critical infrastructure PROTECTION AND RESILIENCE NEWS

Official Magazine of

International Association of CIP Professionals

SPRING 2023
www.cip-association.org

FEATURE:
Protection of Critical Maritime Infrastructure with New Technologies

FEATURE:
Get ready for the transformative effect of blockchain on critical infrastructures

FEATURE:
An Interview with European Utilities Telecom Council

WHAT DOES INTERNATIONAL LAW SAY ABOUT CYBER ATTACKS ON CRITICAL INFRASTRUCTURE?

critical infrastructure PROTECTION AND RESILIENCE EUROPE

3rd-5th October 2023

Prague, Czech Republic

www.cipre-expo.com

Supported by:

MINISTRY OF INDUSTRY AND TRADE OF THE CZECH REPUBLIC

INVITATION TO PARTICIPATE

Securing the Inter-Connected Society

Registration Open - Early Bird Delegate Fees apply

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

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

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

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

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

Register online at www.cipre-expo.com.

To discuss sponsorship opportunities contact:

Paul Gloc
(UK and Rest of World)
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: +1-408-921-2932

Leading the debate for securing Europe's critical infrastructure

www.cipre-expo.com

Co-Hosted by:

International Association of CIP Professionals

Supporting Organisations:

CoESS

IET.tv

NS&RC

ISIO

Media Partners:

World Security-index.com

critical infrastructure PROTECTION AND RESILIENCE NEWS

ARE WE ALL TALK AND NO ACTION?

A Nation's health, safety, and economy depend on the functioning of complex and interconnected infrastructure systems that provide critical services to communities across the nation. The evolution and escalation of threats and stressors to critical infrastructure, combined with their increased reliance on cyber, have led to an exponential increase in risks to national security.

CISA's Resilient Investment, Planning and Development Working Group (RIPDWG) recently published their White Paper, which was developed by the Research and Development (R&D) Task Group of the RIPDWG to highlight research, development, and innovation (RD&I) gaps associated with the resilience of cyber-physical critical infrastructure systems.

It stated "National policy highlights the need for such research, however the federal research enterprise has yet to fully capitalize on the opportunity by collectively executing an integrated RD&I strategy to address critical infrastructure security and resilience challenges, particularly at the community level."

This appears to be a message that has been going round for some time. Certainly since we started the Critical Infrastructure Protection & Resilience conferences nearly 10 years ago, a regular outcome has been the need for research, integration, communication and coordination between infrastructure sectors, yet here we are still appearing to be coming up with the same message - this is what we 'should' be doing.

With increasing tensions in the world, and new and developing cyber threats, which can be borne from the comfort of an attackers sofa, we need to be seeing greater action to protect interconnected infrastructure and the cascading impacts of disruptions that can be caused by a simple blackout, for example.

Having come away from Baton Rouge, where at Critical Infrastructure Protection & Resilience North America saw over 300 delegates from operators, federal and state government, law enforcement and the broader CI industry, following some great discussions and promise of investment in security and resilience, and enhanced cooperation and collaboration.

Make no mistake, there is some great work being done to secure some infrastructure demonstrated by some great example case studies. However, it is still not sufficient when we continue to see reports of cyber attacks across infrastructures especially the power networks, dangerous rail incidents, gunmen attacks on educational establishments. Only time will tell if this is more words or whether action will be taken.

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.

What Does International Law Say About Cyber Attacks on Critical Infrastructure?

The following essay is an excerpt, edited for clarity and brevity, of The Tallinn Manual 2.0 on Nation-State Cyber Operations Affecting Critical Infrastructure by Terence Check. The entire article, including source materials, was published in Volume 13, Issue #1 of the American University National Security Law Brief and is available at https://digitalcommons.wcl.american.edu/nslb/vol13/iss1/1/.

Protecting critical infrastructure from cyber threats is difficult and complex. News headlines abound with reports that show how critical infrastructure—ranging from voting machines to steel mills—have become increasingly vulnerable to cyber operations from state and sophisticated non- state actors. As critical infrastructure becomes increasingly entangled with the Internet and as new tactics, techniques, and procedures rapidly proliferate and evolve, governments and businesses alike must contend with a mutating threat environment that may put sensitive and highly important critical infrastructure assets in serious jeopardy. The vulnerabilities of critical infrastructure, which provide vital services and functions to societies, may pose a particularly tempting way for states to asymmetrically project power during an armed conflict or other crisis. Recent tensions between Russia and Ukraine have provided a useful test bed to consider how cyber-threat actors could couple cyber-based operations with movements of traditional military forces.

The fact that most critical infrastructure assets are owned

or operated by small or local businesses and governments does not shield those assets from international interest: security through obscurity is probably no longer a viable option for an interconnected world filled with sophisticated cyber threat actors with an eye to gain diplomatic, economic, or military advantages by targeting critical infrastructure. Understanding this fundamental fact, that predominantly private entities must contend with a cybersecurity environment shaped by geopolitical trends and forces of the highest order, this essay examines the Tallinn Manual 2.0 on the International Law Relating to Cyber Operations and how the law of armed conflict may impact critical infrastructure assets in cyberspace, especially during an armed conflict. Truly, each of these concepts discussed herein would warrant a fulsome discussion in their own right. This author hopes to provide a better, if cursory, understanding of the Manual's examination of legal norms applicable to critical infrastructure; and to spot issues illuminated by the Manual to enable lawyers practising in the area of cybersecurity to provide better advice to their clients (whether public or private) regarding operational risks that may arise from foreign state actors.

The Tallinn Manual 2.0 (the "Manual") is a treatise that restates the lex lata—the international law as it currently is—regarding cyber operations.10 Both versions11 of the Manual were developed by two groups of pre-eminent legal scholars in the area of the law of armed conflict and international law more generally, known as the International Group of Experts ("Group of Experts" or "Experts").

Because the Experts all hail from Western nations, decision-makers must temper their expectations and reliance on what type of conduct the Manual proscribes because the Manual mainly reflects Western legal perspectives. While customary international law would bind all states' cyber activities, one cannot predict how non-Western governments might apply these legal rules to the still- developing field of cyber operations, so much remains uncertain.

Critical infrastructure owners/ operators and government agencies will find that the Manual's unstated approach to critical infrastructure is a double-edged sword. Unfortunately, it appears that international law as restated in the Manual would permit a state actor to launch cyber operations against critical infrastructure in some circumstances, opening vulnerable and sensitive assets to sophisticated attacks from foreign adversaries. The good news is that many types of critical infrastructure are entitled to some manner of special legal protections under the law of armed conflict. Additionally, there are many tools at a government's disposal, as described in the Manual, to guard against and respond to cyber operations targeting critical infrastructure.

One takeaway from the Manual is that critical infrastructure owners and operators and defending governments should not assume that an attacker will refrain from launching operations merely because there is significant doubt as to a target's civilian status. Therefore, defenders should proceed under the assumption that when in doubt, an attacker will favour military expediency over certainty when resolving doubt as to status of objects, and should assume that civilian infrastructure may be targeted if its civilian status is unclear.

Another conclusion is that certain types or sectors of critical infrastructure may be entitled to additional protections under international humanitarian law. For example, in addition to the heightened duty of care that belligerents must take in targeting civilian objects generally, an even more prescriptive rule applies to critical infrastructure that is "indispensable to the survival of the civilian population." Under Manual Rule 141, attacks on

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

food and agricultural infrastructure and other critical items "indispensable to survival" are prohibited outright. Similarly, dams, dykes, and nuclear plants belong to a class of critical infrastructure assets to which special precautions apply under the law of armed conflict. Article 56 of Additional Protocol I of the Geneva Conventions states that dams, dykes, and other critical infrastructure containing "dangerous forces" (such as large tanks of volatile, toxic chemicals) can never be attacked—no matter how vital the target. Experts disagree, however, as to how far these precautions extend.

Largely, the question of whether a given type of critical infrastructure is entitled to protection—in other words, whether cyber attacks directed at that piece of critical infrastructure may violate the law of armed conflict—is primarily based on two considerations: 1) the ultimate actual effects of that attack on the civilian population and 2) whether the critical infrastructure asset in question falls into one of the specific prescribed categories of specially protected infrastructure. As the Tallinn Manual shows, the lex lata of the law of armed conflict certainly indicates that critical infrastructure—including civilian critical infrastructure—can certainly become a target of a belligerent party during the conduct of hostilities. Nevertheless, the law of armed conflict places limits and prohibitions on attacks on some types of critical infrastructure. It is difficult to make predictive judgments about what kind of critical infrastructure might be a permissible target of a cyber-attack, as definitions pose an interpretive challenge. Still, it is clear that there is some significant risk that a hostile actor might lawfully target critical assets and systems during an armed conflict. Critical infrastructure and the governments that protect such infrastructure should plan accordingly.

About the Author

Terence Check is Senior Counsel at the Cybersecurity and Infrastructure Security Agency, Department of Homeland Security; Adjunct Professor, Cleveland State Law School; LL.M in Law & Government, specialising in National Security Law and Policy, American University Washington College of Law (2015); J.D., magna cum laude, Cleveland State University, Cleveland-Marshall College of Law (2014); Editor-in-Chief, Cleveland State Law Review (2013-2014). This article also does not reflect the views of the Department of Homeland Security, or CISA, or any other institution and all opinions expressed are solely those of the author.

One Sea Association and ESA partner to support the uptake of autonomous shipping in the maritime sector

The One Sea Association and the European Space Agency (ESA) have signed a Memorandum of Intent (MoI) to support the uptake of autonomous shipping in the maritime sector, underpinned by space solutions.

One Sea and ESA have decided to establish a strategic collaboration to promote the development of new space-enabled services which will support the maritime sector's transition towards autonomous shipping. Autonomous shipping offers new opportunities to deploy safe, commercially viable, and environmentally sustainable maritime operations.

Satellite communications and satellite navigation play a key role in the adoption of autonomous shipping technologies and operations. During offshore passages, ships are often further from land than satellites which can offer invaluable secure and resilient communication channels for monitoring, command, and control of autonomous ships. Furthermore, in ports and congested areas, high precision Position Navigation and Timing (PNT) provided by satellites is also critical for the safe operation of autonomous shipping.

This new partnership will combine One Sea's unique expertise in the maritime sector and in autonomous shipping with ESA's technical competence and mandate through the Business Applications and Space Solutions programme to support the development and demonstration of space solutions in addressing user needs.

Protection of Critical Maritime Infrastructure with New Technologies

by Artur Lucas da Silva, Business Management & Administration (MBA & MSc) | Maritime Governance | Maritime Security | Advisory and Consultant Portuguese Navy

Protecting Critical Maritime Infrastructure with Unmanned Maritime Systems

Global trade, transportation, and security require critical maritime infrastructure. As the globe becomes more integrated and dependent on marine transit, these critical infrastructures face more significant challenges. Hence, unmanned maritime systems (UMS) must improve maritime security.

UMS are autonomous marine vehicles. Oceanographic research, environmental monitoring, and search and rescue missions employ them remotely or autonomously. Their best use is protecting critical maritime infrastructure.

Ports, harbours, rivers, bridges, and offshore platforms are critical maritime infrastructure. Terrorism, piracy, smuggling, and natural calamities threaten these infrastructures. Protecting these assets from these risks is crucial to global trade and worker protection.

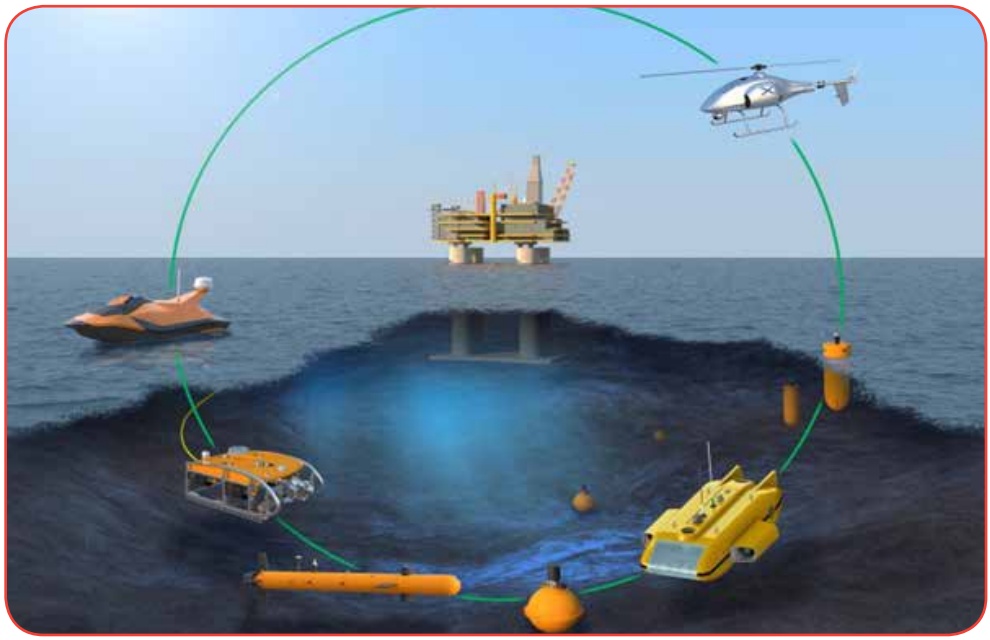
UMS can provide 24/7 surveillance and monitoring of these critical infrastructures. Radar, sonar, and cameras can detect dangers. They can also transmit real-time data to shore-based operators to help them respond to hazards.

Opportunities and Challenges for UMS

UMS's ability to operate in dangerous environments where human assistance is difficult or impossible is one of its main advantages. They can be used to keep an eye on offshore sites vulnerable to bad weather and waves. Sensors may be installed in UMS to monitor the platform for any signs of leaks or damage, allowing for rapid response in the case of an emergency.

Similarly, UMS can prevent smuggling and piracy in harbours and ports. Cameras may be installed on them to monitor passing ships and spot any suspicious behaviour. They can also monitor vessels suspected of breaking port laws or entering prohibited regions. As a result, operators can keep tabs on a sizable region with fewer people and money because of UMS's force-multiplying capabilities.

The vulnerability of UMS to hackers has increased. Cybersecurity technologies can be integrated into UMS to shield vital infrastructure from cyber-attacks.



Source: https://marinet.org

While UMS has many benefits, it comes with its share of difficulties. The legal constraints placed on its implementation constitute a significant obstacle. There is a need for standardisation in terms of technology, operations, and safety, but the international maritime community still needs to develop a complete framework for adopting UMS. Intended for use in rescue missions. In the event of a maritime disaster, UMS can conduct rescue operations. They can be outfitted with sensors to track down survivors and relay that information in real-time to shore-based rescue workers. As a result, UMS can shorten reaction times and improve survivors' odds in marine disasters.

In addition to closely checking things, UMS can defend vital infrastructure from cyberattacks as maritime companies rely more and more on technology, operations, and safety.

Source: https://electronica-submarina.com

Source: https://electronica-submarina.com

Another challenge is the cost of UMS. While the cost of UMS has decreased in recent years, they still require a significant investment. Therefore, there is a need to develop sustainable business models for the deployment of UMS, including public-private partnerships and subscription-based services.

In conclusion, UMS have the potential to revolutionize maritime security by providing 24/7 surveillance and monitoring of critical infrastructure. They can protect ports, harbours, waterways, bridges, and offshore platforms from various threats, including terrorism, piracy, smuggling, and natural disasters. However, there are also challenges in using UMS that need to be addressed.

A short overview of the challenges

A short overview of the challenges of using UMS to protect critical maritime infrastructure.

1. **Regulatory framework**: There currently needs to be a comprehensive international regulatory framework governing the use of UMS; this lack of standardisation challenges operators deploying UMS in different regions and countries. There is a need for a standard framework that addresses technology, operations, and safety.

2. **Cost**: While the cost of UMS has decreased recently, it still requires a significant investment. This cost can be a barrier to entry for many organisations and governments that want to deploy UMS to protect critical maritime infrastructure. There is a need to develop sustainable business models for deploying UMS, including public-private partnerships and subscription-based services.

3. **Technology**: UMS depends on technology to work, and making and keeping this technology up to date takes work. For example, for UMS to work well, it needs sensors, communication, and security systems. The technology must also be strong enough to work reliably in harsh maritime conditions.

4. **Safety**: UMS must be designed to operate safely in the maritime environment. There is a need to ensure that UMS are designed with redundancy and fail-safe mechanisms to prevent accidents. Additionally, operators must be trained to operate UMS safely and respond to emergencies effectively.

5. People may worry about privacy, security, and safety if UMS is used in the maritime domain. It is essential to make sure that the public knows how UMS helps protect critical maritime infrastructure and to answer any questions they may have.

Protecting critical maritime infrastructure with UMS has several advantages. Nevertheless, ensuring their deployment is carried out successfully and securely requires that the difficulties connected with their usage be handled. If these issues are resolved, UMS can contribute significantly to maritime security and critical infrastructure protection.

UMS as a [small] coastal country solution for the protection of critical maritime infrastructure

UMS can be a viable solution for small coastal countries to protecting their critical maritime infrastructure. Small coastal countries often face unique challenges when it comes to maritime security. To protect their maritime borders and critical infrastructure, they may need more resources, including personnel, vessels, and technology. This can make them vulnerable to maritime security threats, including piracy, smuggling, and terrorism.

UMS offer several advantages for small coastal countries looking to enhance their maritime security. For example:

1. **Cost-effectiveness**: UMS can be a cost-effective solution for small coastal countries because

they need fewer people and resources than traditional crewed vessels.UMS can also work for extended periods and cover more considerable distances than manned vessels, making them a better choice for maritime surveillance and protection.

2. **Scalability**: UMS can be scaled to fit the needs of small coastal countries. Depending on their needs and resources, these countries can deploy a single or multiple UMS. UMS can also be customised to suit specific missions and tasks, such as surveillance, monitoring, or detecting threats.

3. **Flexibility**: UMS are highly adaptable and can be used in a variety of maritime environments, including shallow waters, ports, and harbours. They can also be equipped with different sensors and payloads, such as cameras, radars, and sonars, to perform various tasks.

4. **Safety**: UMS can help make the seas safer by lowering the risks of manned vessel operations.UMS can have advanced navigation systems and sensors that can find and avoid collisions and other dangers.

5. **Situational Awareness**: UMS can be used to improve situational awareness in the maritime domain. This gives small coastal countries real-time information about ship movements and possible threats. This can help these countries respond more quickly and effectively to maritime security incidents.

Small coastal countries that want to improve their maritime security and protect their critical infrastructure can use UMS effectively. UMS

offers cost-effective, scalable, and flexible maritime surveillance and protection options. By leveraging UMS, small coastal countries can improve their maritime domain awareness and response capabilities, contributing to a safer and more secure maritime environment.

Food for thought

UMS has emerged as a promising option for protecting critical maritime infrastructure. Maritime critical infrastructure plays a crucial role in the global economy, and its protection is essential to ensure the safety and security of maritime operations.

UMS have some benefits for protecting critical maritime infrastructure, such as being cost-effective, scalable, and adaptable. They can work for long periods, cover large areas, and be outfitted with different sensors and payloads for different jobs.

While challenges are associated with deploying UMS, such as the lack of a regulatory framework and cost and safety concerns, these challenges can be addressed by developing standardised frameworks, sustainable business models, and safety protocols.

In the rapidly changing security environment of today, UMS is becoming more and more important to make sure that critical maritime infrastructure is safe and secure. By using UMS, organisations and governments can improve their understanding of the maritime domain, improve their ability to respond, and protect their critical infrastructure from different threats to maritime security..

UMS are a great way to protect critical maritime infrastructure, and if we want to improve maritime security in the future, we will need to keep developing and deploying them.

CLOSING COMMENTS - CRITICAL INFRASTRUCTURE PROTECTION & RESILIENCE NORTH AMERICA – MARCH 2023, BATON ROUGE

Before we all head off home, back to the office or out for a light refreshment, I just wanted to close the conference with a few comments.

It has been a great pleasure to be able to bring CIPRNA back to Louisiana and fascinating to learn how quickly you can lose $100 in the casino here at this lively venue in the heart of Baton Rouge.

Events such as these provide fantastic networking opportunities and I always go away having learned something new and worthwhile and I do hope you have 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 had a great start on Tuesday afternoon with the keynote session with senior representatives from Government Agencies, the Governor's Office, the Mayor's Office and from Infraguard LA.

Dr David Mussington, the Executive Assistant Director for Infrastructure Security within CISA started us off (without slides!) outlining the significant challenges to infrastructure from a range of threats and hazards both domestic and international. He made a strong point about how the policies designed and driven from Washington have to be developed and structured so that they can be delivered locally and meet local conditions.

This was a point that was continually referenced throughout the conference and was reinforced by Casey Tingle from the Governor's Office of Louisiana who reminded us all – 'that all disasters are local – they start local and end local'.

The keynote session concluded with Eric Rollison, the Assistant Director of risk analysis, resilience and recovery at CESER (the office of Cybersecurity, Energy Security and Emergency Response) focusing on the enormous challenges to the energy sector internationally and also educating the audience on the difference between CISA and CESER, one being a Government Agency and the other being a type of salad.

So, over the three days we have covered a whole range of topics where Cyber Security was by far the main topic of conversation. This was not surprising when you consider how many members of the Cybersecurity & Infrastructure Security Agency (CISA) were in attendance. I think about 80% of staff from their organisations had made the trip to be here with us in Baton Rouge.

The issue of cyber is clearly a major threat and a significant concern to all and some of that concern is obviously exacerbated by the current conflict in Ukraine. However, it was reassuring to note the amount of national effort and innovation currently being put in place and also the practical support available to infrastructure owners and operators.

We heard from several speakers about the importance of Public-Private Partnerships and the inherent challenges in developing trust and relationships. The need for continual collaboration and communication was constantly referenced and the message from almost every Agency present was that – 'when something bad happens you know who to call' – but no one mentioned 'Ghostbusters'.

7th-9th March 2023 saw the latest gathering of the Critical Infrastructure Protection & Resilience community, in Baton Rouge, Louisiana. Critical Infrastructure Protection & Resilience North America (CIPRNA) saw over 300 delegates from across the Americas gather to share stories and experiences amongst peers and industry experts, helping to enhance knowledge and understanding of the latest threats and challenges facing the sector.

Here we share some great memories of this exciting event, where many new contacts were made during the great networking opportunities afforded to the delegates throughout the 3 day conference.

2023 Critical Infrastructure Protection & Resilience North America outline topics of discussion included:

Plenary Session Topics

- CI Interdependencies and Cascading Effects in Community Situational Awareness
- Panel Discussion: "The Last Mile" Community Roles in Critical Infrastructure and National Preparedness
- Emerging Threats against CI
- Crisis Management, Coordination & Communication
- Realities and the CI Resilience Imperative
- Developing Resilience Strategies
- Mitigating Major Threats
- Technologies to Detect and Protect

As well as a series of sector focused symposiums:

Mini Symposiums

- Power & Energy Sector Symposium
- Transport Sector Symposium
- Communications Sector Symposium
- CBRNE Sector Symposium
- Critical Manufacturing & Logistics Sector Symposium
- Government, Defence & Space Sector Symposium

As we look towards the 2024 event, you can submit your abstract for considerations for inclusion in the agenda, through the Call for Papers via the website at: www.ciprna-expo.com/call-for-papers

Co-Hosted by:

International Association of CIP Professionals

Supported by:

INFRAGARD MEMBERS ALLIANCE LOUISIANA

Gold Sponsor:

BOSCH Invented for life

Silver Sponsors:

Johnson Controls

milestone

Bronze Sponsors:

Texas A&M Engineering TEEX Extension Service

Genetec

ECHODYNE

Flagship Media Partners:

critical infrastructure PROTECTION AND RESILIENCE NEWS

GTSC Homeland Security

Coffee Break Sponsor:

AXIS COMMUNICATIONS

Conference Proceedings Sponsor:

PSC PROFESSIONAL SYSTEMS ENGINEERING

Over 300 Delegates

Over 300 delegates attended the conference and expo in 2023.

Key Partners

Key partner organizations, such as CISA, TSA, FBI, USCG, IACI and TIEMS participated in Baton Rouge, LA on 7th-9th March 2023

Save The Dates

Join us in Lake Charles, LA on 12th-14th March 2024 for the next gathering of the CIP industry

The conference covered a whole range of other topics as we moved on from the keynote session, starting with - Making a Business Case for Security – Cost Benefit Budgeting. This was an informed and practical example of how to build an effective business case to secure protection and resilience funding and was a topic that really resonated with those in the room. We all know how difficult it can be to secure the right level of funding unless something dramatic happens and then it is too late.

Other areas explored included:
- Mitigating Major Threats
- Climate Change and related Weather Events
- Insider Threats
- New Technologies
- Transport
- Energy
- CBRNE
- Supply Chain issues and
- Crisis Management Coordination

We had some references to terrorism dotted throughout the conference but not as much as I expected. We were, however, reminded that there has been a significant increase in Bomb Threats in the United States in 2022.

We had some really great presentations – I liked what Dr Ron Martin had to say about being constantly aware of what we are all up against in the struggle to protect our infrastructure when he stated that – 'The people who want to kill us and/or do us harm are working faster and sometimes smarter than we are and we not only have to catch them up but we have to overtake them'.

This tied in very neatly to the session delivered by George Markowsky, from the International Emergency Management Society. He referenced a quote from Sun Tzu, the Chinese Military Strategist – 'Know thy enemy – Know thy self' - reflecting on the fact that we have to understand who our enemies are, what resources they have and what they seek to do to us to cause harm.

We also had a speaker position their views on protection around a fairy tale, that of the Three Little Pigs. Everyone knows the story, the first little pig built a house of straw, having done no real threat assessment whatsoever. The second pig built his house of sticks. He gave some thought to the threats he might face but not enough. The third little pig, the sensible one, built his house of bricks having really thought thorough all of the issues that might arise. The obvious moral of the story being that you have to carefully consider – 'What to protect – from what and how you do it effectively'.

As I said on day one, the world is an unpredictable place and is constantly and rapidly changing. The protection and resilience of our infrastructure and information requires us all to continually change, adapt and innovate and one of my favourite historical quotes, from the great 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'.

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 Lester Millet and Infragard LA for all their assistance in putting the conference together and the support provided by the Governor's Office and the Mayor's Office.

Also, all of our sponsors, in particular our gold sponsor, Bosch.

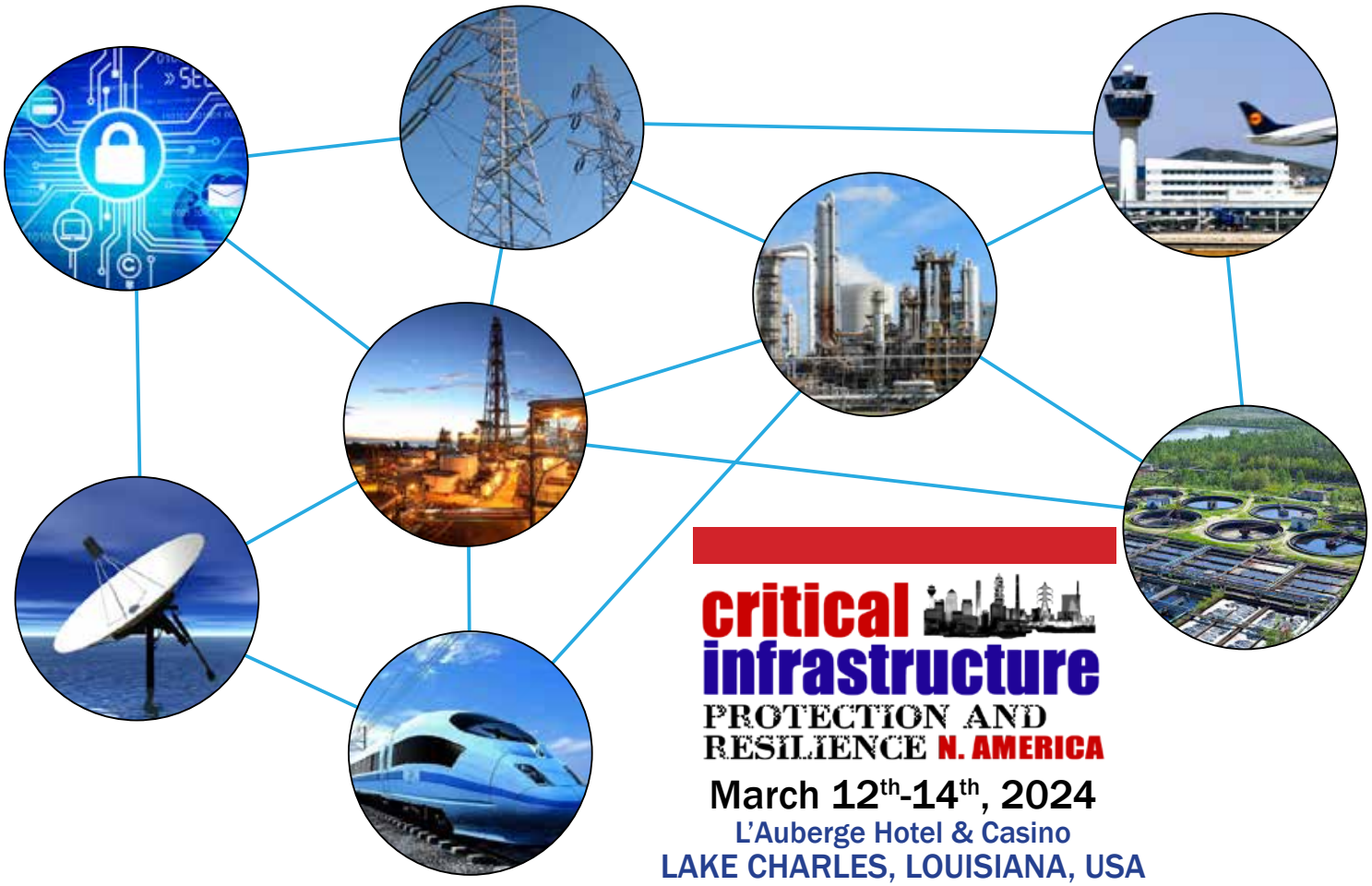
The hotel and the caterers for looking after us so well and helping us all to put on some extra weight.

The AV guys for keeping things running so 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 Louisiana in March next year, the 12 to the 14th and our European event will be in Prague in October this year.

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

John Donlon QPM FSyI
CIPRNA Conference Chair



critical infrastructure PROTECTION AND RESILIENCE N. AMERICA

March 12th-14th, 2024

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

A Homeland Security Event

SAVE THE DATES

Securing the Inter-Connected Society

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

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

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

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

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

To discuss sponsorship opportunities contact:

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

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

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

The premier discussion for securing America's critical infrastructure

Owned & Organised by:

Supporting Organisations:

Media Partners:

IACIPP Speak at CyberCon Conference in Bucharest

John Donlon QPM FSyI, Chairman of the International Association of Critical Infrastructure Protection Professionals (IACIPP), was a guest speaker on behalf of the National Institute for Research & Development in Informatics (ICI Bucharest) at the CyberCon Conference which took place in Romania between the 22nd and 27th May.

John was on a panel session addressing the subject of Cyber Diplomacy. The session was moderated by Carmen-Elena CÎRNU, the Scientific Director of ICI Bucharest and opened by the Director General of ICI Bucharest, Victor Vevera. In his opening address Victor referenced the Romanian position on Cyber Diplomacy from his organisations perspective and also highlighted the continuing partnership with IACIPP and the successful joint conference held in the Romanian Royal Place in 2022.

John delivered a presentation where he outlined his views on how the type and nature of the crisis being faced within our increasingly interconnected, globalised and rapidly changing world were ever evolving referencing the pandemic, the war in Ukraine and the devastating earthquakes that hit Turkey and Syria at the start of this year.

He summarised the development of IACIPP and what it seeks to achieve as a platform for likeminded individuals. The aim being to create a space to share information, connect and communicate on all matters relating to the protection and resilience of national infrastructure and information. The focus being on the part that such an association can play in facilitating communication across both the public and private sectors.

That need for connectivity was a common thread throughout the session. It was acknowledged that the worlds infrastructure and cyber position is a greater target and more vulnerable than ever and in order to address issues of concern there is a requirement to continue to develop a comprehensive approach that aligns both physical and cyber security, protection and resilience through enhanced levels of cooperation and coordination.

There was consensus across the panel and from the audience, of the continued need for greater levels of coordination, cooperation and communication across both nation states and between public and private sector entities.

It was recognised that the development of Cyber Diplomacy along with the growth in Cyber Ambassadors across the globe could go some significant way to addressing cyber problems internationally and improving the connectivity that has to be in place.

CISA Warns of Hurricane/Typhoon-Related Scams

The Cybersecurity & Infrastructure Security Agency (CISA) urges users to remain on alert for malicious cyber activity following a natural disaster such as a hurricane or typhoon, as attackers target potential disaster victims by leveraging social engineering tactics, techniques, and procedures (TTPs). Social engineering TTPs include phishing attacks that use email or malicious websites to solicit personal information by posing as a trustworthy organization, notably as charities providing relief. Exercise caution in handling emails with hurricane/typhoon-related subject lines, attachments, or hyperlinks to avoid compromise. In addition, be wary of social media pleas, texts, or door-to-door solicitations related to severe weather events.

CISA encourages users to review the Federal Trade Commission's Staying Alert to Disaster-related Scams and Before Giving to a Charity, and CISA's Using Caution with Email Attachments and Tips on Avoiding Social Engineering and Phishing Attacks to avoid falling victim to malicious attacks.

Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)

The NIS Directive— the first EU cybersecurity law — is the first horizontal internal market instrument aimed at improving the resilience of network and information systems in the Union against cybersecurity risks. Despite its notable achievements, the NIS Directive has shown certain limitations. The digital transformation of society, intensified by the COVID-19 crisis, has expanded the threat landscape. New challenges have appeared, which require adapted and innovative responses.

To be able to analyse the impact and identify the deficiencies of the NIS Directive, the Commission carried out an extensive stakeholder consultation. The Commission identified the following main issues:

- insufficient level of cyber resilience of businesses operating in the EU
- inconsistent resilience across Member States and sectors
- insufficient common understanding of the main threats and challenges among Member States
- lack of joint crisis response.

As a result, and in order to respond to the growing threats due to digitalisation and interconnectedness, in December 2020 the Commission proposed

a revised set of future-proof rules aiming to strengthen the level of cyber resilience in the Union, on which the co-legislators have reached a political agreement on 13 May 2022 and formally adopted the new Directive in late November 2022.

The NIS2 Directive provides legal measures to boost the overall level of cybersecurity in the EU, in order to contribute to the overall functioning of the internal market. It builds on the 3 main pillars that were the basis of the NIS1 Directive:

1. Building on the NIS1 strategy on the security of network and information systems, in order to achieve a high level of preparedness of Member States, the NIS2 Directive requires Member States to adopt a national cybersecurity strategy. Member States are also required to designate national Computer Security Incident Response Teams (CSIRTs), who are responsible for risk and incident handling, a competent national cybersecurity authority, and a single point of contact (SPOC). The SPOC has to exercise a liaison function to ensure cross-border cooperation between the Member State authorities with the relevant authorities in other Member States and, where appropriate with the Commission and ENISA as well as to ensure cross-sectorial cooperation with other competent authorities within its Member State.

2. The NIS2 Directive also continues the NIS1 framework establishing the NIS Cooperation Group to support and facilitate strategic cooperation and the exchange of information among Member States, and the CSIRTs Network, which promotes swift and effective operational cooperation between national CSIRTs.

3. The NIS1 Directive ensures that cybersecurity measures are taken across seven sectors, which are vital for our economy and society and which rely heavily on ICT, such as energy, transport, banking, financial market infrastructures, drinking water, healthcare and digital infrastructure

Public and private entities identified by the Member States as operators of essential services (OES) in these sectors are required to undertake a cybersecurity risk assessment and put in place appropriate and proportionate security measures. They are required to notify serious incidents to the relevant authorities. Furthermore, providers of key digital services (digital service providers or DSPs), such as search engines, cloud computing services and online marketplaces, have also to comply with the security and notification requirements under the Directive. At the same time, the latter are subject to a so-called 'light-touch' regulatory regime, which entails that those entities are not subjected to ex-ante supervisory measures.

NIS2 Directive significantly expands the scope of sectors and introduces a size threshold to define which entities fall in its scope and would be required to report significant cybersecurity incidents to the national competent authorities.

What are the Key Elements of the NIS2 Directive?

The NIS2 Directive aims to address the deficiencies of the previous rules, to adapt it to the current needs and make it future-proof.

To this end, the Directive expands the scope of the previous rules by adding new sectors based on their degree of digitalisation and interconnectedness and how crucial they are for the economy and society, by introducing a clear size threshold rule— meaning that all medium and large-sized companies in selected sectors will be included in the scope. At the same time, it leaves certain discretion to Member States to identify smaller entities with a high security risk profile that should also be covered by the obligations of the new Directive.

The new Directive also eliminates the distinction between operators of essential services and digital

service providers. Entities would be classified based on their importance, and divided into two categories: essential and important entities, which will be subjected to different supervisory regime.

It strengthens and streamlines security and reporting requirements for companies by imposing a risk management approach, which provides a minimum list of basic security elements that have to be applied. The new Directive introduces more precise provisions on the process for incident reporting, content of the reports and timelines.

Furthermore, NIS2 addresses security of supply chains and supplier relationships by requiring individual companies to address cybersecurity risks in the supply chains and supplier relationships. At European level, the Directive strengthens supply chain cybersecurity for key information and communication technologies. Member States in cooperation with the Commission and ENISA, may carry out Union level coordinated security risk assessments of critical supply chains, building on the successful approach taken in the context of the Commission Recommendation on Cybersecurity of 5G networks.

The Directive introduces more stringent supervisory measures for national authorities, stricter enforcement requirements and aims at harmonising sanctions regimes across Member States.

It also enhances the role of the Cooperation Group in shaping strategic policy decisions and increases information sharing and cooperation between Member State authorities. It also enhances operational cooperation within the CSIRT network and establishes the European cyber crisis liaison organisation network (EU-CyCLONe) to support the coordinated management of large-scale cybersecurity incidents and crises.

NIS2 also establishes a basic framework with responsible key actors on coordinated vulnerability disclosure for newly discovered vulnerabilities across the EU and creates an EU vulnerability database for publicly known vulnerabilities in ICT products and ICT services, to be operated and maintained by the EU agency for cybersecurity (ENISA).

The evaluation of the current rules on security and incident reporting requirements has shown that in some cases Member States have implemented these requirements in significantly different ways. This has created an additional burden for companies operating in more than one Member State.

Furthermore, when it comes to cybersecurity requirements we want to be sure that all companies address the necessary core set of elements in their cybersecurity risk management policies.

For this reason, NIS2 includes a list of 10 key elements that all companies have to address or implement as part of the measures they take, including incident handling , supply chain security, vulnerability handling and disclosure, the use of cryptography and where appropriate, encryption.

When it comes to incident reporting, we need to strike the right balance between the need for swift reporting in order to avoid the potential spread of incidents, and the need for in-depth reporting to draw valuable lessons learned from individual incidents. The new Directive foresees a multiple –stage approach to incident reporting. Affected companies have 24 hours from when they first become aware of an incident to submit an early warning to the CSIRT or competent national authority which would also allow them to seek assistance (guidance or operational advice on the implementation of possible mitigation measures) if they request it. The early warning should be followed by an incident notification within the 72 hours of becoming aware of the incident and a final report no later than one month later.

EU Cooperation is taken forward by allowing Member States to act jointly and tackle emerging security risks posed by the ongoing digital transformation.

More specifically, Member States will be able to jointly supervise the implementation of EU rules and mutually assist each other in the case of cross-border malpractices, have a more structured dialogue with the private sector and coordinate the disclosure of vulnerabilities found in software and hardware sold across the internal market. They will also be able to work in a coordinated manner to assess the security risks and threats related to new technologies, as done for the first time with 5G.

Member States will draw on EU cooperation to improve national capabilities through staff exchanges between authorities and peer reviews. The existing groups, notably the Cooperation Group gathering national cybersecurity authorities and the Network of Computer Security Incident Response Teams (CSIRTs) will contribute to advance cooperation respectively at both strategic and technical levels.

Seabed warfare: Protecting the UK's undersea infrastructure

The attack on the Nord Stream pipelines in September 2022 highlighted the vulnerability of undersea infrastructure, such as cables carrying internet services and energy pipelines, to malicious attack. NATO says Russia is "actively mapping" critical infrastructure on the seabed.

The Ministry of Defence has accelerated the procurement of a new ship specifically to detect threats to the seabed and cables. RFA Proteus is expected to begin operating in summer 2023.

This Insight discusses threats to the UK's undersea critical national infrastructure and how the UK and allies are responding.

Why are undersea cables and pipelines important?

Undersea cables and pipelines form part of the UK's critical national infrastructure, the facilities, systems and networks necessary for a country to work.

On the seabed lie miles of telecommunication cables that enable internet access, financial transactions and the sharing of data essential to business and personal life. Estimates vary, but the Ministry of Defence suggests 99% of global internet traffic goes through undersea cables.

Seabed gas and oil pipelines provide essential energy supplies to the UK; 77% of all of the UK's gas imports came from Norway through pipelines lying under the North Sea.

The Ministry of Defence says the growing use of the seabed has "increased opportunities for adversaries to threaten Western subsea critical national infrastructure".

What is seabed warfare?

Seabed warfare broadly refers to undersea warfare in which the seabed is the focus.

Undersea warfare is not new; submarines have long played a vital role in the Royal Navy's history, while the Royal Navy has for decades maintained mine-countermeasure vessels in the Persian Gulf to destroy unexploded sea mines from the Iran-Iraq war.

What is new, or at least becoming more widely discussed in public, is the growing threat to critical infrastructure on the seabed and the resulting risk to national security.

What threatens undersea cables and pipelines?

The sabotage of the Nord Stream pipelines in the Baltic Sea in September 2022 highlighted the potential vulnerability of undersea cables and pipelines to malicious attack.

While most damage to undersea cables is caused by fishing or shipping activities, such as the damage to undersea cables that cut communication services to the Shetland Islands in autumn 2022, the European Parliament has warned of the "potential for sabotaging undersea cables during times of conflict" (PDF).

Advances in underwater technology, including autonomous and remotely piloted devices, mean seabed exploration has become more accessible.

This means that seabed warfare is "no longer a distant concept" but "represents an immediate and legitimate threat", according to a NATO Parliamentary Assembly committee draft report.

The threat from Russia

The UK Government said in a defence report in 2021 that Russia is developing "deep sea capabilities which can threaten undersea cables".

The Chief of the Defence Staff, Admiral Sir Tony Radakin, says there has been a "phenomenal increase in Russian submarine and underwater activity" over the last 20 years.

The French Government says Russia has been "upscaling in the field of seabed warfare" (PDF) and is "very active" in everything related to underwater combat.

In May 2023 a senior NATO official said Russia is "actively mapping" gas pipelines and internet cables.

How is the UK military responding?

One of the Royal Navy's tasks is to protect undersea critical national infrastructure (PDF).

The Royal Navy already operates Astute-class submarines, capable of detecting underwater activity and mine-counter measure vessels, which operate sub-surface systems. RAF maritime patrol aircraft can track surface and sub-surface vessels.

A new ship to defend undersea cables and pipelines

In 2021 the Ministry of Defence announced plans to develop a new multi-role ocean surveillance capability (MROS) to safeguard critical national infrastructure.

The Royal Navy ordered its first crewless submarine in December 2022 and is developing autonomous vehicles to detect sea mines with France.

The UK will also collaborate in developing undersea capabilities with Australia and the United States as part of the 2021 AUKUS agreement.

Help2Protect against the Insider Threat

Insider Threat Awareness and Program Development Training platform

Help2Protect.info

Protect your company from Insider Threats

In Collaboration with:

International Association of CIP Professionals

See below for 20% Off Special Offer

THREE TYPES OF INSIDERS - ONE TOOL TO DETECT THEM

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

BE PROACTIVE
AWARENESS TRAINING

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

BE READY
PROGRAM DEVELOPMENT TRAINING

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

An eLearning Platform dedicated to Security and the Insider Threat

www.help2protect.info

SPECIAL OFFER FOR IACIPP – 20% DISCOUNT OFF THE COURSE

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

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

Get ready for the transformative effect of blockchain on critical infrastructures

by Adrian Victor Vevera – General Director of the National Institute for Research and Development in Informatics ICI Bucharest, PhD. Eng., Nuclear Physicist by training, Scientific Researcher 2 title in the Romanian research establishment.

Distributed ledger technology took the world by storm through cryptocurrencies and financial innovation such as smart contracts. The repeated boom and bust of the crypto markets and their impact on the public consciousness should not distract us from the transformative effect that blockchain will have on Critical Infrastructure design and resilience. Research undertaken within the European Center for Excellence for Blockchain within ICI Bucharest and as a result of our own development of governmental blockchain application within the Blockchain Software Development Laboratory indicate that we may be on the precipice of stunning transformations. These will affect not only Critical Infrastructure design and operation, but also protection.

Blockchain works by enabling the integrity of distributed databases through computational processes.

With no need for an active central repository of ledgers of financial data, product inventories or private information, new applications and new efficiencies become possible across the breadth of almost every critical infrastructure domain, from finances and public services (the obvious), to transport, energy or defense. In addition to obvious applications such as the management of access rights for users or processes within zero-trust system architectures (which will become a valuable tool in critical infrastructure operation), there are also less than obvious applications – supply chain management with product origin safeguards, decentralized marketplaces (including for illegal products) or credential and claims management for the mass public. The drive for new efficiencies, lower costs and more responsiveness (combined with greater apparent security) will drive blockchain adoption far more rapidly than our capacity to regulate the technology itself outside of narrow areas such as certain financial instruments. The users themselves will not necessarily know that the backend of their product or service has a blockchain component when, for instance, they will want to prove their identity in the airport, transfer money, or sign a contract. This applies to individual and institutional users.

On that day, there will be a revolution in services and in the underlying critical infrastructure, generating new risks, vulnerabilities and threats, simultaneously as it reduces other issues such as fraud or error. Applications for blockchain solutions are possible in SCADA systems, in Infrastructure-as-a-Service system management, and in Common Data Environments, among others.

Our research into this suggests that, beyond the salutary effects of blockchain adoption, whether on efficiency or privacy and security, blockchain also generates new risks, vulnerabilities and threats. It may encourage overly decentralized systems which are, ironically, more opaque to analysts because of their complexity and more liable to sudden busts from undetected propagating systemic dysfunction. System governance is also more difficult in such an infrastructure landscape, with unintended consequences for top-down regulations. The application of blockchain to sensitive command, control and coordination technologies can lead to variability in system performance depending on the underlying blockchain infrastructure used, and even a very secure blockchain may be subverted by hackers or malicious insiders using unrecognized exploits or brute force takeovers. Secure blockchain applications can also lull decision makers into a false sense of security, enabling new threats to coalesce at the system points outside of the blockchain, such as user devices.

I am firmly convinced that a rapid adoption of blockchain is coming and it will result in a gradual new topology of the critical infrastructure landscape to which CIP practitioners, regulators and decision makers will have to adapt. We will be faced with more uncertainty, less information (even as we paradoxically drown in data) and less direct control over complex and distributed CI systems.

Can governments act to prevent this? I do not think we can put this particular genie back inside the bottle, except only to stifle its adoption within the public administration CI. The potential applications are too vast and the efficiencies too great to not entice the private entities that operate 75+% of our critical infrastructures, especially once smaller entities will have made the transition and become leaner and more profitable

as a result. The most that we can do is take charge of a responsible and resilient adoption of blockchain by establishing a close communication between public and private entities, by leading by example in terms of safe adoption and by reserving bans for the most systemically risky developments. Even then, we will just have to factor the problems of blockchain into our CIP calculus from now on, as the situation develops.

Adrian Victor Vevera – General Director of the National Institute for Research and Development in Informatics ICI Bucharest

China could hack US 'critical infrastructure', State Dept warns

Microsoft has discovered malicious activity by Volt Typhoon, a state-sponsored threat actor based in China, aimed at U.S. critical infrastructure organizations.

The campaign is focused on post-compromise credential access and network system discovery. Volt Typhoon typically focuses on espionage and information gathering.

Volt Typhoon is pursuing development of capabilities that could disrupt critical communications infrastructure between the United States and Asia region during future crises, according to Microsoft.

The US State Department has warned that China is capable of launching cyberattacks against critical United States infrastructure, including oil and gas pipelines as well as rail systems, after researchers discovered a Chinese hacking group had been

spying on such networks.

"The US intelligence community assesses that China almost certainly is capable of launching cyberattacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines and rail systems," State Department spokesperson Matthew Miller said in a press briefing.

"It's vital for government and network defenders in the public to stay vigilant," he said.

The espionage group – dubbed "Volt Typhoon" by Microsoft – was the subject of an alert issued by cybersecurity and intelligence agencies in the US, Australia, Canada, New Zealand and the United Kingdom – known as the "Five Eyes".

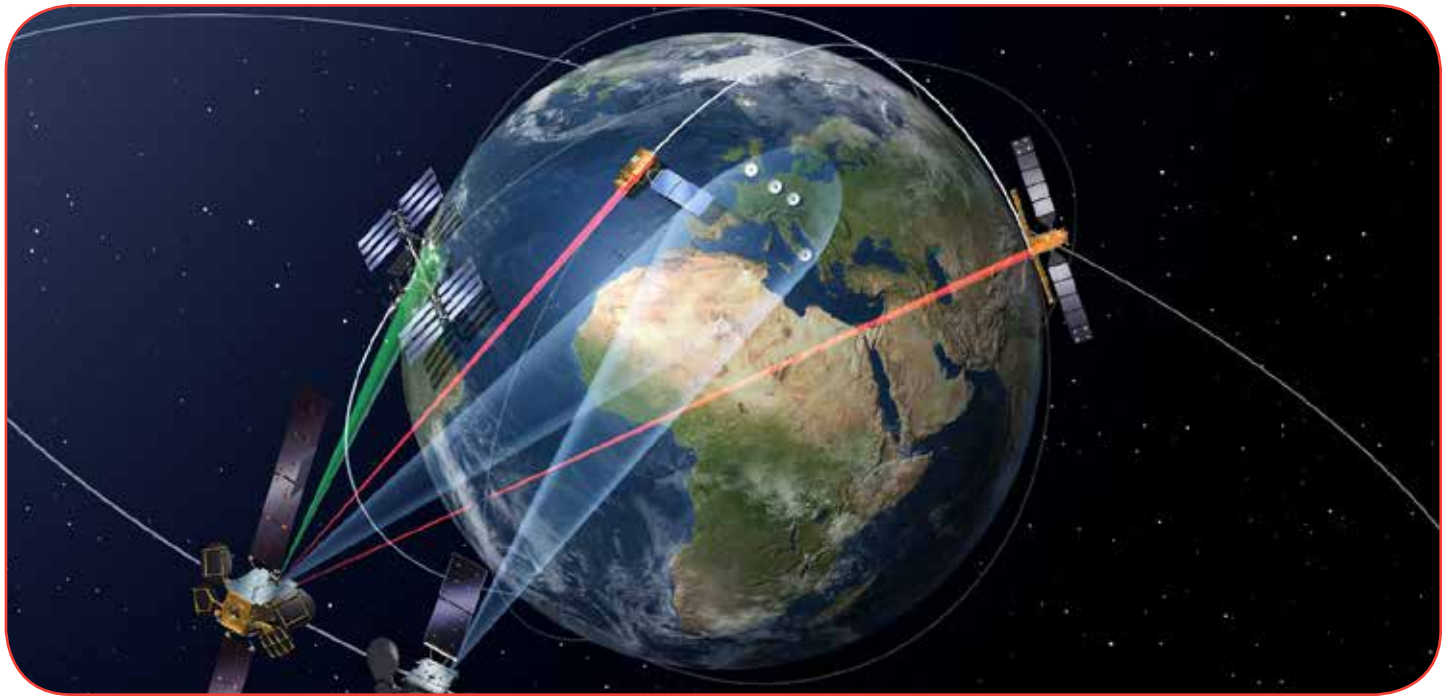
Microsoft researchers said Volt Typhoon was developing capabilities "that could disrupt critical communications infrastructure between the United States and Asia region during future crises" – a nod to the escalating tensions between China and the US over Taiwan and other issues.

Microsoft said the Volt Typhoon campaign relies on "living off the land" attacks, which are fileless malware that uses existing programmes to carry out attacks rather than installing files itself. The tech giant said Volt Typhoon blends in with normal network activity by routing data through office and home networking equipment like routers, firewalls and VPNs, making it extremely difficult to detect.

The hacking group has targeted critical infrastructure organisations in the US Pacific territory of Guam, Microsoft said, adding that the security firm Fortinet's FortiGuard devices were being abused by Volt Typhoon to break into its targets.

The US Cybersecurity and Infrastructure Security Agency (CISA) separately said it was working to understand "the breadth of potential intrusions and associated impacts".

Space Systems are Critical Infrastructure — Other Countries Already Know



At a recent conference in Paris, a Ukrainian general officer showed a slide that made clear that for his country, space systems are critical infrastructure. Why did he make this proclamation? It's simple: From its 2014 invasion of Crimea, Russia has sought to use cyber means to corrode the sovereignty of another country, trying to make it difficult to provide social services, collect taxes, and administer a sovereign government. Russia presaged its 2022 invasion of Ukraine with an attack on the space systems Ukraine uses to administer its civil government, as well as support its armed forces. In other words, Russia attacked Ukraine's sovereignty through the critical space systems on which the Ukrainians depend. Both countries recognize that for Ukraine, space systems are critical infrastructure.

The European Union, observing closely developments in Ukraine, have already declared space systems critical infrastructure; it's our turn now to follow suit.

Some have argued that space systems are really a subset of communication infrastructure. This argument ignores present reality in two ways: proliferation and unique infrastructure. Space missions have proliferated to include satellite communication, GPS services, remote sensing (optical, hyperspectral, etc.), travel, exploration, cislunar operations and soon, mining, manufacturing and settlement. Significant infrastructure is necessary to enable the space economy and all those use cases.

These include space manufacturing facilities, launch infrastructure, ground entry points and post-downlink analytical systems and centers.

Every critical infrastructure already identified in Presidential Policy Directive 21 depends on space systems, as is true for every National Critical Function. Use cases provided by the Space Information Sharing and Analysis Center demonstrate that our country's agricultural systems, oil and gas infrastructure, maritime infrastructures and other infrastructures depend on space systems. Space systems allow us to know exactly where and when to plant, and where to maneuver agricultural equipment to precise locations on our farms. They enable us to find and exploit natural resources, just as they give us the means to assess the extent and effects of climate change.

Space systems themselves represent unique missions, as well as their own unique industrial base and supply chain, and are poised to contribute more than $1 trillion of economic value over the coming decades. We've learned that space systems are vital — critical — to our national security, economic security, technological leadership, intelligence capabilities, civil infrastructure, economic competitiveness and global commitments. As new satellites are placed in orbit (over 7,000 are already aloft), our dependence on space systems will grow. Our rivals and adversaries clearly see our dependence on these systems; they are constantly seeking the means to undermine our ability to use these systems, to the detriment of our economy, national security and global presence.

Designating space systems as critical infrastructure would catalyze and energize efforts to enhance their cybersecurity and resilience. Such a designation can — and should — be followed by development of a national sector risk management architecture, one that unites the public and private sectors in support of our common interest in protecting our space system assets. A national research and development agenda could be developed, one that lowers the cost and raises the effectiveness of space systems cybersecurity solutions, thus making our space systems both safer and more competitive globally. More focused efforts would be undertaken to develop industrywide cybersecurity standards and controls for space systems; information sharing regarding threats, risks, vulnerabilities and mitigations would be enhanced as the government consolidated the architecture by which it informs our country's growing space sector. In turn, the commercial space sector would have an empowered government partner, representing the full range of public interests, with which to enhance space systems cybersecurity.

The designation of space systems as a critical infrastructure sector will require that the administration identify and assign responsibilities to a sector risk management agency. That agency must be equipped with the authorities and resources requisite to partner with industry and to consolidate government capabilities in support of space systems cybersecurity. It must also impart commitment to this role commensurate with its vital importance.

Space systems are growing, in number and in mission, as is our dependence on them. Overdue is the recognition that these systems are vital to the totality of our national interests. Other countries have achieved this recognition. Now, it's our turn.

Edward Swallow is the chief operating officer at The Aerospace Corporation, a nonprofit that operates a federally funded research and development center for the U.S. space enterprise. Samuel Visner is an Aerospace Corporation technical fellow and vice chair of the Space Information Sharing and Analysis Center Board of Directors.

Colonial Pipeline Cyber Attack: 2 Years On

The Attack on Colonial Pipeline: What We've Learned & What We've Done Over the Past Two Years by Jen Easterly, CISA Director; Tom Fanning, Chairman and CEO of Southern Company and Chair of CISA's Cybersecurity Advisory Committee

May 7 marked two years since a watershed moment in the short but turbulent history of cybersecurity. On May 7, 2021, a ransomware attack on Colonial Pipeline captured headlines around the world with pictures of snaking lines of cars at gas stations across the eastern seaboard and panicked Americans filling bags with fuel, fearful of not being able to get to work or get their kids to school. This was the moment when the vulnerability of our highly connected society became a nationwide reality and a kitchen table issue.

The good news is that since that event, the Biden-Harris Administration has made significant strides in our collective cyber defense, harnessing the full power of the U.S. government to address the full spectrum of the threat. At the Cybersecurity and Infrastructure Security Agency (CISA), we have been laser focused on improving resilience across our Nation's critical infrastructure. Recognizing that organizations need a simple way to access actionable and timely cybersecurity information, we developed stopransomware.gov to provide a central location for alerts and guidance for businesses and individuals. Recognizing that only cohesive collaboration across government will scale to meet the threat, we launched the Joint Ransomware Task Force with our

FBI partners to orchestrate the federal government's response to the epidemic of ransomware. And recognizing the need to bring together industry, government, and internal partners and tear down siloes that create gaps for the adversary, we established the Joint Cyber Defense Collaborative (JCDC)—a concept born out of the U.S. Cyberspace Solarium Commission on which one of us served as a Commissioner—to catalyze a community of experts on the front lines of cyber defense—from across the public and private sectors—to share insights and information in real time to understand threats and drive down risk to the nation.

Since its establishment, the JCDC led the national response to one of the most extensive software vulnerabilities discovered; played a central role in CISA's Shields Up campaign to protect critical infrastructure from potential Russian cyber-attacks; and, along with our partners at the Transportation Security Administration (TSA), brought together more than 25 major pipeline operators and industrial control systems partners to strengthen security practices to safeguard the operational technology networks critical to pipeline operations, efforts that complement the Security Directives TSA issued in the aftermath of the attack on Colonial Pipeline. Separately, with the support of Congress, we expanded our capability known as "CyberSentry" which enables heightened visibility into and more rapid detection of cyber threats that could target our nation's most critical operational technology networks. Finally, we worked to help organizations of all sizes and skill levels prioritize the most impactful cybersecurity investments with the introduction of cybersecurity performance goals, or CPGs.

While we should welcome this progress, much work remains to ensure the security and resilience of our critical infrastructure in light of complex threats and increasing geopolitical tension. The U.S. Intelligence Community issued a stark warning of a potential future in its recent Annual Assessment, noting that "If Beijing feared that a major conflict with the United States were imminent, it almost certainly would consider undertaking aggressive cyber operations against U.S. homeland critical infrastructure…China almost certainly is capable of launching cyber-attacks that could disrupt critical infrastructure services within the United States, including against oil and gas pipelines, and rail systems."

We cannot afford to dismiss this warning. We must do everything today to be prepared for such a scenario. First, we must ensure that the technology that underpins the services that Americans rely on every hour of every day is safe and secure. For too long, we have sacrificed security for features and speed to market, leaving us increasingly vulnerable, with the burden of security placed on those least able to bear it. As listed in one of the core pillars in the President's National Cyber Strategy we need security to be built into the creation of new technology—as a foundational imperative—rather than bolted on at the end requiring continuous security updates from consumers.

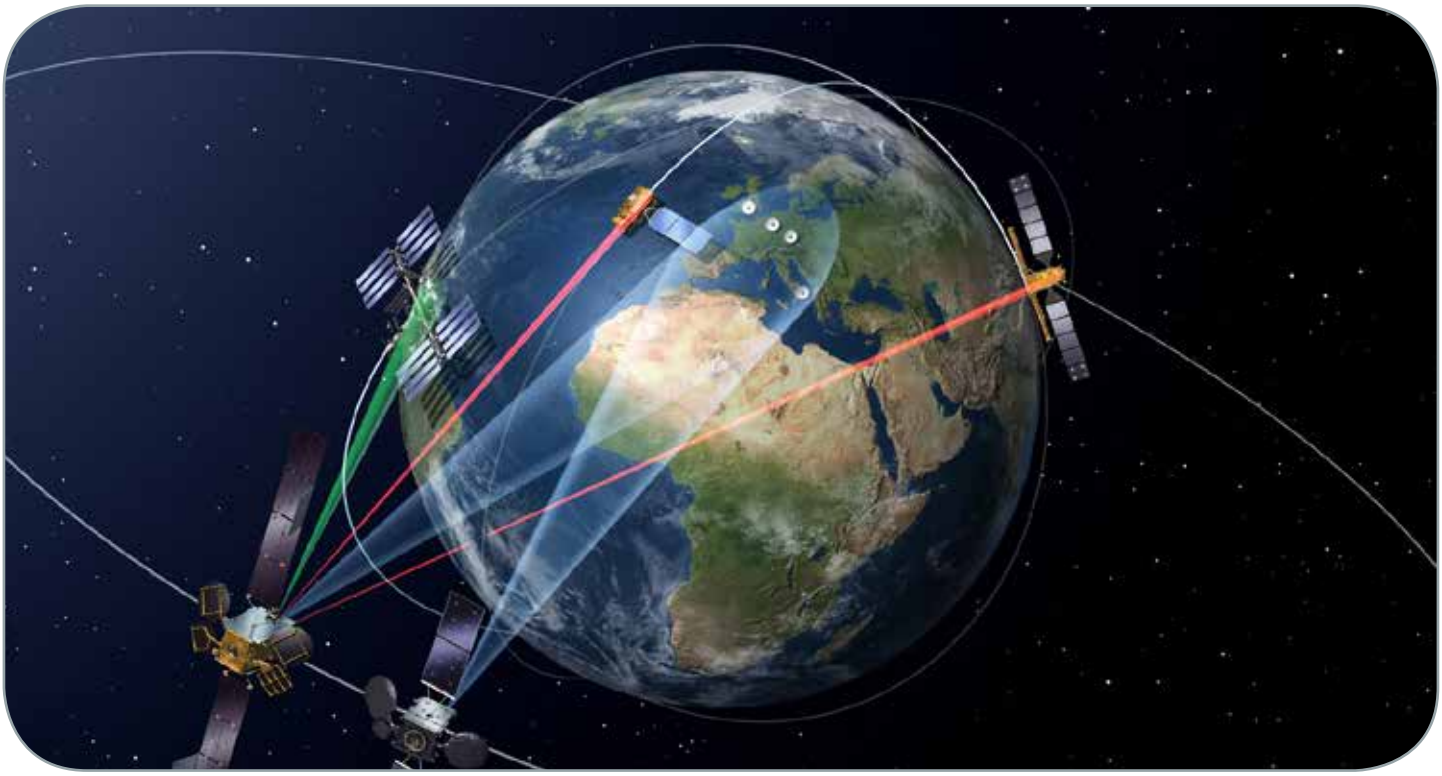
Second, we need to prioritize cybersecurity at the highest levels. The days of relegating cybersecurity to the CIO or the CISO must end. CEOs and Boards of Directors must embrace cyber risk as a matter of good governance and prioritize cybersecurity as a strategic imperative and business enabler.

Third, we must continue to invest in the JCDC model of persistent and proactive operational collaboration between government and industry where the default is to share information on malicious cyber activity, knowing that a threat to one is a threat to all.

Finally, we need to normalize cyber risks for the general public with the recognition that cyber-attacks are a reality for the foreseeable future. We cannot completely prevent attacks from happening, but we can minimize their impact by building resilience into our infrastructure and into our society. We need to look no further than our Ukrainian partners for an example of the power of societal resilience.

These changes are not easy, but we need to hold ourselves accountable to the hard lessons learned from two years ago. Are we going to make the choices that will lead us to a secure, resilient, and prosperous future or are we going to allow inaction to dictate a future in which our national security and our way of life hang in the balance? We have proven that it can be done but only if we act now…together.

An Interview with European Utilities Telecom Council (EUTC)



Ben Lane, CIPRE event manager, met with Julian Stafford, General Secretary of the European Utilities Telecom Council (EUTC).

A net-zero carbon future, end to fuel-poverty, sustainability, security and resilience are some of the major challenges facing utilities in the 2020s, all within strictly regulated industries. The high-level global challenges associated with mitigating climate change are driving very demanding obligations within the utility sector. As a result, the sector is going through a paradigm shift in the way that networks are controlled and monitored as their systems migrate towards an integral smart grid.

Julian Stafford, General Secretary of the European Utilities Telecom Council (EUTC).

All stakeholders are expanding and adapting their operational telecoms systems, using all sorts of technologies including wireless technology, and increasingly integrated into their operational processes in a shared network and services environment. This comes with a plethora of requirements and challenges, among others:

– growing and evolving rapidly to deploy massive numbers of devices

– ensuring cyber security and

resilience for more digitalised critical infrastructure

– operational flexibility to adapt to changing regulations and market needs

The European Utilities Telecom Council (EUTC) addresses these challenges by bringing industry experts together from across Europe, enabling them to share knowledge and stay up to date in this rapidly changing field. The EUTC works in partnership with the relevant stakeholders that actively seek its opinions in important issues such as spectrum allocation and development of the future energy grid. EUTC plays a significant part in shaping the future of standards development, technology ecosystem and key EU policies in order to allow the utility sector to procure cost effective, robust products and services for OT networks. This is achieved through interaction directly with the utility community, vendor supply chain and regulators at national and EU level.

Ben Lane: Can you provide a little bit about your background in this industry?

Julian Stafford: I began working in the electricity industry in Manchester, UK, in the early 1990s. I then migrated into the telecommunications division of that company, which ended up being owned by United Utilities, part of the water industry.

I worked on a whole range of systems, standardization projects, anything to do with mission-critical work. I worked with the nuclear industry, with the rail sector and the power sector, and gained extensive experience in rural broadband networks.

I then migrated and worked at Scottish Power as well in Cable and Wireless within the Vodafone Group. Then about 10 years ago, I became re-engaged with utility telecommunications and then got involved with the EUTC.

BL: Can you describe the EUTC and its work in bridging the commercial telecommunications providers and network operators with utilities in the energy and water industries.

JS: European Utilities Telecom Council represents the collective interests of water, electricity, and gas utilities, and it's been around for more than 20 years. We work on standardization, on knowledge sharing and best practice. We do a lot of consultation responses to energy regulators and telecommunication regulators around the world.

We have sister organisations in Rio, Johannesburg, Canada and Washington DC. We find ourselves touching on a lot of the cybersecurity elements of these networks because a critical national infrastructure is a potential way for bad actors to either exploit people through demanding payments in return for not screwing up their networks and in extreme cases it's a new form of warfare.

Governments throughout the developed world have recognised that cyber attacks on mission critical infrastructure such as utilities represent a new threat alongside physical warfare and terrorism . This is a new form of attack and one that is not following the traditional form that we may have seen in the past.

BL: Tell us about the impact of reducing our reliance on fossil fuels and how this impacts your work at EUTC?

JS: As a society we have got to reduce our reliance on fossil fuels, which means decarbonizing everything from electricity generation to transportation to heat.

As we move towards distributed

renewable energy resources such as solar and wind, battery storage and EVs, all the exciting sexy stuff now happens at the periphery of the network. That means we need real time monitoring control of all of those other devices, so millions of devices need checking. In essence, we have increased the attack surface from a cyber perspective by putting all this connectivity out to the periphery of the network. Therefore, we need to make sure the way this connectivity is safe from a cyber perspective.

Also, any system we put in place must have a very, very long-life lifespan. Twenty-five to 30 years isn't unusual for these types of system. We need interoperability between those systems as well, because historically utility telecoms networks have been typified by proprietary technologies local to just one country or even one company within one country. So, it has become a niche of a niche of a niche.

BL: What are the main challenges you are facing?

JS: Recent figures from the large research institutes indicate the amount of electrical energy distributed every day by 2040 will be between two and a half and four times the amount of energy that has to be distributed now. This

is because we are displacing all of those gigajoules that are delivered through petroleum, gas and oil at the moment and shifting them onto the electrical grid.

At the moment, the grids have a certain peak load and they cannot cope with that amount of additional energy. In order to do that without a smart network, you'd have to double or triple the size of the grid. So that would mean more pylons, more cables, more digging the roads up, more substations. The bill for this would be unthinkable. Across the EU the cost would probably run into a trillion Euros or more, and it would be mass disruption. So, how do we make sure we can use our existing assets in a more dynamic way?

The same applies in the gas sector where we're looking at pumping green or blue hydrogen into gas networks as an alternative to methane. But again, it requires more and more monitoring and control of all those points. Now of course, in the world of 5G and satellite communications and all the other things we hear about every day in the news, including artificial intelligence, one could be forgiven for thinking, "well, how hard can this be? Surely it already exists?"

The challenge we've got is that all of those products on offer and used by consumers are optimized for consumer use. They are "best effort" solutions.

Presently a mobile phone works very well and does a great job of providing consumer-based services. But how long does it work if there's a power outage? If you speak to any of the mobile operators and ask them to sign up to a contract that says, "yes, our network will work for three days in the event of a power failure," they won't be keen to sign up to that promise. But these are the obligations that the water, gas, and electricity companies have to adhere to.

They've got to make sure these things work. It's not an option to say, it's 99.9% available. It's got to be 99.9999 % because otherwise they will fail, and people will die in the same way as if aerospace systems fail or rail systems fail.

This is true in the energy sector to a certain extent; if there's a mass power outage there will be civil unrest, lack of energy to hospitals, healthcare, and big economic consequences, which is why we are working more and more with the blue light services.

BL: Can you give an indicator of what your role will be during the next five years and the challenges you will face.

JS: The speed of transition being set by Governments on decarbonizing a whole range of elements of the industry possibly leading to the outlawing of the sale of internal combustion engine vehicles, will mean a massive shift towards more and more electric or hybrid vehicles.

These are very positive ideas and concepts. It is the same discussion about moving away from gas fired central heating and towards heat pumps, which require more electricity.

However, at the highest Government level, I worry there are lots of very ambitious plans, but the building blocks in order to make those things a reality are missing. And we know this because there was a report from the renewable energy industry stating, we've got something like 15 or 20 gigawatts of additional renewable energy planned to meet the Government's climate change objectives but we can't connect them to the grid because the power companies are saying we haven't got the capacity to allow those things to be connected.

I will borrow an expression from one of the guys in Nokia who said, 'without digitalization there can be no decarbonization'. Digitalization is essential if the UK and Europe is to meet its climate change objectives.

We also have a significant amount of work to do in the cybersecurity space. So EUTC has got partners in the EE-ISAC group. They are a specific utility group that exists to share in a safe space information about cybersecurity vulnerabilities and solutions. This all gets fed into the European Union.

So, over the next five years, the work that I expect EUTC and our members to be involved with, among many other agenda issues, is the further standardization of smart grid requirements in terms of what is the technical specification for these things. How much do they need to cost and how can we standardize them across multiple territories?

In the utility space, as far as we are aware, there's only EUTC driving the future standards required to make 5G and 6G technology more fit for purpose, more optimized for utility use. So, we are really pleased to be involved with that. We will continue our lobbying and advocacy at the political level as well.

There's a huge amount for us to do going forward. We have many, many plates to keep spinning, but I think we are really fortunate to have 20 or so members in the EUTC from both the utility community and the vendor community that genuinely want to work together to improve the situation.

BL: Thank you, Julian, what a great introduction and one hopefully we can explore in more detail at CIPRE 2023, October 3-5, in Prague.

JS: Thank you.

For more information visit eutc.org

New Paper on Cyber-Physical Security in Critical Infrastructure

by Catherina Piana, Secretary General of the Confederation of European Security Servoces (CoESS)

The world's critical infrastructure is increasingly under attack and remains worrisomely vulnerable because of a failure to coordinate protection activities and a lack of persistent investment in security, explains a new report, Cyber-Physical Security and Critical Infrastructure. The report is a joint project of the Confederation of European Security Services (CoESS), the voice of Private Security in Europe, and the International Security Ligue, representing the world's leading security firms.

If the current conflict in Ukraine highlights cyber-attacks carried out in the context of war, it should be emphasized that they are also taking place in other regions experiencing tensions and latent conflicts, such as in the Middle East between Iran and Saudi Arabia. Everyone remembers the Stuxnet attack in 2010, but who knows that it had been active since 2009, and had already infected a dozen companies before attacking Iranian centrifuges? Stuxnet was different from any other virus or worm that had come before. Rather than simply hijacking targeted computers or stealing information from them, it escaped the digital realm to physically destroy equipment those computers controlled. Then, in response to Stuxnet, there was the attack on Saudi Aramco by Shamoon in 2012, which compromised 30,000

computers. Finally, from 2016 to 2018, there were numerous attacks on Saudi Critical Infrastructure networks and on government agencies. And similar examples can be found in all parts of the world.

Cyber-attacks are a strategic weapon of choice in conventional conflict and have been for a long time. They are a primary way in which States, organisations and individuals can harm other States, organisations, and individuals, whether in a public or private setting. And while

computers may be the targets of infection, human action has shown to be a constant factor in these attacks.

It should therefore be emphasized that protecting the access to information and systems is and will remain threedimensional, consisting of physical protection, the human factor, and digital protection. It has become clear that there is no point in trying to protect, let alone respond, to an attack with a siloed approach. Likewise, protecting organisations against threats in the digital world, particularly cyber-attacks, can only be done with a holistic approach.

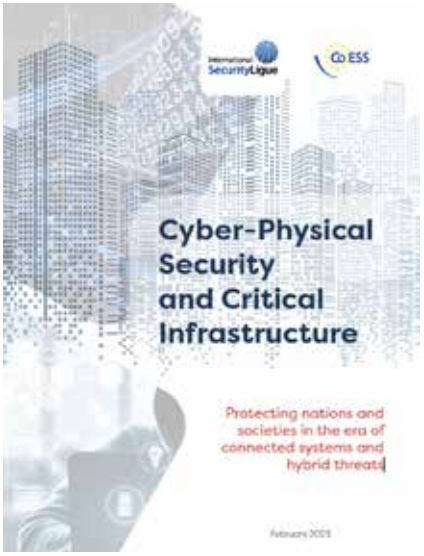
The consequences of cyber-attacks are also three-dimensional: IT infrastructures neutralized or destroyed; industrial production or services blocked or annihilated, with potentially serious industrial accidents; and finally, in human terms, injuries or deaths and job losses.

Whether through accident, negligence, or malicious intent, the human role is eminently present in the development and dissemination of cyber-attacks. As such, the human factor is a constant that must be fully integrated in a protection strategy capable of protecting against both an "involuntary vector" as well as a "malicious vector" (external or insider threat). It is because the human dimension cannot be dissociated from the defense strategy of organisations, that the notion of cyberphysical security has become essential.

Promoting the concept of cyber-physical security, the subject of this White Paper, represents a reasonable and critical response to today's threat. It was written by experts from across the globe under the aegis of the International Security Ligue and CoESS, joining forces to protect people, organisations and infrastructure against combined attacks that unfortunately will continue to be made.

Relevant for operators and owners of critical infrastructure, policymakers and regulators, and other stakeholders, the report details the oversight and management strategies required to protect nations and societies in the era of connected systems and hybrid threats. It summarizes challenges facing the world's critical infrastructure and includes deep dives on critical issues by leading security experts from around the world, on topics including integrated security governance, the role of legislation and regulation, unified penetration testing and risk assessment, and the role of public-private partnerships.

The report traces the escalation of risk to critical infrastructure, which multiply as legacy critical infrastructure systems are opened to communication and pushed to the cloud, providing attackers with new opportunities to compromise these high-value targets. Attacks on privately held, often unregulated



critical infrastructure operators pose critical risks for societies, and may occur as an outgrowth of geopolitical tensions, criminal enterprises holding systems hostage for ransom, or extremists of all sorts seeking to disrupt the status quo of societies.

The White Paper is divided into 2 main sections. Section I provides background and context on the fight to protect Critical Infrastructure (CI). It explores the meaning of CI, the ramifications of connected systems, the rise of physical-cyber threats, and explores security convergence to counter them. Section II examines specific physical-cyber security issues in greater detail, advancing guidance for devising comprehensive solutions co current and future challenges.

The report details the collaborations that are necessary to meet mounting threats: between government agencies and private businesses, public and private security, and among different departments at operators of critical infrastructure. An effective collective defense approach requires recognition that security is truly a shared responsibility between many stakeholders: physical

security, network security, operation and facility management, senior management, and others.

How to get the White Paper?

The joint Ligue-CoESS report on critical infrastructure security is freely available with the goal of helping to protect societies by enhancing the resilience of the world's critical systems. A link to the report is below and feel free to visit the CoESS and Ligue's websites to download this, or any of the organisations' available white papers, special reports, or infographics.

About CoESS: CoESS is the voice of the private security industry at EU level, covering 23 countries in Europe and representing 2 million security officers as well as over 45,000 companies. The private security services provide a wide range of services, both for private and public clients, ranging from Critical Infrastructure facilities to public spaces, supply chains and government facilities. CoESS is recognised by the European Commission as the only European employers' organisation representative of the private security services. Representing a labour-intensive sector, CoESS is actively involved in European Sectoral Social Dialogue and multiple EU Expert Groups related to land, maritime and aviation security, critical infrastructure the EU Operators Forum for the Protection of Public Spaces. www.coess.eu

About the International Security Ligue. Established in 1933, the International Security Ligue is represented in 120 countries by more than 2 million professionals. The Ligue provides a global voice for security profession and actively works to elevate ethical and professional standards for the private security industry and shape global codes of conduct. As a resource for members and the public, the Ligue provides an active forum to understand global trends, share best practices, and explore innovative ideas. www.security-ligue.

NATO and European Union launch task force on resilience of critical infrastructure

Senior officials from NATO and the European Union met to launch a new NATO-EU Task Force on Resilience of Critical Infrastructure. Cooperation to strengthen critical infrastructure has become even more important in light of the sabotage against the Nord Stream pipelines, and Russia's weaponisation of energy as part of its war of aggression against Ukraine.

First announced by NATO Secretary General Jens Stoltenberg and European Commission President Ursula von der Leyen in January, the initiative brings together officials from both organisations to share best practices, share situational awareness, and develop principles to improve resilience. The Task Force will begin by focusing on four sectors: energy, transport, digital infrastructure, and space.

Announcing the initiative in January, Mr Stoltenberg said: "We want to look together at how to make our critical infrastructure, technology and supply chains more resilient to potential threats, and to take action to mitigate potential vulnerabilities. This will be an important step in making our societies stronger and safer."

NATO-EU cooperation has reached unprecedented levels in recent years, and particularly since the start of Russia's war of aggression against Ukraine. In January, NATO and EU leaders signed a new joint declaration to take partnership between the organisations to a new level, including on emerging and disruptive technologies, space, and the security impact of climate change.

Standardisation of Cybersecurity for Artificial Intelligence

The European Union Agency for Cybersecurity (ENISA) publishes an assessment of standards for the cybersecurity of AI and issues recommendations to support the implementation of upcoming EU policies on Artificial Intelligence (AI).

This report focuses on the cybersecurity aspects of AI, which are integral to the European legal framework regulating AI, proposed by the European Commission last year dubbed as the "AI Act".

AI cybersecurity standards: what's the state of play?

As standards help mitigate risks, this study unveils existing general-purpose standards that are readily available for information security and quality management in the context of AI. In order to mitigate some of the cybersecurity risks affecting AI systems, further guidance could be developed to help the user community benefit from the existing standards on AI.

Further observations concern the extent to which the assessment of compliance with security requirements can be based on AI-specific horizontal standards; furthermore, the extent to which this assessment can be based on vertical/sector specific standards calls for attention.

Key recommendations include:

- Resorting to a standardised AI terminology for cybersecurity;
- Developing technical guidance on how existing standards related to the cybersecurity of software should be applied to AI;
- Reflecting on the inherent features of ML in AI. Risk mitigation in particular should be considered by associating hardware/software components to AI; reliable metrics; and testing procedures;
- Promoting the cooperation and coordination across standards organisations' technical committees on cybersecurity and AI so that potential cybersecurity concerns (e.g., on trustworthiness characteristics and data quality) can be addressed in a coherent manner.

Regulating AI: what is needed?

As for many other pieces of EU legislation, compliance with the draft AI Act will be supported by standards.

When it comes to compliance with the cybersecurity requirements set by the draft AI Act, additional aspects have been identified. For example, standards for conformity assessment, in particular related to tools and competences, may need to be further developed. Also, the interplay across different legislative initiatives needs to be further reflected in standardisation activities – an example of this is the proposal for a regulation on horizontal cybersecurity requirements for products with digital elements, referred to as the "Cyber Resilience Act".

Building on the report and other desk research as well as input received from experts, ENISA is currently examining the need for and the feasibility of an EU cybersecurity certification scheme on AI. ENISA is therefore engaging with a broad range of stakeholders including industry, ESOs and Member States, for the purpose of collecting data on AI cybersecurity requirements, data security in relation to AI, AI risk management and conformity assessment.

How Cybersecurity Standards Support the Evolving EU Legislative Landscape

ENISA joined forces with the European Standards Organisations (ESOs), CEN, CENELEC and ETSI, to organise their 7th annual conference.

The conference was organised around four panels, which discussed ongoing standardisation work and future requirements.

The first panel addressed the future of EU standardisation with the "regional versus international" angle. The second panel dealt with the Cyber Resilience Act (CRA) as a game changer and how standards can support it. The Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (or eIDAS) V2 and digital identities were the topics of the third panel, while the final panel gave an overview of the landscape of the EU cybersecurity legislation.

CISA - Building Cyber Hygiene Capacity in Thailand, the Philippines and Indonesia

In March, CISA conducted a series of first-of-their-kind capacity-building engagements overseas in Thailand, the Philippines, and Indonesia. The cyber hygiene workshops focused on highly interdependent sectors, including national defense, banking, business, aviation, and shipping sectors.

During the workshops, CISA cybersecurity and vulnerability management experts covered information technology/operational technology (IT/OT), industrial control systems, threat actors, threat intelligence, cyber-attack frameworks, workforce development tools, and case studies of common attacks. Major themes that emerged during the workshops included the need to develop greater cooperation between IT/OT; raise awareness of phishing and other attack vectors within organizations; and develop the public sector cybersecurity workforce.

To advance these longstanding strategic partnerships in Southeast Asia, CISA and the U.S. State Department worked closely with Thailand's National Cyber Security Agency (NCSA), the Philippine Department of Information and Communications Technology, and Indonesia's National Cyber and Crypto Agency. Indonesia is the largest member state in the Association of Southeast Asian Nations (ASEAN), which develops mutually beneficial dialogues, cooperation, and partnerships on behalf of its member states. Indonesia is also home to the ASEAN secretariat. Thailand and the Philippines are long-time treaty allies of the United States, and many major American financial firms rely on core business processing, such as call centers and back-office operations, outsourced to the Philippines.

CISA, FEMA and FCC Hold First National Meeting of State Alerting Officials

CISA, the Federal Emergency Management Agency (FEMA) Integrated Public Alert & Warning System (IPAWS), and the Federal Communications Commission (FCC) Public Safety and Homeland Security Bureau (PSHSB) held the first National Meeting of State Alerting Officials on April 25-26 in St. Louis, Missouri. This meeting brought together state, tribal, and territorial alerting officials (AOs) to share best practices, discuss challenges, and learn about the latest technology in alerting systems. This stakeholder driven meeting enabled CISA, FEMA IPAWS, and FCC PSHSB to strengthen partnerships and hear firsthand insights from the AO community and identify opportunities to support them as they carry out their critical missions.

The two-day event focused on fostering collaboration and improving communication between AOs, with the goal of enhancing the effectiveness of the emergency communications ecosystem. Participants learned about strategies for reaching all communities, identified, and addressed gaps in alerting plans, and discussed opportunities to enhance the effectiveness of the emergency communications ecosystem from an alerting perspective. By working together and sharing best practices, AOs can ensure that emergency messages are disseminated quickly and accurately, and that communities are better prepared to respond to emergencies and recover more quickly afterward.

U.S., U.K., Australia, Canada and New Zealand Release Cybersecurity Best Practices for Smart Cities

The U.S. Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC UK), the Australian Cyber Security Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC NZ) released a joint guide: Cybersecurity Best Practices for Smart Cities.

Integrating public services into a connected environment can increase the efficiency and resilience of the infrastructure that supports day-to-day life in our communities. However, communities considering becoming "smart cities" should thoroughly assess and mitigate the cybersecurity risk that comes with this integration. This guide is intended to help communities navigate through this complex and important work.

Reimagining Gunshot Detection for Enhanced Community Safety

New portable system employs two methods of detection for increased accuracy and reduced false positives..

New and improved gunshot detection technology will soon make American communities of all sizes safer. The Science and Technology Directorate (S&T) and its industry partner Shooter Detection Systems (SDS) developed SDS Outdoor, a gunshot detection system that builds on existing SDS technology to deliver new capabilities that significantly improve the response and management of outdoor shootings.

Among these new capabilities are portability and ease of system set up at any location, two-source detection—sound and flash—to confirm a gunshot, real-time alerts that provide near-instant situational awareness to law enforcement and emergency medical responders, and enhanced data recording that aids apprehension and conviction of alleged shooters.

Portability allows the system to be set up practically anywhere, including near outdoor events, and a single person can install it. Additionally, the enhanced system tells law enforcement when and where a gunshot originates, cutting response times dramatically and providing police officers actionable information—for example, data that helps them to determine if there is a single shooter or multiple shooters. Agencies can then use that information to coordinate resource response and counter an active threat.

"It takes about two to three minutes for an individual to call 911 after a gunshot. Gunshot detection technology cuts that time in half and sends a notification to local law enforcement. Police could then dispatch a unit quicker to either stop the incident that's occurring or to assist in preventing any lives being taken," said Wilhelm Thomas, officer with the New York Police Department's (NYPD).

Axis Communications and Genetec Introduce New Game-Changing Access Control Solution

With access control as a cornerstone of physical security, and today's businesses requiring more advanced tools, Axis Communications and Genetec Inc.—leaders in network technologies for security, operations and business intelligence—have partnered to introduce an industry-first, enterprise-level access control solution.

Axis Powered by Genetec combines Axis network door controllers and Genetec access control software into an all-in-one solution that offers easy deployment, maintenance and scalability along with enhanced cybersecurity for end users and system integrators alike.

By unifying Axis's next-generation AXIS A1210 and A1610 Network Door Controllers with Genetec's powerful IP-based SynergisTM access control software, customers not only benefit from reduced installation time and hardware costs. They also attain enterprise-level control features, immediate access to hardware and software enhancements, and cybersecurity updates from both Axis and Genetec directly through Genetec Synergis. This new architecture unites the new door controllers seamlessly with Synergis via AXIS Camera Application Platform (ACAP) to enable real-time monitoring of events and alarms, advanced cardholder and access management and comprehensive reporting.

Fredrik Nilsson, VP, Americas, Axis Communications, said, "We recently introduced unified video management and access control for small to medium businesses with AXIS Camera Station Secure Entry. Now, with our valued long-time partner Genetec, we're proud to launch a powerful enterprise-grade solution that integrates our door controllers with Genetec's best-in-class access control software."

LenelS2 Recognized for Cybersecurity Achievements

LenelS2, a global leader in advanced security systems and services, has achieved three key accomplishments demonstrating its commitment to cybersecurity.

The company has attained compliance with the NIST SP 800-53 cybersecurity standard, had its Elements™ cloud-based solution accepted into the Cloud Security Alliance's (CSA) Security, Trust, Assurance, and Risk (STAR) Level 1 Registry, and has been selected as a winner of the Global InfoSec Award by Cyber Defense Magazine. LenelS2 is a part of Carrier Global Corporation (NYSE: CARR), global leader in intelligent climate and energy solutions.

LenelS2 has earned independent verification of compliance with the NIST SP 800-53 standard for its OnGuard®, NetBox™, and Elements™ access control platforms. The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies and the broader public. NIST Special Publication 800-53 ("NIST SP 800-53") provides a catalog of security and privacy controls for organizations to protect organizational operations and assets, individuals, and other organizations from a diverse set of threats and risks.

Additionally, LenelS2's Elements cloud-based access control solution was accepted into the Cloud Security Alliance's (CSA) Security, Trust, Assurance and Risk (STAR) Level 1 Registry, which provides increased transparency around the company's security and compliance posture and security controls it has in place.

"LenelS2 is committed to staying at the forefront of cybersecurity, and we're constantly working to ensure our products and services are as secure as possible," said John Deskurakis, Chief Product Security Officer, Carrier. "Cybersecurity is not just a feature or update, but a fundamental requirement for the industry. That's why we're continually obtaining new certifications and implementing best practices across our portfolio."

XProtect® 2023 R1 release brings user experience, collaboration, and pre-check efficiencies

Milestone Systems advances its enterprise-level video technology with the latest product update, XProtect 2023 R1. This update enhances previous XProtect VMS innovations to provide an easy-to-use, integrated, and powerful user experience.

The R1 update for XProtect improves upon the core needs of Video Management Software (VMS) users, providing reliable, powerful, and easy-to-manage open platform solutions that offer flexibility and security to meet all integrated data-driven video management requirements. With several enhancements to the user experience and system performance, including operator collaboration tools and installation pre-check efficiencies, the 2023 R1 update is a highly recommended software upgrade for all XProtect users.

The 2023 R1 software update offers significant enrichments to the user experience, operator collaboration, and situational awareness. The user experience now includes UX renewals in both the Smart Client and Web Client interfaces. With a modern, intuitive interface and better navigation, users can easily access and manage their video data with greater ease and efficiency. Operator collaboration tools have been significantly enhanced through features such as Bookmarks Sharing, Background Picture in Picture, and Native Screenshots in the Mobile Clients. These tools improve operator efficiency and communication, enabling operators to easily share bookmarks and collaborate on video data analysis. Furthermore, 2023 R1 includes more situational awareness capabilities with Smart Maps in the Mobile clients. This feature provides operators with a map-based overview of cameras and devices, enabling faster response times.

ADVERTISING SALES

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

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

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

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

SAVE THE DATES

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

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

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

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

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

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

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

www.world-border-congress.com

for the international border management and security industry

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

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

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

Supported by:

Media Partners: