure from cyber-attacks and other national security threats. The act would require CISA to conduct a five-year national risk management cycle, which would involve CISA identifying and compiling the major risks to critical infrastructure in a report sent to the President and Congress.

The intelligence community has also highlighted the fact that protecting critical infrastructure is a top national security imperative. The 2021 Annual Threat Assessment of the U.S. Intelligence Community assembled by the Director of National Intelligence concluded that "cyber threats from nation states and their surrogates will remain acute" as countries with nefarious aims "use cyber operations to steal information, influence populations, and damage industry, including physical and digital critical infrastructure."

"Although an increasing number of countries and non-state actors have these capabilities, we remain most concerned about Russia, China, Iran, and North Korea," the assessment said. "Many skilled foreign cybercriminals targeting the United States maintain mutually beneficial relationships with these and other countries that offer them a safe haven or benefit from their activity".

The United States is not the only target. The 2020 World Economic Forum's (WEF) Global Risks Report listed cyberattacks on global Critical Infrastructure (CI) as a top concern. WEF noted that "attacks on critical infrastructure have become the new normal across sectors such as energy, healthcare, and transportation."

The U.S. critical infrastructure is the engine of our industrial economy. The new reality is that almost all critical infrastructures operate in a digital environment, including the health care, transportation, communications, financial, and energy industries. While the information technology landscape has greatly evolved, so have the vulnerabilities. Energy assets and The Grid are especially vulnerable to attacks, both physical and cyber related.

"Because of the aging infrastructure, and combinations of meshed industrial control system networks, it is not surprising that threat actors would be engaged in mapping and targeting energy facility networks."

It is not a new phenomenon that energy assets have been continually tested by adversaries. Over the past decade, nuclear and electric grid facilities have been subjected to attacks by state threat actors, criminals, terrorists, and others. Cyber-attacks have been

the preferred modus operandi of adversaries.

The energy sector stands out as being particularly vulnerable among critical infrastructures. This energy ecosystem includes power plants, utilities, nuclear plants, and The Grid. Protecting critical Industrial Control Systems (ICS), Operational Technology (OT), and Information Technology (IT) systems from cybersecurity threats is a difficult endeavor. They all have unique operational frameworks, access points, and a variety of legacy systems and emerging technologies.

Because of the aging infrastructure, and combinations of meshed industrial control system networks, it is not surprising that threat actors would be engaged in mapping and targeting energy facility networks. Much of the equipment that comprises the electric Grid infrastructure is antiquated and needs updating. The Grid itself is critical infrastructure comprising a network of more than 7,650 power plants, which are integrated via 450,000 miles of high-voltage transmission lines. Estimates are that The Grid includes 70,000 transformer power substations and thousands of power generating units. The Grid is mostly dependent on legacy technologies: 70% of transmission lines are at least 25 years old and approaching the end of their lifecycle, and 60% of the circuit breakers are more than 30 years old, compared to useful lives of 20 years.

State threat actors do pose significant threats. Admiral Mike Rogers, former head of the National Security Agency and U.S. Cyber Command, has stated that at least two or three countries could launch a cyber-attack that could shut down the entire U.S. power grid and other critical infrastructure. Additional threats can also come from rogue extremist states such as North Korea and Iran.

There are a variety of challenges to stopping breaches, and the biggest one is the growing sophistication and resources of the attackers. We are seeing an increasing level of sophistication from our adversaries – including the use of exploiting supply chains, such as the recent Solar Winds breach. The types of tools they use include phishing scams, bots, ransomware, and taking advantage of malware and software holes that leave vulnerabilities in networks. There are also threats from physical incursions (access control), terrorism, and potential hostile insiders to contend and mitigate.

The integrated makeup of The Grid is also challenging for security. The electric utility networks are comprised of ICS (both OT and IT) that are constituted by both physical and digital connectivity. The severity of any industrial control system cyber-attack depends on whether hackers managed to breach not only its traditional OT computer systems, but also the connected IT internet-connected systems that manipulate its physical equipment. The convergence of OT and IT networks expands the attack surface and is being used by adversaries to exploit vulnerabilities from the connectivity. And what works in Cybersecurity IT may pose risk to OT Cybersecurity. For example, patching may not be an option as updates disrupt real-time system operations.

Information Technology (IT), Operational Technology (OT) and the Industrial Control Systems (ICS) supply chains in CI can be particularly vulnerable as they cross-pollinate and offer attackers many points of entry. Older Legacy OT systems were not designed to protect against cyber-attacks. There is often a visibility problem of the lack of telemetry data. Many organizations do not know if an attack has occurred, nor do they have the systems to monitor or detect breaches in control systems used in energy infrastructure.

Another factor is the growing sophistication of attackers. One of the reasons why the sector has become more vulnerable is that hackers have gained a deeper knowledge of control systems and the converged OT and IT architectures, how they can be attacked, and how they can employ weaponized malware against power stations and other energy related assets.

In July 2020, an investigation highlighted how an attacker could get into critical U.S. infrastructure via unsecured ICS. They claimed it could be done by attackers using search engines and tools dedicated to scanning all open ports and remotely taking control. Senior Researcher Edvardas Mikalauskas of CyberNews summarized: "Our research has previously highlighted that many ICS panels in the U.S. are critically unprotected and easily accessible to threat actors. The most vulnerable infrastructure appears to belong in the energy and water sector."

The National Security Agency (NSA) recently released a Cybersecurity Advisory on this exact issue of integration and connectivity of OT and IT systems. The advisory details "how to evaluate risks to systems and improve the security of connections

between OT and enterprise networks. Information Technology (IT) exploitation can serve as a pivot point for OT exploitation, so carefully evaluating the risk of connectivity between IT and OT systems is necessary to ensure unique cybersecurity requirements are met."

"In addition to ports on IT and OT networks, process sensors on energy have been one of the most preferred and easiest methods for breaches."

"Each IT-OT connection increases the potential attack surface. To prevent dangerous results from OT exploitation, OT operators and IT system administrators should ensure only the most imperative IT-OT connections are allowed, and that these are hardened to the greatest extent possible. An example of this type of threat includes recent adversarial exploitation of IT management software and its supply chain in the SolarWinds compromise with publicly documented impacts to OT, including U.S. critical infrastructure".

"NSA recommends taking steps to improve cybersecurity for OT networks when IT-OT connectivity is mission critical, as appropriate to their unique needs. For IT-OT connections deemed necessary, steps should be taken to mitigate risks of IT-OT exploitation pathways. These mitigations include fully managing all IT-OT connections, limiting access, actively monitoring and logging all access attempts, and cryptographically protecting remote access vectors."

In addition to ports on IT and OT networks, process sensors on energy have been one of the most preferred and easiest methods for breaches. "Process sensor issues have been directly involved in many of the more than 1,300 actual control system cyber incidents to date that have killed people and caused more than $80B in direct damage. Russia, China, and Iran are aware of the cybersecurity gaps in these devices and in some cases are currently exploiting the lack of sensor authentication.

Process sensors are assumed to be secure, authenticated, and correct. Those assumptions at the very least depart from the IT principle of "zero trust". Process sensor data are the input to process control, safety systems, OT networks, predictive maintenance programs, historians, etc. Compromising process sensors (or not recognizing sensor deviations) can circumvent cybersecurity mitigation as well as engineering safeguard protections. However, there is minimal cybersecurity in the process sensor ecosystem. Worse, there are built-in vulnerabilities that cannot be bypassed."

In addition to cyber-attacks, the Grid is vulnerable to other assorted malicious actions that need to be included in any threat matrix. This includes: Physical (terrorism, explosives, electro-magnetic attacks – EMP), Weather Events (lightening), Electric and Geo-magnetic super-storm (Carrington Event 1859), Solar Flares, Cascading power (over usage), and Human error blackouts. Attacks via digital means are most likely and should be prioritized; however, protecting critical infrastructure needs to be a holistic and comprehensive approach.

How can we better protect the critical infrastructure and networks? While the threats to nuclear facilities and power plants are complex, there are several themes and safeguards to adhere to mitigate risk. These include:

• Be prepared and have a framework. It is necessary to continually analyze and game the energy cyber-threat landscape, as the methods, means and malware variants are constantly morphing. Emerging technologies are changing both the defensive and offensive cyber and physical security landscapes.

• Energize Public-Private Partnerships. It is vital to share and communicate cybersecurity information between the public

and private sectors. DOE's 100-day Plan is based on the premises of collective defense in cybersecurity and a collaborative approach that recognizes the value of threat information sharing. However, there are still significant gaps in information sharing by the government with the private sector. DHS CISA has made public-private partnerships for protecting critical infrastructure a top focus. Government and industry are currently using pilot programs including the Cybersecurity Risk Information Sharing Program and the Trusted Automated Exchange of Indicator Information to facilitate rapid sharing of security information. DHS CISA has established active and successful programs in this area.

• Upgrade and follow industry protocols, especially those related to Supervisory Control and Data Acquisition (SCADA). Power companies use SCADA networks to control their industrial systems, and many of these networks need to be updated and hardened to meet growing cybersecurity threats. Standards should include NIST, IEC 62443, and ISO 27001. The energy industry also needs to know the National Institute of Standards and Technology, North American Electric Reliability Corporation, Federal Energy Regulatory Commissionand S. Nuclear Energy Regulatory Commission cybersecurity protocols.

• Access Control is Key. Who has privileged access to networks, sensors, equipment, and devices and are they monitored? It is important to maintain robust access management control and cyber incident response programs.

• Emerging Technologies are arriving. The technology landscape is evolving, and it is important to invest in next-generation security controls and cybersecurity technologies. Procurement of automation tools such as Artificial Intelligence (AI) and Machine Learning are especially needed. Also, energy providers should invest in hardening targets, both from physical and cyber-incursion.

• Risk Management. Ultimately, the most effective way to address these challenges is by utilizing a strategy of comprehensive risk management. There are a variety of risk frameworks to consider. This includes "Security by Design" – build agile systems with operational cyber-fusion to be able to monitor, recognize, and respond to emerging threats. Install Intrusion Prevention Systems (IPS) or Intrusion Detection Systems (IDS) to monitor malicious activity on your industrial network. Also, enable security settings on energy system networks. And "Defense-in –Depth" that includes layer cybersecurity technologies, processes, air-gapping, hardening, encryption of data flowing from sensors and segmentation of OT and IT. The newest framework is "Zero Trust" a term for an evolving set of cybersecurity paradigms that move defenses from static, network- based perimeters to focus on users, assets, and resources. A Zero-Trust Architecture (ZTA) uses zero trust principles to plan industrial and enterprise infrastructure and workflows. Protecting ICS used by utilities from both physical and cybersecurity threats is really a component of the dynamic threat environment using all approaches.

CONCLUSION

In July of 2020, at the G20 Summit, an international forum for economic cooperation on energy security, the importance of Security by Design was stressed. The G20 members countries were told that cyber-attacks are always evolving when it comes to capabilities and tactics and that state actors, "hacktivists" and other attackers homing in on energy critical infrastructure have become more technologically sophisticated. It was noted that the scale and frequency of attacks are alarming and that protecting critical energy infrastructure from cyber-attacks requires Security by Design. Finally, it was summarized that energy security now necessitates building agile systems with operational cyber-fusion to be able to monitor, recognize and respond to emerging threats. G20 member countries account for approximately 80 percent of the world's economic output, 75 percent of international trade and two-thirds of the world population.

Because of the modernization of critical infrastructure and replacement of legacy OT and IT systems, there may be opportunities to implement the Security by Design and Zero Trust strategies. Awareness of the threat is half the battle. The '100-day Plan to Accelerate Cybersecurity Detection, Mitigation, and Response Capabilities Across Electric Utilities' is certainly a right step in the direction for energy security.

An Interview with Weibel Doppler Radars

An Interview with Richard Engelholm, Business Development, Weibel

Explain a little about your role at Weibel Scientific.

My name is Richard Engelholm, and I work with Business Development in Weibel. Basically, I strive to identify companies, agencies and authorities that would benefit from our XENTA long-range drone surveillance radar. However, since I'm not a sales guy I don't have the obligation of insisting that our product solves all of your problems. I have the privilege and time to dive into the counter drone realm and get to know all about the challenges, friction and pitfalls, and I have the freedom to share that knowledge with stakeholders looking to engage in counter drone solutions.

Describe how different stakeholders from various parts of the critical infrastructure sector perceive the current and future threat of drones.

The future proliferated drone threat can be described in two different axis. One axis constitutes the responsible end-user, e.g. private corporations vs. governmental institutions. To the first category, the threat is first and foremost a commercial threat where drones interrupt the operational stability, where the governmental institutions will be oriented towards their responsibility to protect their citizens. Both directly by ensuring safe daily lives in and around crowded areas and events, and indirectly by protecting e.g. parliaments, heads of states and law enforcement facilities from drone attacks.

The other axis constitutes the

addressed drone threat that overall can be divided into non-hostile and hostile drones. Off course, a drone is not hostile in itself – it is merely a tool to carry out hostilities, sometimes operated by a pilot and sometimes pre-programmed for autonomous flight.

These two axis put together result in four ring corners where end-user motivation, responsibility, cost level and acceptable tolerances are variables.

Can you explain the two areas of "protecting high value assets" and "ensuring operational resilience and stability" and how best manufacturers such as Weibel should respond?

As mentioned, any state has an obligation to protect both its citizens and its governmental institutions. Especially the protection of heads of states are of the utmost importance and these institutionalized individuals are often – by an adversary – considered high value targets and so they require a high level asset protection. To put it blunt, the adversary needs to succeed only once, while we need to succeed every time. That calls for extremely low tolerance which increases the complexity and cost of the needed system (of systems).

As a contrary to this low-tolerance-high-cost demand, commercial actors like industrial ports or airports take a different approach. To them, the counter drone system is an investment in ensuring operational stability and resilience. This motivation leads to a mandatory decision on the trade-off between system costs and acceptable risks. An airport might feel forced to accept some minor risk of perimeter intrusion, as long as the air traffic safety isn't compromised.

Can you explain the long-range surveillance radar, XENTA and why / how it was developed?

For 45 years Weibel Scientific has developed and manufactured some of the world's best Doppler Radars. Where a traditional pulse radar needs (at least) two measurements in order to identify an object's movements, a Doppler Radar uses continuous wave technology thereby providing instantaneous information of an object's velocity and direction. Our portfolio of Doppler Radars are designed to detect and track all kinds of aerial objects from small projectiles via aircraft to the warheads of an intercontinental ballistic missile thousand miles away. Actually, our largest Doppler Radar is able to discriminate such a warhead from the surrounding decoys and chaffs allowing the ballistic missile defence to engage the right object in a time critical situation.

Approximately five years ago Weibel took it upon ourselves to utilize our know how in Doppler Radar technology to create a drone surveillance radar. To a radar it is a highly complex task to detect and classify a drone. How do you discriminate it from the surrounding birds? How do detect it if it hides in front of an air-condition fan or spinning car wheels? We use supervised machine learning to ensure and continuously improve XENTA's classification ability, and the radar classifies objects in six categories: Class I drones, Class II drones, missiles/artillery, helicopters, aircraft and birds/unidentified. Off course, when you want to detect very small objects, you also detect a lot more non-interesting objects like trees, cars, wind turbines and so on. To avoid too much of this so-called clutter, we've trained XENTA to discriminate between objects in four parameters; direction, elevation, range and velocity. This way, XENTA picks up even the smallest drones without cluttering the radar picture to the operator.

There are quite a lot of very capable short range drone detection radar manufacturers out there, and most of them are very good at detecting drones at 1-2 miles. However, there are only a couple of manufacturers on a global scale that are able to detect drones significantly beyond that range. In what we refer to as the long-range drone detection spectrum, we've learned that XENTA is first among equals. Besides detecting and tracking e.g. a Phantom IV sized drone at six miles and classifying it beyond four miles, the radar has extremely high performance in accuracy. Last year, XENTA participated in the Interpol counter drone exercise in Gardermoen International Airport (Oslo, Norway) as well as the NATO Technical Interchange Exercise in The Netherlands. At both events, XENTA succeeded in detecting, tracking and classifying the required aerial targets, and as the only radar it did so without any false alarms – neither false positives nor false negatives. And that is equally important to good detection range.

Can you describe how XENTA counters the growing challenges of drones on commercial safety, homeland security and military capabilities.

XENTA is a long-range drone surveillance radar that uses an open-source interface (e.g. ASTERIX protocol) to ease integration into any air traffic management system, command and control system or similar.

XENTA picks up the disturbance in the air from propellers, wings and aerial signature thereby detecting all aerial targets including hostile drones, remotely operated drones and autonomous drones.

In your presentation at CIPRNA 2022 you advocated end-users should work with technical advisers (such as Weibel Scientific) and not to jump to conclusions or make rash decisions. Can you expand on this point?

Putting together a counter drone system a highly complex task. Initially you have to carry out an analysis of the threat. Are your only concern the clumsy but compliant hobby pilots, or do you also need to be able to detect hostile and/or autonomous drones? Afterwards you should analyse the facility you have to protect. Is it a clutter rich environment? Do you have a lot of tall buildings creating masks? Are you only interested in a perimeter protection, or do you also need to be able to track objects that succeed in penetrating your perimeter protection?

After your threat analysis and analysis of your own facility and situation (including regulatory mandates and required time to respond), you can start to look for the sensors you need and the effectors, you are allowed to have. Radars are instruments of physics and so the same laws of nature apply to all radars. Weibel have chosen the X-band (8.5-10.5 GHz) because we believe these wavelengths offer the best trade-off between accuracy and resolution vs. range and weather resilience. If you instead chose the C-band (5-6 GHz), you would – generally speaking – have higher range and better weather resilience, but on the other hand lower resolution and lower "small-object-detection-capability". Likewise, if you went for a K-band radar (18-27 GHz), you would – again generally speaking – have shorter range and higher weather vulnerability but increased resolution and a better "small-object-detection-capability.

This is just one example that a radar is not just a radar, and you shouldn't demand from yourself to be able to navigate these highly complex systems. Therefore, the best advice I can give you even without knowing your situation is to ally with a technical expert that can help you translate your operational needs (and financial ability) into technical specifications. When you've identified the potential components in your system, you should insist on having them tested in the exact same conditions they will be operating in. The same harsh weather, and the worst scenarios from your threat analysis.

How will Weibel continue to lead the way in tackling drone threats in the future?

At Weibel, we are not interested in feeding you a squared solution to a problem that might be circular. Weibel are deeply concerned with the threat from drones as they are more and more integrated in our modern societies. The most innocent but clumsy behaviour can easily pose great danger to aircraft safety or supply security, and careless or criminal citizens have very easy access to inflict much greater havoc than before. Most people are very enthusiastic with the potential benefits of drones in our daily lives, but not that many have an eye out for the unintentional, negative consequences.

We are using quite a lot of our energy on bringing people together and connecting stakeholders in order to facilitate the best knowledge sharing. It's imperative that our communities do the right thing from the start. When I look at my own capital, Copenhagen, it's evident that the airport should acquire their own system, whereas the government is obliged to establish a counter drone system protecting the parliament and the royal family. However, all of these sensors and systems should from the beginning be made ready for integration with each other in a bigger and broader unmanned traffic management system that will enclose the entire capital region. Otherwise we will keep on chasing our own tails for many years to come.

Takedown of SMS-based FluBot spyware infecting Android phones

An international law enforcement operation involving 11 countries has resulted in the takedown of one of the fastest-spreading mobile malware to date. Known as FluBot, this Android malware has been spreading aggressively through SMS, stealing passwords, online banking details and other sensitive information from infected smartphones across the world. Its infrastructure was successfully disrupted earlier in May by the Dutch Police (Politie), rendering this strain of malware inactive.

This technical achievement follows a complex investigation involving law enforcement authorities of Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands and the United States, with the coordination of international activity carried out by Europol's European Cybercrime Centre (EC3).

The investigation is ongoing to identify the individuals behind this global malware campaign.

Here is how FluBot worked

First spotted in December 2020, FluBot has gained traction in 2021 and compromised a huge number of devices worldwide, including significant incidents in Spain and Finland.

The malware was installed via text messages which asked Android users to click a link and install an application to track to a package delivery or listen to a fake voice mail message. Once installed, the malicious application, which actually was FluBot, would ask for accessibility permissions. The hackers would then use this access to steal banking app credentials or cryptocurrency account details and disable built-in security mechanisms.

This strain of malware was able to spread like wildfire due to its ability to access an infected smartphone's contacts. Messages containing links to the FluBot malware were then sent to these numbers, helping spread the malware ever further.

This FluBot infrastructure is now under the control of law enforcement, putting a stop to the destructive spiral.

International police cooperation

With cases spreading across Europe and Australia, international police cooperation was central in taking down the FluBot criminal infrastructure.

Europol's European Cybercrime Centre brought together the national investigators in the affected countries to establish a joint strategy, provided digital forensic support and facilitated the exchange of operational information needed to prepare for the final phase of the action. The J-CAT, hosted at Europol, also supported the investigation. A virtual command post was also set up by Europol on the day of the takedown to ensure seamless coordination between all the authorities involved.

Illegal webtoon site shut down as part of joint collaboration

Joint collaboration between INTERPOL, Korean and Moroccan law enforcement resulted in the shutdown of an illegal webtoon site and detention of a suspect. Moroccan authorities facilitated this action, thereby dismantling the criminal enterprise and protecting the rights of copyright holders.

The investigation into this website, SkyManga and the subsequent arrest of a Moroccan national followed a request from the Korean Ministry of Culture, Sports and Tourism. INTERPOL was then able to coordinate the efforts between Korea and Morocco.

The SkyManga website illegally distributed webtoon materials in Korean, Spanish and Japanese. At the same time, it profited from advertisement and donations.

"It is our pleasure to support the I-SOP project and to work in partnership with INTERPOL and all member countries against online piracy. We especially thank NCB Rabat and Moroccan law enforcement agencies for their contribution on the case," said Yong-han YUN, Director of the Copyright Protection Division of the Ministry of Culture, Sports and Tourism, Korea Republic.

"NCB Rabat always endeavours to collaborate with other NCBs and seek the information needed from other NCBs to investigate a crime committed in Morocco and assist another country. NCB Rabat was pleased to provide support on this International case and bring it to a satisfactory conclusion," said Mohammed DKHISSI, Head of NCB Rabat, Morocco.

The successful collaboration comes under the INTERPOL Stop Online Piracy Project (I-SOP). This five-year project is the product of close cooperation between INTERPOL and the Republic of Korea's National Police and Ministry of Culture, Sports, and Tourism. By working in collaboration with member countries and private and public bodies, I-SOP aims to combat crimes involving intellectual property infringement such as trademark counterfeiting and copyright piracy.

Digital piracy is a global threat, affecting creative industries such as film, TV, music and publishing, as well as the economy at large. Illegal downloads and distribution of such content cause substantial financial losses for the industries concerned which in turn affects tax revenue and jobs. Other related concerns centre on the fact that these crimes are often linked to other criminal activities, such as terrorist financing, money laundering and human trafficking.

Hundreds arrested and millions seized in global INTERPOL operation against social engineering scams

A worldwide crackdown on social engineering fraud has seen scammers identified globally, substantial criminal assets seized and new investigative leads triggered in every continent.

The two-month (8 March – 8 May 2022) Operation, codenamed First Light 2022, saw 76 countries take part in an international clampdown on the organized crime groups behind telecommunications and social engineering scams.

Police in participating countries raided national call centres suspected of telecommunications or scamming fraud, particularly telephone deception, romance scams, e-mail deception, and connected financial crime.

Based on intelligence exchanged in the framework of the operation, the Singapore Police Force rescued a teenage scam victim who had been tricked into pretending to be kidnapped, sending videos of himself with fake wounds to his parents and seeking a EUR 1.5 million ransom.

A Chinese national wanted in connection with a Ponzi scheme estimated to have defrauded nearly 24,000 victims out of EUR 34 million was arrested in Papua New Guinea and returned to China via Singapore.

Get-rich-quick schemes

With the Internet creating new online career prospects, companies and professionals who turn to e-commerce affiliate and EBShopp business opportunities are increasingly being scammed.

As part of Operation First Light 2022, the Singapore Police Force arrested eight suspects linked to Ponzi-like job scams. Scammers would offer high-paying online marketing jobs via social media and messaging systems where victims would initially make small earnings, and subsequently be required to recruit more members to earn commissions.

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

March 7th-9th, 2023

BATON ROUGE, LOUISIANA

A Homeland Security Event

Collaborating and Cooperating for Greater Security

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

Invitation to Exhibit

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

The 4th 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 in Baton Rouge, Louisiana 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 exhibiting and sponsorship opportunities contact:

Ray Beauchamp
(Americas)
E: rayb@torchmarketing.co.uk
T: +1 559-310-0330

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

Supporting Organisations:

Media Partners: