WORLD SECURITY REPORT

Official Magazine of

International Association of CIP Professionals
www.cip-association.org

SEPTEMBER / OCTOBER 2019
www.worldsecurity-index.com

FEATURE:
6 Days That Shook America - Event Security, Are We Doing Enough?
PAGE 9

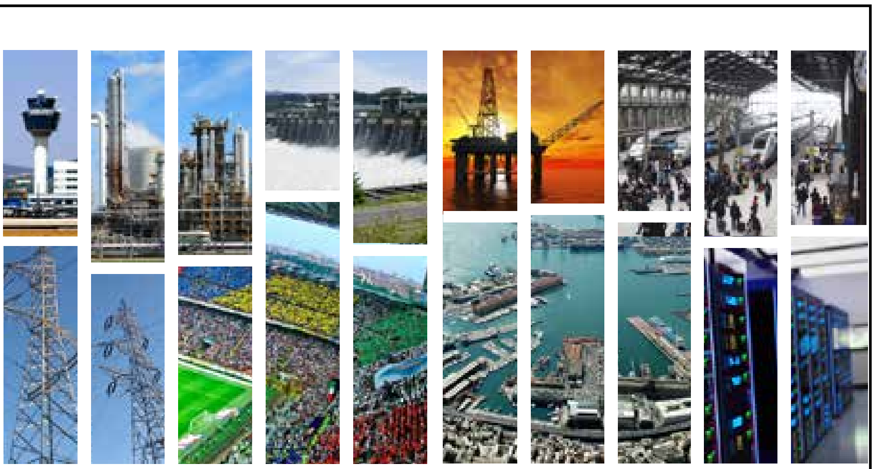
FEATURE:
Assessing Modern Threats and Vulnerabilities in the Sports Landscape
PAGE 20

FEATURE:
Why should Critical Infrastructure companies invest in electronic locking system to protect their operations?
PAGE 26

HUMANITARIAN RESPONSE; LESSONS FROM HURRICANE IRMA

critical infrastructure
PROTECTION AND RESILIENCE EUROPE

www.cipre-expo.com



14th-16th Oct 2019 | Milan Italy

Co-Organised by:

International Association of CIP Professionals

Regione Lombardia

REGISTRATION OPEN

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

Early Bird Deadeline - 14th September - register today!

Keynote Speakers include:

- Italian Critical Infrastructures Secretariat - Presidency of the Council of Ministers
- Roberto Baldoni, Deputy Director of the Department for Security Information (DIS), Italian Cybersecurity Agency
- Fernando J. Sánchez Gómez, Director, Centro Nacional de Protección de Infraestructuras y Ciberseguridad (CNPIC), Spain
- Brian Harrell, Assistant Director, Cybersecurity & Infrastructure Security Agency, DHS, USA

Italy faces some of the most challenging natural threats in Europe.

In western Europe, the region with the highest seismic hazard is the mountainous backbone of Italy, the Apennines. It has a long record of earthquakes spanning back to Roman times.

But recent earthquakes have been some of the most dramatic. In August 2016 there was a 6.2-magnitude earthquake near Amatrice that killed more than 250 people. That was followed by a 6.1 earthquake, which struck Visso on 26 October. Four days later, the village of Arquata del Tronto was destroyed by a 6.6 earthquake. Scientists predict that more earthquakes are highly likely.

In southern Italy the highly populated city of Naples is located near Vesuvius and within the larger caldera volcano Campi Flegrei, and some scientists are warning that Campi Flegrei is showing signs of activity that could mean that an eruption. This is on top of the active stratovolcano of Mont Etna on the island of Sicily.

In October 2018 severe storms caused widespread and severe flooding across Italy causing numerous casualties.

In addition to natural threats Italy along with Greece has borne the brunt of mass migration into Europe, which places stress on and poses security threats to its critical national infrastructure.

Milan is an ideal location for Critical Infrastructure Protection & Resilience Europe because it is the regional capital of Lombardy, one of Italy's greatest cities, and its industrial and financial powerhouse.

We look forward to welcoming you on 14th-16th October 2019.

Discover more and register your place at www.cipre-expo.com.

Confirmed Speakers include:

– Dr. Christopher Rodriguez, Director of Homeland Security and Emergency Management for the City of Washington DC, USA

– Georg Peter, Head of Unit Technology Innovation in Security, Joint Research Centre, European Commission

- Andrew Palmer, Border Security Manager, Gatwick Airport, UK

– Prof. Paolo Trucco, PhD Full Professor – Risk and Resilience Management of Complex Systems research group Politecnico di Milano – School of Management

– Vittorio Rosato, Head Laboratory of analysis and protection of critical infrastructure, ENEA, Italy

– Luca Boselli, Partner, KPMG Advisory S.p.A., Italy

– Alessandro Lazari, Regional Director for Mediterranean, International Association of CIP Professionals

– Sandro Bologna, Board Member, Italian Association of Critical Infrastructures' Experts (AIIC)

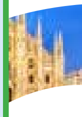
– Cevn Vibert, Global Director Industrial Cyber, Vibert Solutions

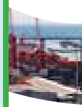
– Dr Ugo Finardi, Researcher, CNR-IRCrES National Research Council of Italy, Research Institute on Sustainable Economic Growth

– John Donlon, Chairman, International Association of CIP Professionals

– Dr. Serkan Girgin, Scientific Officer, European Commission Joint Research Centre (JRC)

– Alexandru Georgescu, Researcher, ROMSPACE – Romanian Association for Space Technology and Industry





Leading the debate for securing Europe's critical infrastructure

Platinum Sponsor: KPMG

Bronze Sponsor: ABLOY

Supporting Organisations: AIIC, NS&RC, ISIO, IET The Institution of Engineering and Technology, ECRRN European Cyber Resilience Research Network, CoESS, SPF, IET.tv

CONTENTS

WORLD SECURITY REPORT

» p.5

» p.9

» p.24

» p.16

COULD THERE BE A RETURN TO THE 'TROUBLES'?

The border between the UK and Ireland is one of the most contentious in the world. For much of the 30 years of the so called 'Troubles' much of the border region was a no-go area for the Royal Ulster Constabulary (RUC) and all other agencies of law and order. This meant that the borders were actually patrolled by the British army instead.

A lesser known fact about that period is that the IRA commanders in areas like South Armagh operated much like mafia bosses in 1920's America.

The difference in the economies between the UK and the Republic of Ireland meant that smuggling of anything, from fuel to washing powder was big business and made those in the higher echelons of the IRA wealthy men.

Whilst clearly these 'commanders' would have done their time in IRA active service units, as time went on the business of smuggling and making money became a primary motivation.

It was in their interest that border regions were no-go areas to border guards, customs and police.

Whilst the army would of course routinely stop vehicles in fixed and pop-up vehicle check points, soldiers generally make poor customs officials. They are checking for weapons and bad people, not inventories.

So, IRA commanders sent out young volunteers to do the dirty work of shootings and bombings, whilst they got on with the business of smuggling and reaped the financial rewards.

There was of course no shortage of young volunteers. They could see the 'big men' driving around in nice Mercedes when everyone else in the area struggled for a decent living, and bathing in admiration (or fear) whilst dispensing largesse in places like the Three Steps Pub. Fired up by patriotism, righteous indignation and youthful testosterone they were only too willing to fight for 'the cause', prove themselves and maybe one day be one of the 'big men' and a commander themselves, if they lived long enough.

If we do end up with a hard border, it will play into the hands, not just of staunch republicans' radicals just waiting for an excuse but also criminal elements for which a return to the Troubles is a business opportunity too good to miss.

Tony Kingham
Editor

READ THE FULL VERSION

The full version of World Security Report is available as a digital download at www.torchmarketing.co.uk/WSR

www.worldsecurity-index.com

Editorial:
Tony Kingham
E: tony.kingham@knmmedia.com

Assistant Editor:
Neil Walker
E: neilw@torchmarketing.co.uk

Features Editor:
Karen Kingham
E: karen.kingham@knmmedia.com

Design, Marketing & Production:
Neil Walker
E: neilw@torchmarketing.co.uk

Subscriptions:
Tony Kingham
E: tony.kingham@knmmedia.com

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 130,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, armed and security forces and civilian services and looks at how they are dealing with them. It is a prime source of online information and analysis on security, counter-terrorism, international affairs, warfare and defence.

Humanitarian response; Lessons from Hurricane Irma

Winds of more than 180mph had laid waste to their paradise home, but a lack of communication quickly brought a fresh security maelstrom for devastated Caribbean communities following Hurricane Irma in September 2017.

The first responders to arrive in the British Virgin Islands following the Category 5 storm which had killed five, found a dystopian environment where human activity was in just as much turmoil as nature.

Ocean going yachts lay beached inland; cars wallowed in the harbours; and the remains of light aircraft and helicopters hung upside in trees and bushes stripped of every scrap of greenery, while communities struggled to come to terms with having had their lives turned upside down.

There was no mains electricity, no clean water and no regular communications system.

It has long been understood that managing disasters requires effective communications in order to coordinate rescues, sustain order and start to bring in the food, water and shelter needed for recovery, but the more we all become accustomed to instant communications and effortless data transfer in our day-to-day lives, the more any population is going to feel lost without it.

Lack of communications is going to mean any disaster response is delayed and limited, and so it was after Irma.

Instincts for security, however, usually survive.

Volunteers from the British humanitarian response charity Serve On who arrived at Beef Island, Tortola, found the airport in chaos with aircraft hangars reduced to twisted metal, perimeter fences down and the airport buildings trashed, and yet uniformed immigration staff were still trying

to process fleeing islanders and the new arrivals with little means of communicating with government colleagues to check the bona fides of the incoming or outgoing passengers.

Mindful of the importance of customs and immigration controls for an island community, the charity workers simply set to work to re-secure the airport fences and clear the wrecked furniture from the arrival and departure lounges to prepare the way for outgoing locals and incoming aid while they waited for the official approval to enter the islands.

Gaining situational awareness for everyone concerned was especially difficult without communications, and many of the far flung communities on Tortola were cut-off not only by downed telephone lines and radio masts but by roads that had been blocked or washed away.

The first task of the volunteers from Salisbury, Wiltshire, UK therefore, was to access isolated communities, to assess their needs and to communicate the information back to the authorities in Road Town.

They cleared roads, visited numerous hurricane shelters and the communities that had used them, and carried out a full range of assessments.

There was another security problem brewing, however.

In the absence of reliable communications, unreliable communications run wild.

To the stories of lootings and shootings circulating on the bush telegraph, were added rumours that scores of dangerous criminals were on the loose.

The prison in Road Town had indeed been emptied as Irma approached, for the safety of the inmates who would have been in danger of drowning in their cells when the hurricane hit.

Now there were tales of all kinds of murderers and robbers at large.

In fact a tiny minority of dangerous criminals, once freed, were thought to have escaped the islands altogether. The vast majority of inmates had simply gone home as instructed and reported back to the prison when they were meant to. The remainder were quickly and easily rounded up by Royal Marines sent to help maintain law and order.

Curfews were generally well respected, but that didn't mean there was not opportunistic pilfering. Plenty of damaged shops had their goods 're-distributed', and the power of the hurricane had seemingly not only been enough to toss vehicles far and wide but had also emptied all of their fuel tanks!

Wild rumours did not just concern the prison.

There was talk that British police who had already been present on the island to mentor the locals had in fact been there to take over policing of the islands; that the government had been about to be replaced; that there was an escalating problem with high-end corruption and international drug smuggling; that relations between the local communities and the police were at breaking point.

Had any of it been true? Had Hurricane Irma pre-empted any take-over of the British overseas territory that had been due to happen? The lack of communications meant no answers were available and the rumour mill had free rein, adding to insecurity.

On Virgin Gorda, where the Serve On volunteers were among the first outside responders to arrive, the lack of publicly available telephones meant use was made where possible of maritime radio, but it was not secure.

At least that meant the local recovery group was able to listen in to some elements planning a robbery, though the would-be raiders were also able to listen in on the posse which headed off to stop them, so nothing happened.

Sourcing the food and water and medicines needed for the devastated communities on the island, however, remained difficult without proper communications and there was the additional problem, when boat loads of supplies were sourced, of keeping the news off the grapevine in case they sparked unrest among desperate residents when they arrived.

Discovering information on which vulnerable islanders had what medical or other needs, without physically driving to find them, was also complicated by the fact that all computerised data sources were unavailable.

For the charity volunteers, the value of liaising with the UK military and UN entities, via their satellite communications, was highlighted. The small deployment of Royal Marines, with a Royal Navy medic, who arrived on Virgin Gorda were the model for effective stabilisation.

They had all deployed previously, and had recent experience of Afghanistan, and, along with British policemen, were expertly able to de-escalate any potential trouble, provide calm reassurance along with necessary security.

Looming over all the recovery work was the prospect of Category 5 Hurricane Maria hitting the already devastated islands within days.

There was a varied amount of support from very wealthy islanders, most of who had their own security teams.

A noteable few very high-profile residents sent their security officers and very talented staff to assist at every opportunity, liaising and collaborating with the local recovery group and putting assets such as light aircraft and helicopters at the disposal of the recovery effort.

Others were interested principally in guarding their assets from the local population.

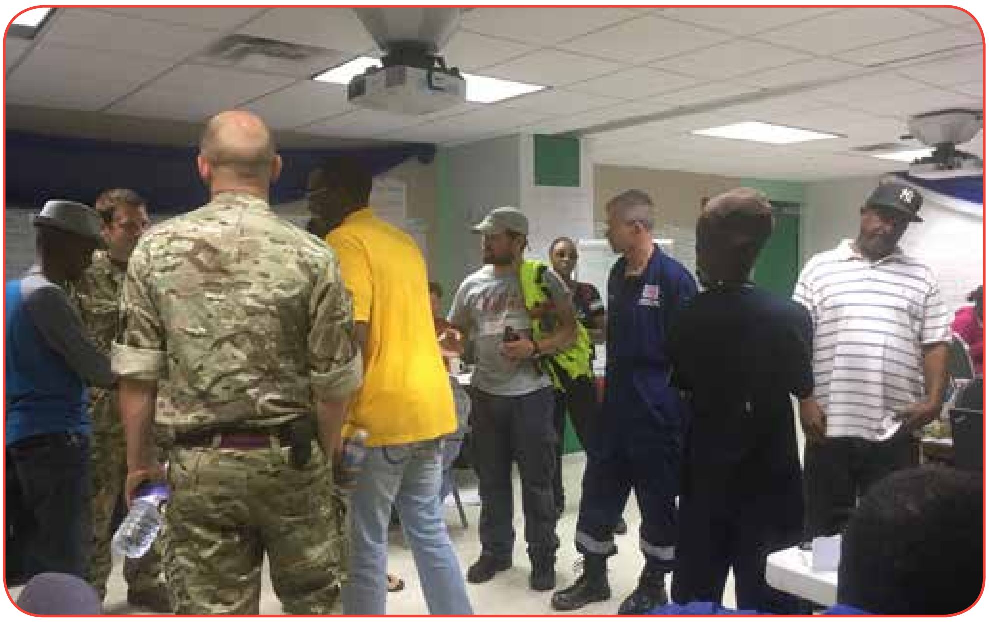
The Serve On volunteers, meanwhile, as well as carrying out assessments across Virgin Gorda, and providing thousands of litres of clean drinking water with their portable water filtration system to compensate for the destroyed local desalination plants, helped to instigate an incident command system (ICS) to aid the local recovery group.

Serve On Operations Director Dan Cooke said: “One of the most successful aspects of our deployment was being able to help rally the local community to create highly-motivated teams to get urgent tasks completed.

“It’s not the first consideration of a search and rescue team, but it was a responsibility to help that we took very seriously,” he said.

Establishing communications was vital, not just to organising necessary water, food and shelter, but also to engaging the community, keeping them informed, and thus smoothing age-old tensions between the ‘belongers’, the ‘non-belongers’, the ‘down islanders’ and other factions on the island which, in a communications void, could have quickly deteriorated.

Indeed, the work of the local recovery team was so successful that they reached a tipping point where they felt the island was being more efficiently run after the



hurricane than it had been before and Serve On were involved in the delicate negotiations for a hand-back of control to the government.

"For every aspect of the recovery, the provision of communications was essential," said Cooke.

That is why Serve On experts are now hoping to return to Virgin Gorda to install emergency communications equipment to give islanders a life-line in the event of future hurricanes.

Volunteers from the charity, which was set up to give military veterans and emergency services personnel renewed purpose in life in highly-trained rescue teams, helped to cut a path through dense vegetation to the top of Mount Gorda before they left two years ago, ready to site a future radio repeater station.

Now they have sourced and tested the equipment needed to install a portable digital VHF repeater and an FM broadcast system that can be taken down if islanders get warning of another killer storm.

The off-grid, solar-powered equipment can then be put back in place once any hurricane has passed, so that vital communications can quickly be restored.

The FM broadcast system will enable a radio station – VG Rock, based in the island's capital, Spanish Town - to give islanders important weather and safety information, and public address messages, before and after a hurricane.

The digital VHF repeater station will link 70 VHF radios located around the island at hurricane shelters and elsewhere. It will mean that people can communicate soon after a storm has subsided, assisting emergency services and recovery teams.

All of the kit has been built and tested in the UK and is ready to be flown to the British Virgin Islands where the Serve On team aim to install it and train locals how to use it. They just need to find the funding to be able to do so.

Serve On Operations Manager Craig Elsdon said; "It will be good to return to Virgin Gorda to see the community back on its feet. It will be very different from when we last saw them two years ago in the aftermath of Hurricane Irma.

"We hope they never have to go through anything like that again but it is hurricane season again right now and we want to help them to be prepared this year and in future years.

"We have worked with a lot of people to get this project ready in order to enable a very resilient community to look after itself if the worst happens. I know every penny we can raise to make this happen will be massively appreciated by the wonderful people there."

*Martin Phillips is a member of the Serve On International Response Team.

www.serveon.org.uk

https://gogetfunding.com/emergency-radio-project/

6 Days That Shook America - Event Security, Are We Doing Enough?

Spanning six days and occurring over 2,000 miles apart, the recent actions of individuals at two separate events both shocked and stunned social media and the world. The attacks had vastly different impacts on the lives of those involved in them and the question needs to be asked: When it comes to event security, are we doing enough?

On Sunday July 28th, lone gunman Santino William Legan breached the perimeter fence at Gilroy Garlic Festival, held annually in California's central coast. With ultimate bravery and dedication to their badge and the public, officers of Gilroy Police Force were able to stop him within 60 seconds of him opening fire. Tragically, three lives were lost within that minute, (including two children), with over a dozen more injured.

As people all around the globe reeled from this attack, another group of individuals were planning to attack a popular music festival in Chicago- This time with different intentions. Described as a pack, probing the perimeter security of Lollapalooza Festival, upwards of 50 people tore down and jumped over the Temporary Event Security Fencing placed around Grant Park. Videos surfaced across social media channels showing the scale of the problem that the organizers and volunteers had to deal with to uphold Event Security.

Ask yourself this question: What would you do if 50 people came running at you only 6 days after a shooting at a festival? Can you imagine the fear and need to 'flight' away from this? While the aims of the attackers at these festivals were different, Please join us in discussing...

ACCELERATING SECURE TRADE AT PORTS & BORDERS

New Tech, Better Detection, More Trade

November 13, 2019 • Webinar Hosted by World Border Security

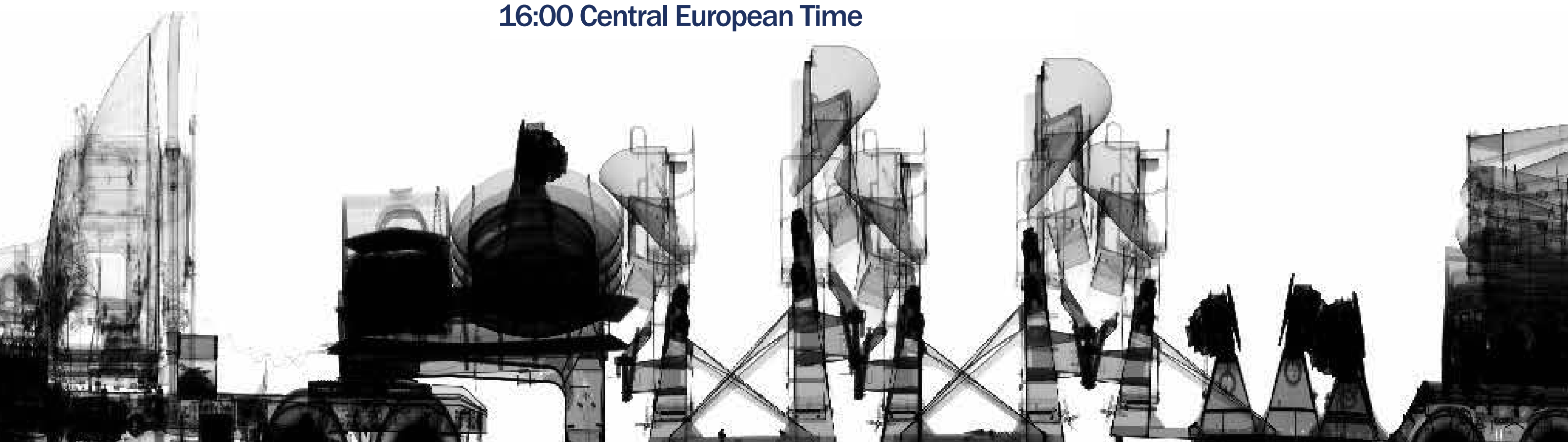
S2 GLOBAL
An OSI Systems Company

Further details and to Register at www.border-security-report.com/S2-webinar

Upgrading inspection capabilities by integrating systems allows ports and borders to create fast entry lanes that are capable of 100% inspection.

During this webinar, representatives working with US CBP, international Customs agencies, global port operators, trade executives and defense leaders will discuss initiatives that enable data sharing between agencies and facilitate more inspection, better detection, faster Customs clearances and increased trade.

November 13, 2019
10:00 Eastern Time Zone (US)
16:00 Central European Time



one designed to maim and kill and the others aiming to get free entry to a festival; the route of attack was the same.

In both cases, the route of entry was not via organized access control zones with metal detectors, armed officers; chicane and HVM deployed systems. Access was gained by either going over or through Temporary Chain Link Event Security Fence Panels. Looking on a USA suppliers' website typical purchase price for these at 6-foot-high is around $16.40 per foot. These types of event security fencing systems are used across the United States of America to demark the physical boundaries of events and festivals. In effect to keep control of the location and assets, be them people or physical.

Chain Link is considered in the American marketplace as a temporary security fence; in general, most people expect it to withstand an attack. Back in the early 2010's CLD Fencing Systems held a closed-door live security event at BRE Global (Watford, England). Security consultants from across the United Kingdom attended to watch various types of fencing systems attacked and to demonstrate the security standard LPS 1175; which offers a guaranteed delay against attack. In never seen before footage in the public arena, the following video shows an attack on chain link fencing using a standard set of pliers (wire cutters) ...

...a full breach of the Chain Link Fencing occurred within 20 seconds. Less time than it takes to make a coffee. In early 2018, High Tensile Chain Link Fencing Panels were attacked again by the LPCB Testing team at another closed-door event in the Middle East. Penetration of the fence line occurred at 24.07 seconds.

This information isn't new. while it may shock many people hearing this for the first time; for years security advisers have been talking of the dangers of these types of event security fencing systems. The problem, until recently, was that there wasn't a solution on the marketplace that was able to offer something more secure at around the same price.

Chain Link can be scaled with ease, and the use of braces means that with enough people the whole fence can be pulled down, as seen in Chicago. Likewise, heights of 6 feet tall means that the top bar of the event security fencing becomes an easy hand hold to pull yourself up and over. Furthermore, many hostile security topping systems, such as barbed wire or razor coil, are considered unsuitable for crowded places. This continues to persuade event security that they have no other option than what is currently available across the States to stop scaling.

However, is that enough? Are event security set up teams looking at the latest products?

• Are they reviewing security standards such as LPS 1175 and seeing what is available to them?

• Do their physical perimeter systems work as they should and when were they last reviewed against modern methods of attack?

• Can they use PIDs (Perimeter Intrusion Detection Systems) and if so, how do these integrate with the fencing?

• Have non hostile security toppings been explored?

It is always worth remembering that any form of Temporary Event Security Fencing will not stop an attacker. However, they can delay them long enough to allow a response. In Gilroy the response time was 60 seconds; if you can detect and delay for that amount of time, the next event may be able to stop them before they even gain entry to the site.

The Role of AI in Physical Security for Critical Infrastructure

Security infrastructures are undergoing a digital transformation with increasing adoption of intelligent access control, video surveillance and analytics as well as IoT devices and sensors – generating more data than ever before. For critical infrastructure, properly harnessing the influx of data with artificial intelligence (AI) and a risk-based approach, the data can be leveraged to improve life safety, minimize risk and speed response times in emergency situations.

Whether you're protecting cities, nuclear facilities, airports, hospitals, or any other critical infrastructures, or just trying to keep risk at bay, it's time to make security smarter. The technology is here now and ready to integrate with your critical systems, data and assets to protect what matters most.

Let's explore what exactly AI is and how it works to analyze risk, deliver actionable intelligence and adapt security to lessen the impact of threats and breaches. AI simulates the human intelligence process – it acquires information and learns; it identifies patterns; and, it reacts based on those understood patterns. One of the core components this learning process is an Artificial Neural Network (ANN). Similar to the human brain, the ANN works with thousands of sensors.

Our human sensors are eyes, ears, nose, skin – identifying what our environment includes – people, things, temperature, light or darkness, moisture, sounds and many other things. As those sensors activate, we learn. Our internal variables adjust and we identify patterns and react accordingly. For example, if we smell smoke, we know there is fire and our brain sends signals to the body to take appropriate action to escape danger.

The artificial neural net (ANN) sensors are cameras, sensors, access control devices, IoT devices, big data, social media plug-ins and human input. As those sensors feed internal variables, the ANN learns and identifies patterns of risk providing real-time situational awareness to the humans.

Today, we are flooded with data. AI can constantly evaluate large amounts of data to identify threats we might not otherwise see. This fundamentally changes the game in physical security and will impact all traditional components of a layered solution.

A security system armed with AI can dramatically improve how you protect your environment. The biggest advantage it delivers is proactive protection. It can give early warnings of a threat based on analysis of all the integrated data helping to avert a risky situation from escalating to the point of loss or damage.

The AI-assisted security system can see what humans may miss – especially when it comes to costly internal and advanced threats. Your security team might think a user is authorized to access an area, but under certain circumstances or a series of suspicious events, an AI security system identifies when the employee could potentially pose a risk with ill intent. AI leverages the data inputs from across the environment to "see and hear" everything, from everywhere, at all times. This leaves no gaps, no missed opportunities.

AI can integrate, analyze and notify security teams giving them the edge needed when seconds count most. While your security team can't be expected to know in great detail everything that's going on at all times, an AI security system does – human limitations are no longer constraints to your security operation.

When it comes to protecting critical infrastructure, here are a few examples where AI can help to significantly enhance security and life safety:

Go from Video Analytics to Intelligence

While analytics are fairly new to physical security, the dependence upon video is not. Yet only recently did we learn to leverage mass amounts of video feed into intelligence through the use of analytics. It should come as no surprise then to learn that there is a large chunk of data being ignored: context.

Video analytics are advancing at accelerating rates, including facial recognition and sentiment analysis. However, this is not the only analysis needed. These video data feeds need a brain – an artificial neural network (ANN) – to provide context for the video data and to properly detect risk. Video cameras need central intelligence with memory that can process multiple sensors to make sense of the view.

Traditionally, SOC operators are presented with hundreds, possibly thousands, of cameras to monitor. Studies show that human attention spans are limited in their ability to effectively monitor video and identify every potential threat. However, when video is a component in an AI-based solution, the attention span is limitless. AI never gets bored or distracted. AI can sift through the mundane and assist the human in identifying threats as they are growing.

With AI for risk analytics, operators are no longer forced to monitor and analyze everything simultaneously. Risk intelligence can detect early warnings across multiple data systems, compare it to policy, and determine the level of threat – all before a security breach occurs.

Make Access Control Risk-Adaptive and Dynamic vs. Role-Based and Static

No physical security solutions have benefitted more from AI than physical access control systems. When integrated with an AI-based solution, an access control system can now react to threats reaching unacceptable levels of risk and adjust access permissions accordingly. Risk-adaptive access control in a physical security environment is new. Providing the ability to identify anomalous events, insider threats, hazardous

Organised by:

CyberSecurity MALAYSIA

Endorsed by:

MINISTRY OF COMMUNICATIONS AND MULTIMEDIA MALAYSIA

Supported by:

CHIEF GOVERNMENT SECURITY OFFICE

NACSA

MDEC

csm-ace 2019

11th CYBER SECURITY MALAYSIA AWARDS, CONFERENCE & EXHIBITION

Cyber Security Malaysia Awards, Conference & Exhibition (CSM-ACE) is a prestigious cyber security event organized by CyberSecurity Malaysia endorsed by the Ministry of Communications and Multimedia (KKMM).

23 - 27 September 2019 | Royale Chulan, Kuala Lumpur

#cyberdefence

THE BIGGEST CYBER SECURITY INDUSTRY EVENT

in Malaysia and the only 4-in-1 cyber security event in the region.

SATELLITE EVENTS

- Cyber Forensic Colloquium
- Cyber Security Risk Management
- Malaysian Technical Programme (MTCP) 2019 Closing Ceremony
- Cyber Security Job Fair
- NICTSED 2019
- CIO Roundtable Discussion By Malaysia Airport Holding Berhad (MAHB)
- OIC-CERT Academic Colloquium

COMPONENTS

6 AWARDS

MALAYSIA CYBER SECURITY AWARDS 2019

26 September 2019

1 CONFERENCE

KEYNOTE & PANELIST SESSION

23 September 2019

RM636.00 (Inclusive 6% SST)

45 EXHIBITORS

LOCAL & INTERNATIONAL COMPANIES

23-25 September 2019

11 TRAININGS

CERTIFIED & COMPETENT TRAINING PROGRAMS

23-27 September 2019

HRDF CLAIMABLE

#TOP5 CYBER SECURITY CONFERENCE IN REGION

REGISTER NOW

Awards	www.csm-ace.my/nomination_criteria.html	Exhibition	www.csm-ace.my/enquiry.html
Conference	www.csm-ace.my/registration.html	Training	www.csm-ace.my/training.html

SCAN ME!

This is a QR code. Use a smart phone to read it, and it will take you to CSM-ACE 2019's website.

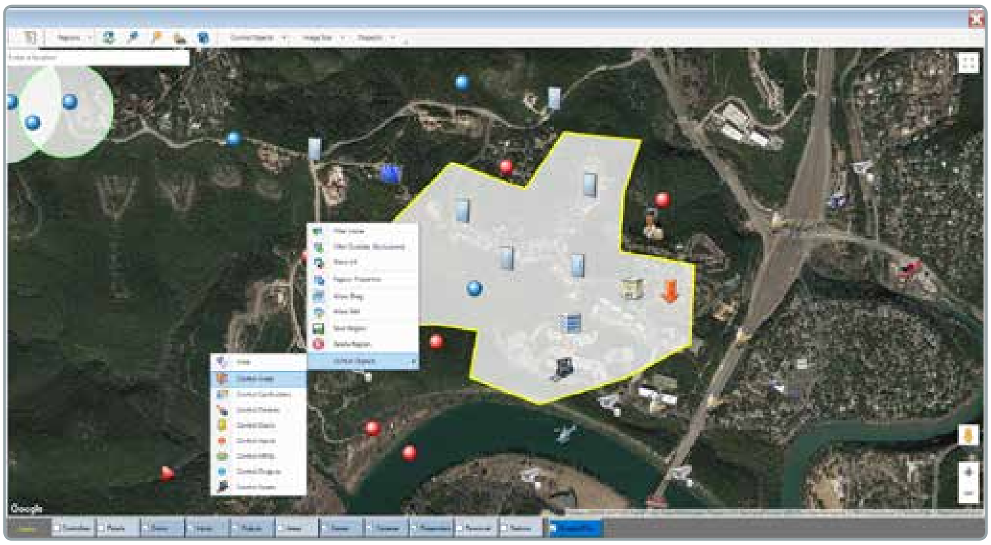
- Download and install a free QR Code reader application.
- Take a picture or scan the QR Code with your mobile device.
- The code will take you to CSM-ACE's website.

Tel: +603-8800 7999

Fax: +603-8008 7000

E-mail: secretariat@csm-ace.my

For more information about CSM-ACE 2019, go to www.csm-ace.my



situations and dynamically changing access permissions is a major breakthrough for the physical security world.

The use cases in this category are wide ranging. For example. when AI is applied to access control, it can identify unusual activity such as off hour access, abnormal location access and combine it with other threat indicators to quickly identify insider threats. Risk-adaptive access can prevent people from entering an area where a traditionally "non-obvious" danger exists, and, it can allow a first responder with the right credentials to access an area when threatening conditions exist.

Case in Point: A nuclear power plant employee may have authorized access to a specific location, but there may be multiple reasons at a particular moment that the employee should not enter. This could be for security of the organization, or for personal safety. There might be a safety threat and the risk-adaptive access control system would leverage AI to recognize this and prevent him or her from entering.

Consider some of the high-risk situations and what could occur if an unsuspecting person entered an area of risk. Chemical spills, radioactivity, fire and other incidents are dangerous examples to name a few. Those are relatively obvious risks and even legacy access control systems can provide some rudimentary measures to seal off areas of concern. However, without added intelligence and insight capabilities such as risk scoring and AI to identify these risks, the current access control systems cannot adjust based on rising or sudden threats. However, if the facility integrated its AI-driven physical access control system with other systems, such as Certification Management, Building Automation, IoT sensors or video analytics, any entrance then becomes risk-adaptive and proactively secure.

Get Ahead of Threats with Intelligence

Security operators tasked with monitoring an overwhelming number of systems. It can result in information overload and alarm fatigue. The cause? Too many false alarms and not enough early warnings.

To make matters worse, the only alarms the operators receive are either too late to act on or they are inaccurate. AI provides a new level of situational awareness for physical security enabling teams to receive early warnings and reduce false alarms from a single platform. This provides a common operating picture across every building, controller, credential and sensor. Adopting this intelligent and more proactive posture provides actionable insights in real-time, so complex and daily threats can be stopped before they turn into breaches.

Case in Point: Everything in an airport is in high-speed transit: pilots, passengers, luggage, as well as data. The problem with things in motion is they are challenging to monitor and control consistently, making it a high-risk environment. On top of all the security equipment, there is plenty of operational technology (OT) required to keep the airport moving. The result is many types of high-speed and volatile data needing real-time analysis. With AI, airports can ensure OT doesn't affect physical security, and vice-versa, while also making sure there are limited false alarms. This improves accountability of the entire operation and can give early warnings in order to prevent small deviations from becoming international headlines.

Real damage – physical or digital – can be caused by breaches into operational systems throughout an airport, through physical access to IT assets, or through direct access to these systems and multi-vector attacks can wreak havoc quickly. For example, at the Bristol airport, a digital breach took down the flight display systems, creating chaos for all travelers. This resulted in missed flights and increased confusion, all while forcing employees to revert to manual procedures to communicate flight updates. Similarly, suspicious drones flying over the runway were able to seriously disrupt holiday travel plans for more than 10,000 passengers traveling through Gatwick airport in 2018.

Having risk-aware, AI-based

physical security technologies in place can help to identify those "unknown unknowns" before they disrupt flow of traffic and flights. And, if safety is at risk, time is of the essence so intelligent, adaptive controls are key to effective risk mitigation.

Move from Reactive to Proactive in Emergency Situations

The risk landscape has shifted with the modern enterprise. Threats now come in different shapes from all directions at the same time, making collaboration with the right people at the right time increasingly difficult. AI-powered emergency management is a tool that helps distill intelligence from big data, providing real-time decision support to operators and first responders. This means that organizations can collaborate better and mitigate faster when seconds matter most.

In combination with a geospatial tool, AI-powered emergency management can immediately identify people, buildings or assets at risk based on the severity, type and location of the threat. This awareness can be combined with live video feeds of a facility and other forms of intelligent insights to improve the time and quality of any first response.

Case in Point: Security around active shooter situations require a high level of collaboration – across data siloes as well as organizations. In the case of an emergency lockdown situation at a campus, first responders with proper identification and smart device can gain access to a building door or even be allowed to access the video surveillance system to see inside the building before entering. Today, with legacy access control systems, the first responder would be locked out and unable to quickly get eyes on the situation. Further, through integration with ballistic detection, social media, web feeds, mass notification and GPS, AI can quickly compile evidence and forensic records and actionable guidance for first-responders to further boost visibility and minimize the overall impact of the incident.

Embrace the Power of AI Today and Be Prepared for the Threats of Tomorrow

These examples are proven based on standard equipment, established practices and available technology. It's possible to harness the power of AI to transform any security posture into a proactive, intelligent security posture.

By Clayton Brown, Executive Vice President, ReconaSense

Do Criminals Dream of Electric Sheep: How technology shapes the future of crime and law enforcement

New report triggers discussion about innovation and strategic foresight in EU policing

"It is no longer good enough to be reactive... our agency's ability to predict which emerging technologies criminals will turn to next is instrumental to our mission of keeping EU citizens safe."

Catherine De Bolle
Executive Director of Europol

The advent of so-called disruptive technologies – those that fundamentally alter the way we live, work and relate to one another – provides criminals with new ways to pursue their illegal goals, but also equips law enforcement with powerful tools in the fight against crime. To remain relevant and effective, it is necessary for law enforcement authorities to invest in understanding and actively pursuing new, innovative solutions. Europol has published today a report, which will serve as a basis for future discussions between Europol, EU law enforcement and their stakeholders.

Some of the emerging technologies include Artificial Intelligence (AI), quantum computing, 5G, alternative decentralised networks and cryptocurrencies, 3D printing and biotech. These are set to have a profound impact on the criminal landscape and the ability of law enforcement authorities to respond to emerging threats. The disruption comes from the convergence between these new technologies, the previously unseen use cases and applications, and the challenges posed by existing legal and regulatory frameworks.

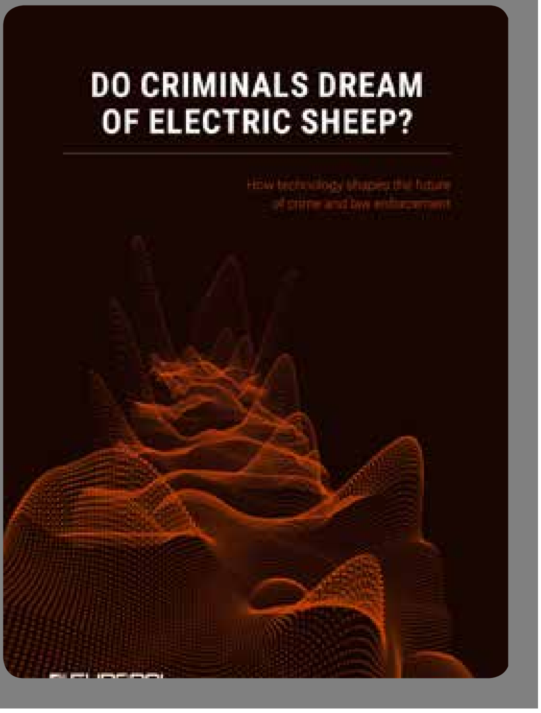
The report aims to identify the security threats associated with this and points to ways for law enforcement to use the opportunities brought by these technologies to combat crime and terrorism. It also highlights the pivotal role of the private sector and the importance of law enforcement to engage more with these actors. Furthermore, it is of paramount importance that the voice of law enforcement is heard when legislative and regulatory frameworks are being discussed and developed, in order to have an opportunity to address their concerns and needs, particularly with regard to the accessibility of date and lawful interception.

Europol can deliver additional value in an age of rapid digital technological development by increasingly engaging in expertise coordination and collective resource management, which avoids unnecessary duplication of resources and expertise at national level. The Europol Strategy 2020+ set out for the organisation to support the Member States by becoming a central point for law enforcement innovation and research.

Europol's Executive Director, Catherine De Bolle, said: "Europol's strategy sets out our ambition to firmly establish Europol as an innovator in law enforcement at the European level. It is no longer good enough to be reactive. Our ability to predict which emerging technologies criminals will turn to next is instrumental to our mission of keeping EU citizens safe. We hope to start a discussion with law enforcement in the Member States and other stakeholders."

Download the full report "Do criminals dream of electric sheep: how technology shapes the future of crime and law enforcement".

https://www.europol.europa.eu/sites/default/files/documents/report_do_criminals_dream_of_electric_sheep.pdf


DO CRIMINALS DREAM OF ELECTRIC SHEEP?
How technology shapes the future of crime and law enforcement

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

International Association of
CIP Professionals

I recently watched, for the first time, the Bruce Willis film – Die Hard 4 -'Live Free or Die Hard' which was released in 2007. I am sure most of you will have seen it and how it has taken me 12 years to get round to watching it I will never know. Now I am not the greatest 'Die Hard' fan but this film based on an article 'A Farewell to Arms' written in 1997 did catch my attention.

I have been reading a lot about Cyber activity, both good and bad, over the last few months, as we at the International Association of Critical Infrastructure Protection Professionals (IACIPP), have been developing our interactive member's platform on our web site. Within this there is a considerable focus on the cyber threats and the ongoing work across government agencies, industry and academia seeking new and innovative solutions to the challenges that continue to emerge.

For those of you who know the plot in Die Hard 4, you will recall that it is all around a tech-savvy villain launching an attack on America's computer infrastructure which is basically a cyber-attack designed to disable the nation's infrastructure. And to cut a long story short, it sends a clear message, well it was clear to me anyway, that even when fighting a high tech threat you often have to rely on, not just high tech solutions but also some old fashioned methods, like ensuring the very basics of general security principles are in place and effective.

In the film one of the intentions of the villains is to shut down the electricity power grid, something which in itself remains very topical today, but to do so the baddies have to gain physical access to the power station (which they do) to finalise their intentions.

My simple point in all this, is that although infrastructure security professionals are very aware of the balance required to address the current and emerging threats, it is very easy to get distracted by the major cyber threats facing us all. This is particularly so when a real concern articulated by many, as highlighted in a recent report from the Chartered Institute of Information Security (previously known as the IISP) identified that the current level of cyber threat is outstripping the corresponding increases in investment to deal with the issues and cyber security professionals feel their budgets are not giving them what they need.

It is, therefore, hardly surprising, that the limited resources that are available are often invested in the cyber direction which has the potential to have a detrimental impact on the innovation and effort still required within the realm of physical security. Combining cyber and physical security into one

The IACIPP Poll

The results are in! Responses to the recent poll give the following insight.

Q. Where do you see your next major security threat?

- Cyber attack - 42%
- Insider Threat - 28%
- Terrorist attack - 15%
- Man Made / Ineptitude - 14%
- Natural Disaster - 1%
- CBRNE threat - 1%

As nearly half respondents are viewing a cyber attack as their next main threat, our latest poll aims to investigate this further:

Q. How prepared do you feel for a cyber attack?

- Very well prepared
- Well prepared
- We are preparing but not yet there
- We have just started preparations
- We are not prepared but have started, not prepared
- We have not made any preparations and unprepared

Visit www.cip-association.org to cast your vote.

integrated strategy is not just desirable but crucial.

The combination of both cyber and physical into a holistic security strategy is something that we within the IACIPP encourage. It is also one of the reasons why we continue to support the Critical Infrastructure Protection and Resilience Europe Conference (CIPRE).

This year's event will take place in Milan between the 14th and 16th October and is being hosted by the Lombardia Regional Government. It is designed to incorporate a twin track approach to explore the challenges and innovations around both cyber security and protective security. This format has worked extremely well in previous conferences and the agenda for this year looks great. Have a look at the website ww.cipre-expo.com to see what is being lined up.

If you want to know more about the work that we within the IACIPP are doing on infrastructure security and resilience please have a look at our website – www.cip-association.org

If you do make it to Milan I look forward to seeing you there.

John Donlon QPM FSyI

Chairman IACIPP

The International Association of Critical Infrastructure Protection Professionals Appoints Sheraz Ali as Director for Cybersecurity Sector, North America

The International Association of Critical Infrastructure Protection Professionals (IACIPP) is delighted to announce the appointment of Sheraz Ali as Director for Cybersecurity Sector, North America

Mr. Sheraz Ali is the digital evangelist, serial entrepreneur, guest lecturer, researcher and valued international speaker on the subjects of Digital Transformation, Cyber Security and Risk Management.

Mr. Ali has almost two decades of experience in numerous management and consulting roles in the fields of Digital Transformation, Cybersecurity, Risk Management, Information & Technology Services, Security Education Training and Awareness, Business Consulting and Financial Services.

He also holds several positions in the executive advisory boards. He is the founder and Executive Director of the European Cyber Resilience Research Network (ECRRN), which focuses on building cross industry bridges to help enhance Cyber Resiliency of organizations in Europe. He is also the Chair of Board of Directors of The Resiliency Council of Canada (TRCC) committed to help Canadian Industry develop and deliver disruptive Intelligence, Surveillance and Reconnaissance (ISR) technologies to increase the security and resiliency of the Canadian digital ecosystems through improved technical, social, and regulatory solutions for adverse scenarios.

Mr. Ali have supported NATO, The Transatlantic Steering Committee and C level Business Executives, CIO's and CISO's among fortune 500 businesses with effectively reframing (complex) Business and IT problems into value adding business opportunities. As an example, He have supported C-level executives at NATO Communication and Information Agency (NCI Agency to deliver ultimate Customer Experience while maintaining Agility, Speed, Security and E-Privacy with the "Best in Business Award" winning digital security solutions.

John Donlon QPM Chairman of the IACIPP said, "I am delighted that Sheraz has accepted the position as Director for Cybersecurity Sector, North America with us. Sheraz brings a wealth of experience in the cyber security and defence sector, so will be a tremendous asset to the organisation and the global CNI community."

Assessing Modern Threats and Vulnerabilities in the Sports Landscape

In the second of this two part feature, Stephanie Jenkins, Cyber Security Analyst Sporting and Critical Infrastructure and Dr. Nathaniel Evans, Cyber Analysis and Research Program Lead from the Argonne National Laboratory, analyse the protection and resilience of stadiums and arenas.

The development of an applicable, high-level risk assessment tool offers significant benefits if executed at various levels of facility characterizations. From high schools to collegiate venues, to professional stadiums and arenas, there are varying levels of threats and vulnerabilities that require consideration. A sport risk assessment tool would accommodate the evolving landscape of threats specific to facilities. An assessment that is broken down into major subsections can ensure that varying aspects of safety, security, and emergency management are met.

First, it is important to establish the environment and facility design and characterization for an assessment. Location and proximities to adjacent facilities and critical infrastructure provide a basis for recognizing the facility environment. Both physical and cyber perimeters need to be established to assess controls and mitigation steps that are already in practice. Physical securities would encompass traffic, barriers, ingress and egress locations, and any pre-established emergency and medical entrances.

The breakdown of threat ratings can highlight any vulnerabilities that should be addressed for prevention and mitigation as well as their level of urgency. Using a scaling system to assess the likelihood of an event can give an outlook on these susceptibilities. Threats can range from severe weather conditions, to criminal acts, terrorism, to sabotage, which can encompass shootings, explosions, chemical attacks, or cyberattacks. Once these threats are highlighted, current mitigation techniques are reviewable. These mitigation procedures can be technological in nature, include detection systems, or include material solutions or trainings. Types of threats to consider can have voluminous range. A growing threat remains within cyber, but incidents regarding inclement weather, riots, and even pandemics should also be discussed.

Access control measures, when applied to stadiums or arenas, are effective if properly managed and monitored. The level of credentialing that is enforced amongst employees at a venue can have an impact on the protection of critical systems and information. Potential penetration of access control systems through a cyberattack needs consistent monitoring, especially if a particular system uses electronic keycards. Procedures can include: monitoring for an abnormal number of login attempts from a single gateway, and determining if or how restricted IT is physically secured. Electronically locked gates and entry points can also benefit from surveillance. Monitoring multiple attempts of swipes on keycards can raise concerns if an employee continuously tries to gain access to an area to which they are not allowed. Certain levels of employees that have been granted access to restricted areas and high-level networks can be monitored through frequent background checks. Employee lists should be updated constantly, and electronic badges should reflect this status. This practice is applicable to the entire employee spectrum, ranging from contractors to full-time and single-event personnel.

With high traffic volumes of sporting events, traffic control has come to rely on some network aspects with regard to signage and ingress and egress locations. Public transportation systems that run adjacent to a facility need to be considered and monitored for any suspicious activities in conjunction with event times. As demonstrated in the aforementioned Dallas incident, the ability of hackers to gain access to traffic signage can lead to confusion and disruption of traffic management. While it may not pose an imminent danger to a venue, vehicular threats remain prevalent as a platform to target groups of people. By conducting vehicle checks and monitoring information against law-enforcement databases, these threats can be mitigated. Vehicular access control through physical security measures is most common, but in all reality, simple technological measures can make a difference.

Surveillance and detection should also be discussed in conjunction with access control measures. While there may be physical barriers for such areas as the loading dock or production trucks, an extra layer of security can include the monitoring of these restricted areas through the use of CCTV or live video feed. To prevent adversaries from infiltrating live video feeds or access to CCTV, security measures and mitigation steps are necessary. For large-scale events, it is also essential to use the command and control center to monitor social media outlets for posted or referenced suspicious activity. The command center can also monitor cameras both inside and directly outside of a venue to pinpoint any other suspicious activities. Command centers are vital to the protection of both physical and technological components of a stadium, especially at events that have such high profiles as the Super Bowl. A command center must also be equipped with backup systems to maintain open communication capabilities with response forces.

The topic of drones and the threats and hazards they pose to stadiums and spectators continues to circulate in safety and security discussions. While counter-drone technologies are an issue in and of themselves, there seems to be little action taken to prevent a disaster occurring from the origin of a drone. In one example, a local resident flew a drone over Levi's Stadium and dropped leaflets about conspiracy theories. How would have the venue responded if the adversary had dropped a chemical agent or a chemical weapon? Current Federal Aviation Administration regulations prohibit drones from operating within three nautical miles of certain National Association for Stock Car Auto Racing (NASCAR) events as well as stadiums hosting National Football League games, Major League Baseball games, or National Collegiate Athletic Association (NCAA) football games. Drones are also prohibited one hour before and after an event's scheduled time; however, these rules have been broken in the past. Deploying some level of drone detection may be necessary for standardizing mitigation processes.

Though emergency management protocol varies from one venue to the next, a basic application of an emergency action plan should be established no matter the venue. This ranges from shelter-in-place protocol to evacuation routes, medical care, and event disruption modules. Interoperable communication systems are vital as well, and require alarm systems, radio systems, and backup communication systems in the event of an emergency. An incident response plan should be practiced and put into place long before any potential emergency. Depending on the size of the venue, this may include local and state jurisdictions. Technological procedures are recommended in order to detect, deter, delay, and respond to criminal acts, weather events, terrorism, or potential sabotage. Ultimately, a risk assessment can be the core to establishing a solid emergency action plan, as a risk score considers the likelihood, severity, and overall impact of a potential event.

An important aspect to gain from a risk assessment is determining whether the venue has a disaster recovery and restoration plan for IT as well as for telecommunications for critical data and systems. There is a heavy reliance upon telecommunication and information technology infrastructure within professional stadiums in today's sport landscape. Critical systems and networks should be considered, as the core of venue operations may rely on these capabilities. Wi-Fi and point-of-sale (PoS) systems can also be affected by potential loss of power or lack of restoration efforts. At esports events and venues, Wi-Fi and Internet connections are the backbone to the entirety of the sport. Looking at PoS, as of 2019, Major League Baseball's Tampa Bay Rays have become the first major U.S. sports team to forego cash and instead solely accept payments via credit cards, gift cards, Apple Pay, and Samsung Pay. Tropicana Field will implement the same sales system in an effort to reduce queuing times for an overall increase in fan satisfaction. This will be beneficial to fans attending events at the venue, but a PoS system or terminal can potentially succumb to a cyberattack as well. Previous incidents of PoS-related data breaches have affected companies such as Target and Home Depot, leading to compromised credit card information for millions of customers. A PoS system that is infected with malware could be specifically designed to steal information and codes, leading to issues within business continuity for organizations.

An emergency action plan should also consider the capabilities of individuals and employees on site. If there is a cyberattack on critical systems, responsible personnel should be identified prior to an attack. Members of the IT department are a key aspect of mitigating the threats and cyber vulnerabilities throughout a stadium or arena. Command centers of larger venues, either onsite or offsite, need to be well equipped with Internet and video capabilities in order to handle cyber incidents. Through the use of command centers, intelligence sharing can also proliferate should a grandeur attack occur. The District Detroit, located in the heart of downtown Detroit, Michigan, is one of the largest sports and entertainment developments in the United States. It is home to theaters, restaurants, shops, parks, and three professional sports venues, all within walkable distances. While The District Detroit has already had a positive impact on the economic growth of the city, the concentrated area of high-profile professional sports venues, namely those of Major League Baseball, the National Hockey League, the National Basketball League, and the National Football League, raises concerns. The idea of network segmentation would be imperative for such a concentrated area. Segmenting networks from stadium to stadium is a mitigation tool to decrease the likelihood that if an adversary gains access to one system, they essentially gains access to all stadiums. Stadiums should also consider implementing an information-sharing system by which one stadium is informed of an incident at a near-site location. Also, by isolating cyber systems from business systems internally, an organization can add to its business continuity protection and programming.

While many venues are technologically advanced, the backbone of security still stems from response forces. Even

though venues rely heavily on automated systems and technological capabilities, a concrete core of trained and prepared groups of personnel is still essential. Specific tabletop exercises are suggested to include a focus on cyber and technology incidents and injects, in conjunction with physical response forces. Within exercises, the review of the documentation outlining the venue capabilities and response plans need to be presented clearly. The training for cyber incidents is not only important for stadium IT response forces but also for facility management personnel. Cross-training in critical systems amongst various departments offers long-term advantages. The ability to recognize suspicious or abnormal cyber activity while also mitigating potential hackings must be a constant component of emergency planning and exercises. Tasks such as monitoring for an unusual number of login attempts within certain systems, or key-card swipes are simple enough for cross-trained employees to accomplish.

Critical systems are vital to the daily operations within a facility. With the continuous growth of technological dependencies for critical systems, cybersecurity vulnerabilities continue to rise. Building control systems include HVAC, lighting and power, cameras and surveillance, and fire suppression systems. Intrusion detection systems are an application that can also be implemented to monitor malicious activity. Continuous monitoring of these systems is essential to the safety and security of any stadium or arena, especially if the systems are available externally over the Internet, which can make them even more vulnerable. Power continuity and redundancy are also vital to the successful running of baseline functions for game-day operations. With a heavy reliance upon integration amongst critical systems, the monitoring and maintenance of those servers is crucial. If the servers go down, the impact can be immediate. Redundant capabilities within critical IT systems should be tested and monitored by personnel not only on game days, but also on regular business days. The possibility that an adversary gains access to the fire suppression system or the fire alarm system is a reality, as seen through the example in Dallas from 2017. Cyberattacks can then directly lead to physical attacks and threats.

Communication systems strengthen the backbone of the successful operation of a stadium. Communication systems can include message boards, public address systems, and the ability to extend emergency communications. A hacker has the potential to gain access to the visual displays throughout a stadium, which can lead to falsifying messages on the boards throughout a venue. The panic and confusion would hastily ensue. A false evacuation announcement can lead to confusion not only amongst spectators but also amongst staff members. Then, imagine false evacuations occurring at various venues concurrently in a densely populated district, where there are multiple sporting events occurring simultaneously. Mass evacuations can be a sitting target which could lead to physical threats and hazards, all linking back to an adversary gaining unauthorized access to a critical system within a venue.

Cybersecurity threats and vulnerabilities within stadiums and arenas will only continue to increase in the future. The conversation around this growing field within sports should depict the increasing prevalence of real threats. Stadiums and arenas have advanced technologically, but the security of these systems and networks lack these advancements. A self-defense stance on cyber should be reflective of the self-defense practices for physical threats to a venue. Having specific staff that are dedicated to the application of cyber guidelines and best practices can help mitigate the growth of threats at various levels. If a third-party vendor is used for security measures at a venue, it is important to keep an open line of communication regarding expectations and policies. Coordination and open communication with service providers can also be beneficial in such incidents as a power outage or loss of communication systems.

In 2018, the National Football League's San Francisco 49ers became the first US sports team to supplement its stadium security with a real-time stadium operations system. The analytical tool is powered by SAP and will help manage stadium operations from a digital boardroom, providing instantaneous response mechanics to resolve issues, to increase stadium experiences for fans, and provide an extra layer of digital security. The system tracks an array of operations simultaneously processing throughout the stadium, including parking, concessions, retail, weather, ticketing, and social media. While this approach focuses more on the fan experience on game day, the security integration is applicable to stadium operations. A tool to monitor suspicious activity on networks or systems within a venue can assist personnel with the monitoring of cybersecurity issues.

At the 2019 National Collegiate Athletic Association (NCAA) College Football Playoff title game, Respond Software did just that. In conjunction with venue security and students from Norwich University, Respond Software was responsible for monitoring and mitigating potential cyberattacks. More than 243,000 cyber events were monitored during the game using an artificial intelligence-based decision platform. Of those 243,000 events, 200,097 were investigated in depth. Of those, 431 events were deemed malicious, and 13 were declared as needing immediate mitigation. This gives a quantitative insight in to just how many cyberattacks can occur during a singular sporting event. Under general cyber best practices, intrusion detection systems (IDS), intrusion prevention systems (IPS), and security information and event management (SIEM) systems improve mitigation strategies for potential cyberattacks or adversaries gaining access to in-house networks or systems. Real-time analysis of security abnormalities and the monitoring of systems for malicious activity can provide instantaneous awareness of potential cyber incidents.

As emergency drills address physical threats, network and system security tests should likewise be conducted to address cyber threats. Security system checks can bring to light any malfunctions or unusual activities through hardware and software scans. A dedicated staff of security personnel for cyber aspects may not be necessary for every venue, but the enactment of such a team can help mitigate cyber threats before and after high-profile sporting events. The role of monitoring security systems should be identified throughout venues. The dedication to developing a cyber staff can also depend on the number of systems and their reliance on Internet and technology. Regardless of staff dependencies, the venue itself should have a cybersecurity plan that includes the outlined restoration plans, response, and mitigation procedures. Standard operating procedures need to be highlighted as well. As a subsector of critical infrastructure and potentially housing thousands of fans, stadiums' critical functions need to be maintained during disruptions. Segmented environments, firewall technologies, and the monitoring of removable media within all systems can improve resiliency within the network of a venue. Scoreboard systems, emergency management systems, critical systems, public networks, enterprise systems, and point-of-sale systems can benefit from being segmented throughout a venue.

Conclusion

The deployment and implementation of the Sports and Entertainment Risk Assessment tool is a step toward building a solid, standardized foundation for safety, security, and emergency management in the commercial sector. There is a growing emphasis on the technological advancements within critical infrastructure, and the ability to assess and monitor these changes is vital. With this tool, venues can conduct internal assessments as well as gain comparative results to benchmark themselves against similar facilities. Opening communication amongst the commercial sector can be beneficial for the implementation of modern day protocols and best practices. The threats and hazards remain prevalent in today's landscape, and the best defense is a proactive approach to preventing and mitigating these threats. At the very core of prevention and mitigation is the first step of conducting a risk assessment. The influential impact of an assessment tool can reap many benefits for venues.

This work was partially supported by the U.S. Department of Energy, Office of Science under contract DE-AC02-06CH11357.

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 new 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 currently FREE to qualifying individuals - see **www.cip-association.org** for more details.

Our initial 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

Why should Critical Infrastructure companies invest in electronic locking system to protect their operations?

Critical Infrastructure plays a dynamic role in supporting the seamless assimilation and progression of the modern society.

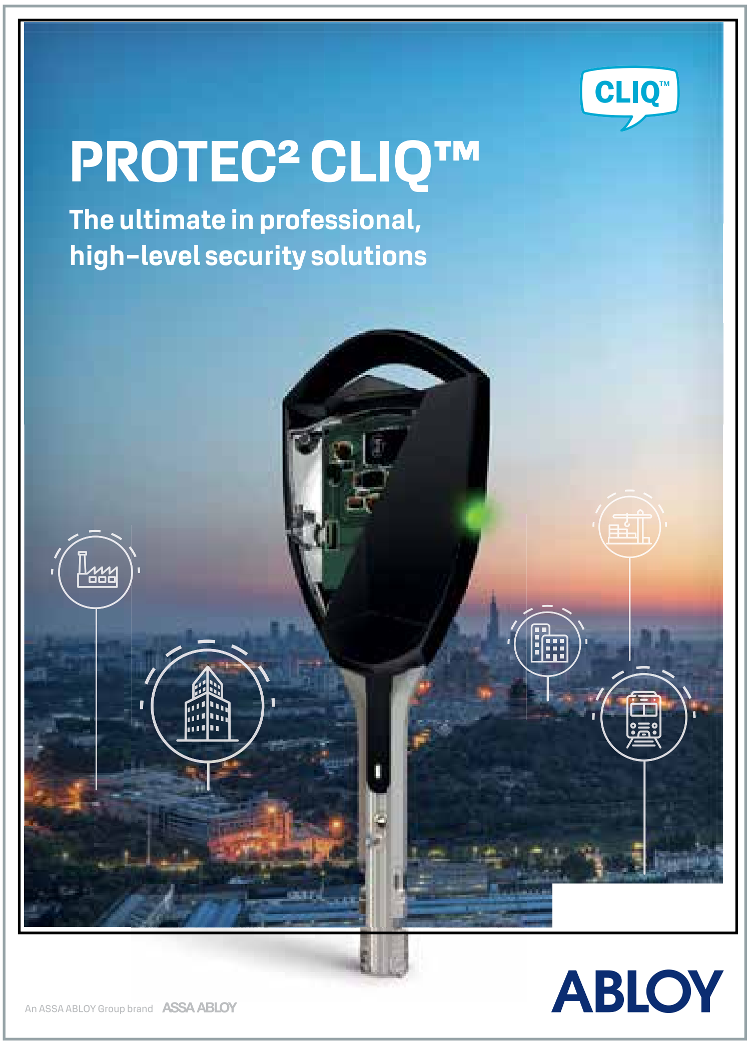
Physical protection of critical infrastructure performance and reliability as well as securing continuous operation is today easier than ever with electronic locking systems. At its best physical access control becomes integral part of company's ecosystem combining work management, compliance, subcontractor management and remote monitoring systems, just a few to mention.

Electronic locking systems provides users value in several areas:

- Key management becomes simplified and risk free, since smart phone apps can be used to validate access with central online access management. This is a great convenience for critical infrastructure operations with multiple locations across vast distances with large numbers of people needing access.
- Convenience of digital technology in smart keys, locks and access control systems takes logistics out of the equation. Convenient web based access rights management ensures right people have access to right places at the right time. Transparency with audit trails gives visibility and increases the trust for your operations.
- Electronic access rights can be granted or cancelled remotely increasing the flexibility of the operations and removing the risk of lost keys.
- Implementation of modern electronic locking systems is

cost-efficient when solutions are wireless. Upgrading of existing legacy systems into electronic and digital systems is quick and easy when new locks fit existing infrastructure. Energy efficiency of wireless locks delivers significant cost savings.

Abloy offers security and locking innovations dedicated to creating more trust in the world. Combining digital and mechanical expertise, Abloy Oy develops industry-leading security solutions that protect people, property and business. Abloy is part of the ASSA ABLOY Group, the global leader in access solutions. Every day, we help billions of people experience a more open world. www.abloy.com


CLIQ™
PROTEC² CLIQ™
The ultimate in professional, high-level security solutions
An ASSA ABLOY Group brand ASSA ABLOY
ABLOY

Advanced walk through screening solution tested by European Union regulator for use in airports

Rapiscan® Systems, a leading global supplier of security inspection technology, today announced that its Metor 6E people screening solution has achieved the European Civil Aviation Conference (ECAC) and European Union (EU) performance standard for walk-through metal detectors.

ECAC has established a Common Evaluation Process (CEP) and standards for testing security equipment. Passing the performance standard for walk through metal detectors signifies that the Metor 6E can be used in airports within the ECAC/EU.

Rapiscan's Metor 6E is a state-of-the-art walk through metal detector, built to support the most demanding and high-traffic security screening environments. Designed with advanced features including automatic interactive sensitivity adjustment, automatic frequency selection, power guard and violation monitoring, the Metor 6E delivers powerful screening for airport checkpoints. The sleek, easy-to-install system was developed to comply with internationally recognized aviation requirements, and to integrate seamlessly into high-risk security infrastructures.

"Achieving this performance standard is a great accomplishment for the Rapiscan team, and demonstrates our commitment to investing in the highest quality technologies," said Mal Maginnis of Rapiscan Systems. "Many customers around the world rely on the ECAC/EU when setting their own standards and now will be able to acquire the Metor 6E."

MARSS awarded NiDAR perimeter security and drone detection system contract for 90m+ superyacht

MARSS have secured a contract for the installation of their NiDAR perimeter security and drone detection system onboard a 90m+ superyacht.

NiDAR provides long range 360 degree perimeter surveillance detecting surface and air approaches in the vicinity of the vessel while underway, at anchor and in port. The system operates autonomously and discreetly 24/7 while smart software

algorithms automatically analyse and rank threats, triggering alerts to notify crew and security personnel.

By integrating security radars, advanced thermal cameras and searchlights, NiDAR presents a real time awareness picture to operators via an intuitive touch screen interface. An integrated tracking system also enables the crew and security teams to track the live location of tenders and toys via the NiDAR interface.

The vessel is under construction and due for delivery in 2021.

DHS S&T Awards $200K to San Diego's Planck Aerosystems Inc. for Final Testing of Small Unmanned Aircraft System

The Department of Homeland Security Science and Technology Directorate (S&T) awarded Planck Aerosystems, Inc. of San Diego, California, $200,000 to begin testing its autonomous small Unmanned Aircraft System (sUAS) in operational settings.

Planck received its award as part of S&T's Silicon Valley Innovation Program (SVIP) in partnership with U.S. Customs and Border Protection (CBP). Planck's system capability enables a sUAS to launch from and land on the bed of a moving vehicle, in addition to providing fully autonomous

navigation coupled with a securing mechanism, advanced computer vision capabilities, and customized communications interfaces.

Through a combination of integrated technologies, including full-motion video, automatic target detection and geolocation, Planck seeks to provide CBP agents with a portable, ruggedized detection system that provides real-time situational awareness in the field.

"S&T is looking for technologies to enhance the efficacy of CBP patrols while simultaneously increasing the safety of patrolling agents," said SVIP Managing Director Melissa Oh. "We look forward to the ways Planck will further refine its technology in support of this homeland security mission."

In this fourth phase of SVIP, Planck will focus on functional usability improvements, such as improving user interfaces and increasing nighttime functionality.

Companies participating in the SVIP are eligible for up to $800,000 of non-dilutive funding over four phases to adapt commercial technologies for homeland security use cases.

CONTROP Presents a Complete Solution for Coastal and Maritime Surveillance at DSEi, with its Two Proven Systems – the TORNADO-ER and the SPEED-ER

CONTROP a company specializing in the field of Electro-Optics (EO) and InfraRed (IR) Defense and Homeland Security solutions – presents a unique EO suite comprising the TORNADO-ER and the SPEED-ER systems.

The TORNADO-ER provides a panoramic InfraRed (IR) image, automatic detection of moving maritime targets as well as multi-target tracking capability, covering dense maritime areas and detecting swimmers at short ranges and vessels up to 12km. The SPEED-ER is a long-range observation system that is cued to those targets which have been detected by the TORNADO-ER, enabling users to explore the targets and their contents, and providing highly accurate locational details. The two solutions are controlled by a dedicated C2 system, a man-machine interface (MMI) which includes intuitive panoramic imagery, maps, enlarged images, and observation videos. The user-friendly MMI presents targets on the map and on the panoramic image, providing all required information upon request.

The TORNADO-ER includes two mid-wave infrared (MWIR) cameras. The live videos from these cameras are "stitched together" to provide one panoramic stream. The system scans at a rate of 3 seconds for 360°.

The SPEED-ER has an extended long range camera and highly stabilized optics, featuring CONTROP's unique technologies. The sensors include MWIR, Short Wave InfraRed (SWIR), Daylight Channels, Laser Range Finder (LRF) and an optional Laser Pointer.

"Always attentive to the needs of our customers, we have developed a comprehensive coastal solution for maritime surveillance that enables a single operator to essentially control the seas," says Mr. Ra'anan Shelach, CONTROP's VP Marketing. "It is already in operational use, providing highly effective surveillance capabilities, mainly in dense waters and seas with crowded traffic, such as ports, waterways, straits, etc."

3DX-Ray complete training package for Middle East customer

UK based technology company 3DX-Ray have completed another training package for an unspecified Middle East customer at their restricted port facility.

3DX-RAY provide comprehensive training for all of their systems, and a range of training courses are available both on-site and off-site. Training courses are tailored to meet specific customer requirements and all training is carried out by their qualified engineers.

This course was specifically to train the customer in the use of the MailScan2-M cabinet x-ray system, used for screening mail, parcels and small packages for potentially harmful items and contraband. The trainees were introduced to the principles of x-ray imaging and given an understanding the importance of the image enhancement features provided within the software. On completion of the course the trainees demonstrated enhanced skills in the recognition of prohibited and dangerous goods amongst everyday articles

In the MailScan2-M a large inspection chamber and imaging area is packed into a remarkably small footprint. This makes 3DX-RAY's MailScan solution ideal for locations where space is at a premium, such as mailrooms, as in this case.

Unrivalled image resolution and industry-leading image processing software, together with powder-detection, allow the operator to analyse images quickly and accurately. Items such as weapons, improvised explosive devices, razor blades, biochemical attack threats, powders and drugs are easily detected.

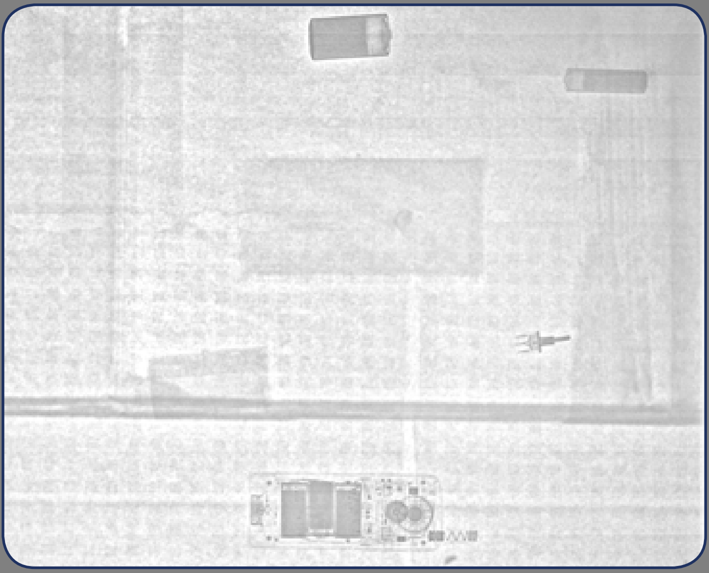
Increasing prison security using portable X-Ray systems

Prisons security reqierments increasing as technology and prisoner's sophistication evolve.

A prison in Columbia needed a solution to inspect outside of the entrance, dozens of new prisoners that Arriving with large bags containing their private stuff: food, sheets, mattresses and electric devices, which will not fit in the standard luggage scanners.

Another request from a prison in Guatemala was to scan the cells walls to make sure no money, weapon or mobile phones are hidden inside.

The solution for both missions and others, is a portable X-Ray system that can be deployed everywhere in minutes and scan objects in different dimensions, shapes and density.



Using lightweight yet strong battery operated portable X-Ray sources allows to penetrate even thick walls, a sophisticated software Installed on a laptop allows to enhance and save the images so they can be used as evidence if needed, In order to make the process faster, possible to combine up to 9 flexible imaging plates, each in size of 36X43 cm and scan them all together in a very high resolution to cover large areas.

Systems are designed to work in every weather condition or terrain and all parts are packed in a rugged and portable case.

System is safe and only requires to keep several meters distance during operation.

VCsecurity can offer several solutions to fit every client needs and budget.

In the example image you can see Money, batteries and phone concealed behind 20cm of thick Ytong wall.

Multi-million pound project to enhance Police Scotland IT

Police Scotland is investing £3.9m in a faster computer network to improve service and efficiency across the country.

Officers in rural areas are among the first to benefit from a move to a single provider – giving them access to video conferencing and faster file sharing.

The National Network Project – NatNet2 – has been installed in 20 pilot sites across the country ahead of a national phased rollout until March next year.

NatNet2 will deliver increased network performance, stability and capability by removing legacy network services and directing them to BT as a single provider.

The project is a part of the organisation's 10-year strategy to improve policing in Scotland and forms part of its Digital, Data and ICT Strategy Martin Low, Interim Director of ICT Martin Low said: "Delivering new network services for Police Scotland will have a big impact on the working lives of our officers and staff and improvements to the network effectively underpin our programme of technology enabled transformation"

"NatNet2 will ease some of the frustrations colleagues feel about how our systems perform on a day-to-day basis."

David Wallace, director of BT's Enterprise division public sector business in Scotland and chair of BT's Scotland board, said: "We're proud of the part we're playing in transforming Police Scotland's computer network. We're helping to connect its offices the length and breadth of Scotland to faster, more reliable broadband. By making use of our extensive network, we know the faster speeds will be welcomed by police staff, especially in rural areas."

Officers involved in the pilot had previously reported struggling to upload files of any size, but under NatNet2 40mb files of video interviews are accessed in a few seconds.

Video conferencing is now accessible to many areas and officers who previously complained that simply logging on to a legacy system could take up to ten minutes, are now able to access the network in seconds.

Vehicle mounted net capture system will be launched at DSEI London 2019

OpenWorks Engineering is pleased to announce the release of the world's first vehicle mounted drone capture system, SkyWall Auto Response. The system provides security forces with a way of protecting a large area using the operationally proven SkyWall net capture technology, already deployed at critical national infrastructure around the world.

SkyWall Auto Response looks like any typical commercial vehicle at first sight as the drone capture system is hidden under rapidly deployable covers, ensuring the system remains discreet when not in use. When a drone threat has been detected, the vehicle can be manoeuvred quickly and the SkyWall net capture system is automatically deployed from under the cover.

OpenWorks expects the first operational deployments of SkyWall Auto Response to be in the coming months, as plans are already progressing and excitement in the end user community has been building over a considerable period. The system will be displayed in the outdoor space (next to Taylors Bar) at DSEI 2019 (10th – 13thSeptember), at the Excel Centre London, as the system is formally launched to the world.

Pelco Introduces Sarix Professional Series 3 Fixed IP Cameras

Pelco has released the Sarix Professional (Pro) Series 3 Fixed IP cameras. Offered in mini-dome, bullet, box, and wedge configurations, these IP cameras deliver a balanced set of features and performance at affordable price points that allow for deployment across a wide range of indoor and outdoor applications, including low light and wide dynamic range capabilities with options of 1MP, 2MP, 3MP, and 5MP resolutions.

Sarix Pro 3 cameras are ideal for industries such as Commercial, Government, Healthcare, and Education that demand a robust set of features, superior performance, and image clarity in an easily installed and maintained camera system.

"The Sarix Pro 3 IP Camera Series solves real security video challenges in a broad range of industries by providing more security detail in challenging scenes with excellent low light and wide dynamic range performance," said Kevin Saldanha, Principal Product Manager. "In Healthcare and Education verticals, where vandalism and bi-directional audio communication is required, this camera series has models with IK10 vandal resistance and built-in microphones that can meet those requirements seamlessly. For Commercial industry-related needs that require several hundreds to thousands of high-resolution cameras with 24/7 monitoring on a limited budget, the Sarix Pro 3 Series delivers cost-savings with less bandwidth and storage requirements supported by h.265 video encoding and Pelco Smart Compression," he concluded.

These cameras work with VideoXpert on both H.264/H.265 and with Endura and Digital Sentry along with VxToolbox. They are also ONVIF Profile S, G, Q, and T compliant and work with well with third-party video management systems that conform to these ONVIF Profiles.

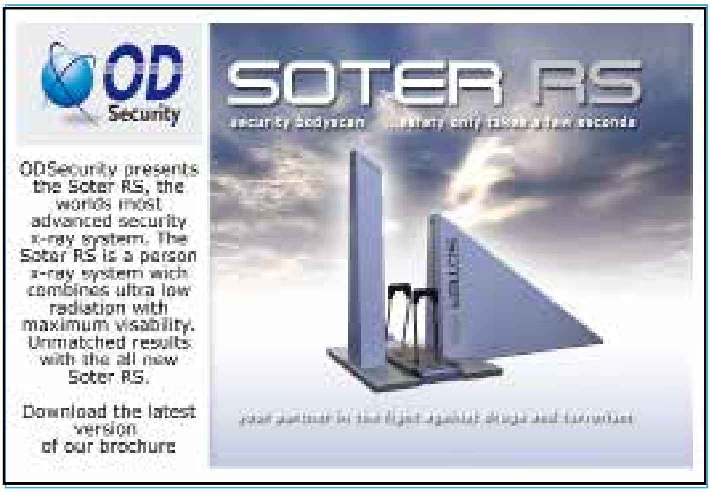
World Security Report

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 130,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, security and armed forces and civilian services and looks at how they are dealing with them. It aims to be a prime source of online information and analysis on security, counter-terrorism, international affairs and defence.

Clantect Ltd
Institute of Sound and Vibration Research
Southampton, SO17 1BJ, United Kingdom
Phone: +44 (0) 23 8055 0883
Email: info@clantect.com

Border Security Report

Border Security Report is the bi-monthly border management industry magazine delivering agency and industry news and developments, as well as more in-depth features and analysis to over 20,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.



ODSecurity presents the Soter RS, the worlds most advanced security x-ray system. The Soter RS is a person x-ray system wich combines ultra low radiation with maximum visability. Unmatched results with the all new Soter RS.

Download the latest version of our brochure

Wagtail International
leading specialists in detection dogs and dog handler training

Click here to view our profile

September 2019

10
Insider Threat Symposium
Laurel, Maryland, USA
www.nationalinsiderthreatsig.org

10-13
Defence & Security Equipment International (DSEI)
London, UK
www.dsei.co.uk

18-19
Dispax World
London, UK
www.unrulypax.com

22-24
AVSEC Global Symposium 2019
Dubai, UAE
www.emiratesgroupsecurity.com/events

24-26
Securex East Africa 2019
Nairobi, Kenya
www.securexpoeastafrica.com

October 2019

2-3
Finnsec
Helsinki, Finland
www.finnsec.messukeskus.com

9-10
Cyber Security Europe
London, UK
www.cybersecurity-europe.com

14-16
Critical Infrastructure Protection & Resilience Europe
Milan, Italy
www.cipre-expo.com

To have your event listed please email details to the editor tony.kingham@knmmedia.com

November 2019

20-21
International Safety & Security Aviation Conference
Prague, Czech Republic
www.safsecprague.cz/en

March 2020

March 31-2 April
World Border Security Congress
Athens, Greece
www.world-border-congress.com

April 2020

28-30
Critical Infrastructure Protection & Resilience North America
New Orleans, LA, USA
www.ciprna-expo.com

ADVERTISING SALES

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

For Rest of World contact:
E: marketing@knmmedia.com
T: +44 (0) 1273 931 593

Paul McPherson
(Americas)
E: paulm@torchmarketing.us
T: +1-240-463-1700

critical infrastructure
PROTECTION AND RESILIENCE AMERICAS

April 28th-30th, 2020
New Orleans, LA, USA

A Homeland Security Event

Are you sure your national infrastructure is secure?

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.

Call for Abstracts

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

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure.

The 3rd 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.

You are invited to submit an abstract for consideration for inclusion in the conference programme - visit www.ciprna-expo.com/call-for-papers for further details.

Join us in New Orleans, LA, USA for the premier event for operators and government establishments tasked with the regions Critical Infrastructure Protection and Resilience.

For further details visit www.ciprna-expo.com

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Critical Manufacturing Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
- Financial Services Sector
- Food and Agriculture Sector
- Government Facilities Sector
- Healthcare and Public Health Sector
- Information Technology Sector
- Nuclear Reactors, Materials, and Waste Sector
- Transportation Systems Sector
- Water and Wastewater Systems Sector

To discuss exhibiting and sponsorship opportunities contact:

Paul McPherson
(Americas)
E: paulm@torchmarketing.us
T: +1-240-463-1700

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

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

The premier discussion for securing America's critical infrastructure

Supporting Organisations:

International Association of CIP Professionals · NS&RG · IACI International Association of Certified ISAOs · ISIO · SPF

Media Partners:

WORLD SECURITY REPORT · World Security-index.com