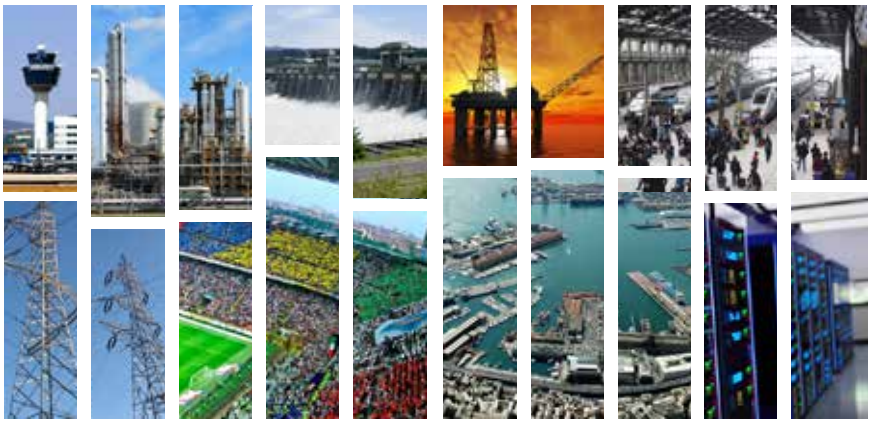
WORLD SECURITY REPORT

Official Magazine of

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

JULY / AUGUST 2019
www.worldsecurity-index.com

ARGONNE PARTNERS TO STRENGTHEN PUERTO RICAN INFRASTRUCTURE



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

Keynote Speakers include:

- Italian Critical Infrastructures Secretariat - Presidency of the Council of Ministers
- 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. Serkan Girgin, Scientific Officer, European Commission Joint Research Centre (JRC)

– Dr. Athanasios Sfetsos, Project Manager, EU Circle

– Massimo Rocca, Chairman, EE-ISAC

– Dr. Gordan Akrap, President, Hybrid Warfare Research Institute

– Prof. Roberto Setola, Complex Systems & Security Lab, Unicampus Rome

– Alberto Neri, RESISTO Project Leonardo Technical Coordinator – Cyber Security Division, Leonardo

– Fabio Panada, Senior Security Consultant, CISCO

– Gianluca Riglietti, Head of Research & Intelligence, Panta Ray

– 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

– Aman Panu, Vice President AD&S, Frost & Sullivan, UK

- Luca Boselli, Partner, KPMG Advisory, Italy

Leading the debate for securing Europe's critical infrastructure

Platinum Sponsor: KPMG

Bronze Sponsor: ABLOY

Supporting Organisations: AIIC, NSaRC, 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.14


» p.18

ARE WE TAKING THE THREAT TO CNI SERIOUSLY ENOUGH?

The growing crisis between Iran, the US and the UK continues to dominate the headlines from the Gulf, and with good reason, as each tit-for-tat incident has the potential to escalate the crisis into a shooting war, which the hawks in the US administration will see as the inevitable and long overdue conclusion.

But they should not underestimate the ability of Iran to defend itself and damage and disrupt the global economy. Simple geography means that Iran has the ability to plug the Gulf and deter any tankers from making the dangerous run through the Straits of Hormuz.

Iran has an arsenal of sophisticated weapons at their disposal, but they have also been developing and practising low tech attacks, such as fast attack boats, for years.

Whilst there is no doubt who would win a high intensity conflict, there is little the US could do to stop Iran disrupting the global oil trade, which is likely to be their main response.

This is evident from other events in the region that have not all made the headlines in the West, but may have a huge significance for the Gulf region and the wider world; a sustained attack by the Iran backed Houthi militia on many critical national infrastructure sites within Saudi Arabia and the UAE.

These events have included the use of scuba divers to attack four oil tankers in the Emirati port of Fujairah, which holed all four vessels, and drone attacks against the oil infrastructure in Saudi Arabia. There have also been repeated drone attacks on airports in the UAE and Saudi Arabia. These attacks, especially those against the Saudi airports have taken at least one life and injured many more.

However, the primary objective of these attacks was not to kill and maim. There are much more effective ways to do that. Instead, it is to demonstrate their capability to strike back against far more powerful adversaries, whilst damaging and disrupting their economies.

The Houthi's are armed and trained by the Islamic Revolutionary Guard Corps (IRGC), so it makes sense to assume that their tactics reflect thinking within the IRGC.

The influence of the Iranian's doesn't stop there. If you believe what you read online, the IRGC have links with the Japanese Red Army, the Armenian Secret Army, the Kurdistan Workers' Party, the Iraqi Da'wah Party, the Islamic Front for the Liberation of Bahrain, and of course Hezbollah and Hamas.

And finally, of course, there's ISIS. Whilst in theory Sunni terrorist group ISIS is the mortal enemy of Shia Iran, according to Israeli sources they are prepared to co-operate in places like Sinai, and who knows where else if it suits their purpose.

Physical attacks on CNI are real, they are happening and are only likely to increase. So, it is time to take the threat more seriously, not just in the Middle East, but everywhere!

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

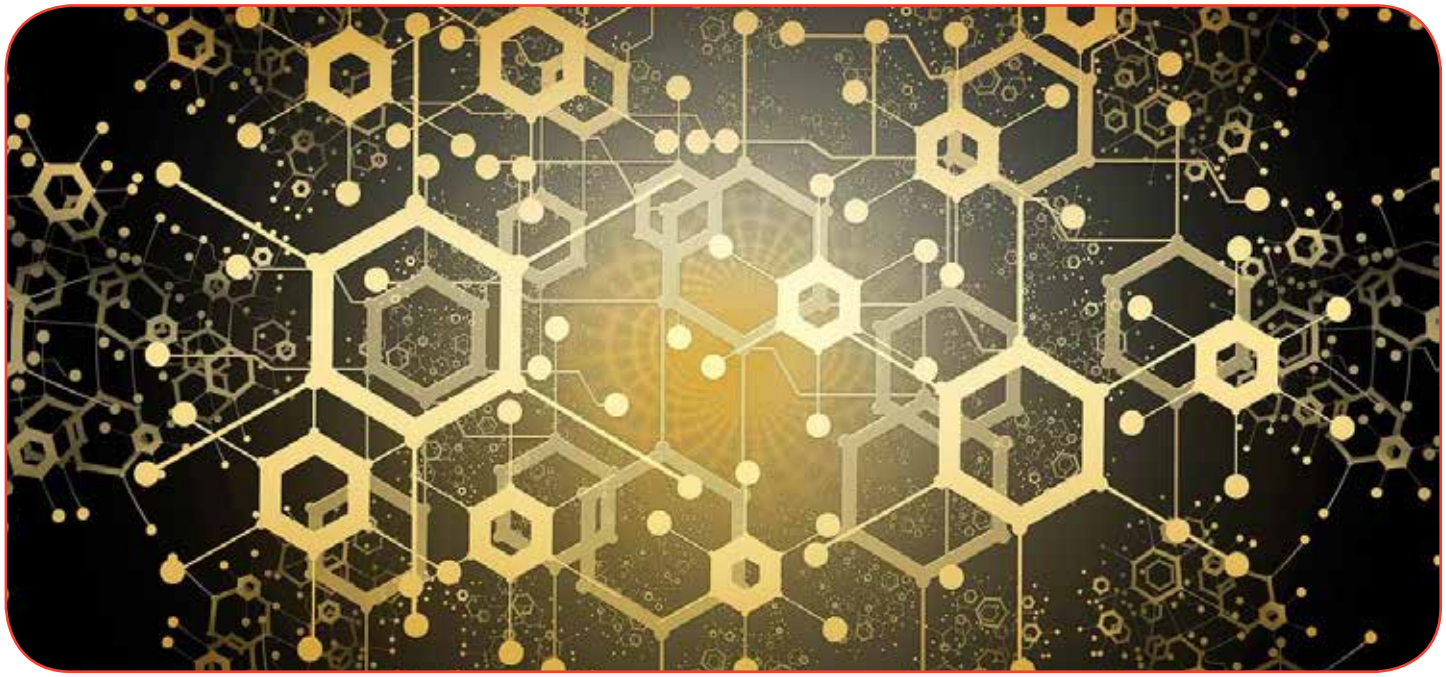
Features Editor:
Karen Kingham
E: karen.kingham@knmmedia.com

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.

US DHS S&T's Blockchain program focuses on security, privacy, interoperability & standards



There has been a lot of buzz lately about how Blockchain will revolutionize the secure transfer of information. However, many are still unclear on exactly what Blockchain is, where its applications can be used and how the leaders in the field will be able to deliver usable software to potential buyers.

As an emerging tech trend, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has been tracking Blockchain's birth, development and progress for years. S&T was particularly interested because of the potential for building resilience into digital transaction systems.

By understanding its potential applications and impact, and setting universal standards for usage, S&T is paving the way for multiple agencies such as U.S. Customs and Border Protection (CBP), U.S. Citizenship and Immigration Services (USCIS), Transportation Security Administration (TSA) and others to successfully and easily integrate Blockchain into their mission.

As the DHS science advisor, S&T prides itself on keeping its finger on the pulse of emerging technologies. When the assessment is made that the time is right, S&T may even offer assistance to industry to help the tech both achieve its full potential and reach perspective government buyers and users. That is exactly what happened with Blockchain.

What is Blockchain?

Blockchain first gained wide notoriety as the system that runs the Bitcoin digital currency transaction confirmation process.

What makes it so different from previous models is that each transaction of the digital monies forms a new "block" in a public ledger. The ledger is transparent and communally verifiable within

an open and shared database. As a shared, synchronized and geographically disbursed database, with no centralized data storage, the system is designed to remove the "single point of failure" risk (including technical malfunction and malicious alteration) that is present in many other systems.

One of the other key differentiators from previous structures is that since it is a "distributed electronic ledger," if one wants to track the historical transactions of a specific unit of currency (or data) from its introduction into the system until a specific date, that can be done and verified by multiple independent users. The blocks form an unbroken "chain" that acts as a visible digital paper trail.

So far, Blockchain has proven extremely resistant to any type of hacking or alteration, and that makes it especially attractive for Homeland Security Enterprise (HSE) uses.

SVIP and Blockchain

S&T's Silicon Valley Innovation Program (SVIP) bridges the public/private sector gap by cultivating relationships, advising and educating innovators on DHS needs and then offering opportunities to fund and test technologies.

According to Anil John, SVIP Technical Director, "About three years ago, we saw that the global interest in Blockchain technology was not matched by technical investments that ensured that the technology incorporated fundamental security, privacy and interoperability functions. In other words, while its capabilities could represent a dramatic change in the way that things will be done in the future, so much so that it could disrupt the current norms in multiple sectors, there were still missing links in the chain. That's when we offered our assistance."

And with that, S&T launched a program for Blockchain that focused on security, privacy and interoperability specifications and standards.

Although it may sound mundane at first, one of S&T's other lesser known roles within the HSE is to assist components and vendor partners with identifying, creating and setting standards for the technologies themselves.

By developing standardized specifications, S&T creates a common language and criteria for vendor and end-user, alike. This shared understanding facilitates seamless interoperability which enhances utility, efficiency and ultimately, mission success.

The goal of the Blockchain program was to further understand the technology's capabilities, and also to support and, as needed, create broadly accepted standards to benefit both government entities and the companies in the emerging sector.

By supporting a set of vetted standards, S&T enables government and non-government users to avoid spending additional time and money "re-creating the wheel" to build multiple new interfaces that connect with individual proprietary vendor tools.

John pointed out that, "Historically, when new technologies or solutions are incorporated into legacy systems, there are obstacles that create slowdowns as work-arounds are developed so that the systems mesh properly. However, through the use of globally acceptable and implemented specifications and standards, we are addressing and removing those interoperability hurdles before deployment. That way our industry partners and government components can hit the ground running."

This is important because multiple agencies can immediately benefit from the advantages of Blockchain.

Throughout the HSE, agencies issue entitlements, attestations and certifications. The holders of those credentials might be an individual, organization or product, but from the HSE perspective, they all have at least one thing in common—the documentation must be quickly verified, extremely robust and resistant to tampering. Paper-

based, manual verification solutions are slow, non-centralized and pose are greater risk of forgery and counterfeiting. Blockchain is tailor-made to address and mitigate these security and speed issues.

CBP and Blockchain

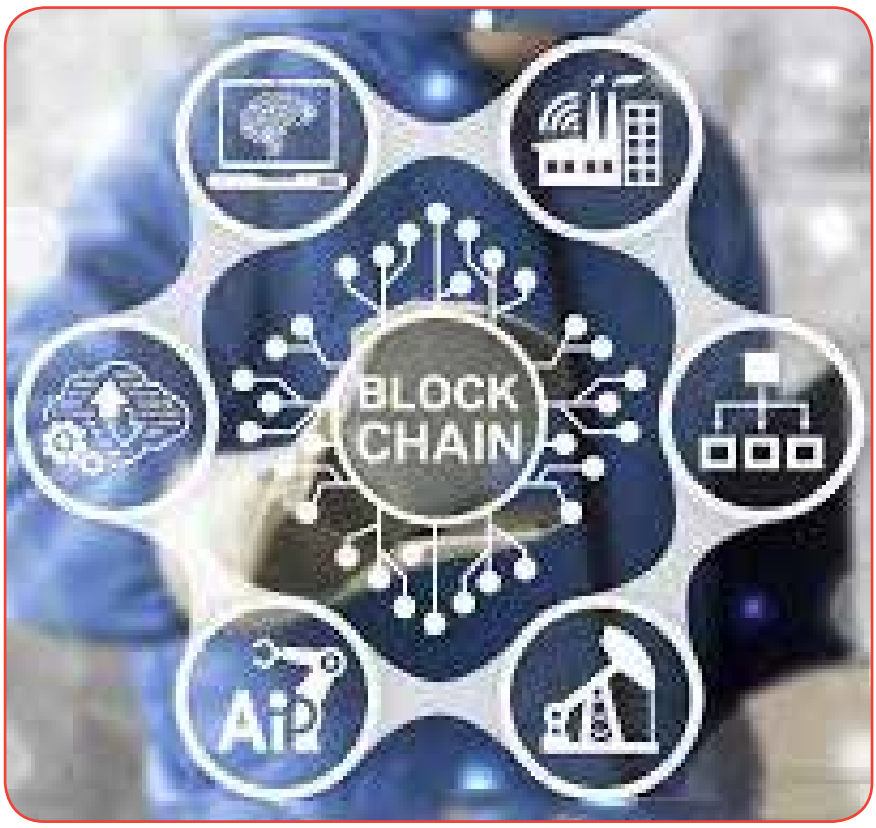
S&T first piloted Blockchain with CBP; the nation's leading law enforcement agency to facilitate lawful international trade across U.S borders. CBP has primary responsibility over the import/export supply chain (the system responsible for bringing a raw product or service to the end customer), verifying international treaty certifications and providing for the timely approval and movement of cargo.

John explained, "We are a support organization for components and their operators. CBP saw that we were ahead of the curve with our understanding of the Blockchain landscape, so they reached out to us. It's a great example, because their desires intersected with our knowledge."

The tracking and validation of goods, their elements and their origins throughout the entire supply chain for audit and compliance purposes, is extremely challenging. CBP was interested in updating the paper-based system that they had been using to verify and approve trade agreements.

They saw that Blockchain could enable stakeholders (broker, importer and government) to know instantly the status of import products. By adding a level of secure transparency to the supply chain, all involved parties would be able to track and verify each product from origin to destination.

"Blockchain and CBP's needs were an excellent match and the lessons learned in the pilot are being applied to additional agencies." said John.



Based on the success with CBP, additional DHS Components are starting to explore how Blockchain technologies could help with their missions. In particular, throughout the HSE, agencies such as USCIS issue entitlements, attestations and certifications. The holders of those credentials might be an individual, organization or product, but from the HSE perspective, they all have at least one thing in common—the documentation must be quickly verified, extremely robust and resistant to tampering. Paper-based, manual verification solutions at areas such as TSA checkpoints are non-centralized and pose are greater risk of forgery and counterfeiting. Blockchain is a potential solution that can address and mitigate these security and speed issues.

USCIS and Blockchain

USCIS is responsible for issuance of documentation proving citizenship, immigration and employment work-status authorization. They wanted to upgrade their existing manual system to be faster, more accurate and more secure.

"USCIS wanted a solution to reduce fraud in citizenship, immigration and authorization documentations. And that is exactly the type of functions where Blockchain excels." added John.

By working and partnering with SVIP to sponsor the "Preventing Forgeries of and Counterfeiting of Certificates and Licenses" Call, USCIS is seeking how Blockchain technologies can help secure and automate these processes, which translates into faster and more accurate verification.

TSA and Blockchain

The TSA is the lead organization responsible for the security of the travelling public. In that role, it is responsible for verifying that each passenger that interacts with a TSA checkpoint presents lawful and legitimate proof of identity that also matches them and their boarding pass. Currently, much of this verification is done

manually and by visual assessment. With Blockchain, passenger identification could be accelerated, and detection of fraudulent documentation enhanced.

"TSA is another great capability match," remarked John. "Blockchain is the infrastructure that supports the validation of credentials. Greater speed and accuracy at checkpoints means a better and safer traveler experience."

By partnering with SVIP to sponsor the "Preventing Forgeries of and Counterfeiting of Certificates and Licenses" Call, TSA is seeking how Blockchain technologies can help secure, automate and speed up the credential validation processes at checkpoints.

S&T, SVIP, Blockchain and the Future

S&T is taking the lead in developing the processes for the use of Blockchain. This work will accelerate the development and deployment of this important technology throughout the HSE and other government agencies. By modernizing these systems, Blockchain will save time, money and reduce fraud.

Development of standards enables a robust and competitive marketplace for Blockchain uses that will benefit both the government clients and the private sector industry manufacturers and sellers.

Meanwhile, S&T SVIP is continuing to fund and explore new ways to facilitate the speedy and secure transfer of authenticated data and the verification of documentation to secure trade, travel and ultimately, the country.

"The work we're doing with Blockchain will enable the HSE to execute its mission more efficiently. By automating a multitude of time-consuming tasks, agents will be freed to focus on other areas of trade, travel and security," said John, "The program's success will serve as the foundation of our 'whole of government' approach to Blockchain in the future."

Source: US Department of Homeland Security - Science and Technology Directorate

Argonne partners to strengthen Puerto Rican infrastructure

Argonne researchers have helped Puerto Rico's long-term recovery by bolstering the planning for its critical infrastructure systems. By Brett Hansard

Lawrence Paul Lewis, upon his arrival to Puerto Rico in June 2017, recognized the same culture and vibrancy that he knew from New Orleans, where he had lived and studied for many years.

"My first reaction was that there was something so comfortable and familiar about it," he said.

Lewis, the program lead for technology implementation in the Decision and Infrastructure Sciences (DIS) division at the U.S. Department of Energy's (DOE) Argonne National Laboratory, was in Puerto Rico to lead a Regional Resiliency Assessment Program (RRAP) project for the Department of Homeland Security (DHS) Office of Infrastructure Protection (IP).

Argonne had been conducting resiliency studies for DHS since 2009, and this one was supposed to examine the strength of regional freight networks between Continental U.S. ports and the Caribbean.

But then came Hurricane Maria, directly on the heels of Hurricane Irma.

When Maria struck Puerto Rico on September 20, 2017, it was a high-end Category 4 hurricane, the most powerful and deadliest storm of the year.

Quickly shifting gears, DHS-IP asked Argonne to instead support the Federal Emergency Management Agency (FEMA) with long-term recovery planning for critical infrastructure systems, such as energy, water, communications and transportation.

Lewis, who had survived hurricane Katrina years earlier, returned to Puerto Rico in November 2017with a new focus – and a painful sense of déjà vu.

"It was heartbreaking," he said. "It reminded me of New

World Border Security Congress

March 31st-2nd April 2020

ATHENS, GREECE

www.world-border-congress.com

Building Trust and Co-operation through Discussion and Dialogue

REGISTRATION NOW OPEN

REGISTER FOR YOUR DELEGATE PASS ONLINE TODAY

Greece lies at the crossroads of East and West, Europe and the Middle East. It lies directly opposite Libya so along with Italy is the primary destination for migrants coming from that conflict zone and is a short boat trip from Turkey, the other principal migrant route for Syrians fleeing there conflict there.

Greece has over sixteen thousand kilometres of coastline and six thousand islands, only two hundred and twenty-seven of which are inhabited. The islands alone have 7,500 km of coastline and are spread mainly through the Aegean and the Ionian Seas, making maritime security incredibly challenging.

The sheer scale of the migrant crisis in late 2015 early 2016 had a devasting impact on Greek finances and its principle industry, tourism. All this in the aftermath of the financial crisis in 2009. Despite this, both Greece and Italy, largely left to handle the crisis on their own, managed the crisis with commendable determination and humanity.

With their experience of being in the frontline of the migration crisis, Greece is the perfect place re-convene for the next meeting of the World Border Security Congress.

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

The World Border Security Congress Committee invite you to join the international border security and management community and Apply for your Delegate Pass at **www.world-border-congress.com.**

We look forward to welcoming you to Athens, Greece on March 31st-2nd April 2020 for the next gathering of border and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

To discuss exhibiting and sponsorship opportunities and your involvement please contact:

Paul Gloc
UK & Rest of Europe
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

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

Supported by:

OSCE Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

AFRICAN UNION

ISIO

NSeRC

Media Partners:

BORDER SECURITY REPORT

WORLD SECURITY REPORT

World Security-index.com

Argonne's Paul Lewis, Duane Verner and Leslie-Anne Levy relied on this new tool to find the ideal dependencies and interdependencies for Puerto Rico's grid network.

Orleans."

Identifying Puerto Rico's infrastructure needs

In the aftermath of Maria, the challenges in Puerto Rico were immense. In July 2018, Governor Ricardo Rosselló Nevares released a draft "Economic and Disaster Recovery Plan for Puerto Rico" in which he said "emergency services were severely compromised and residents lacked electricity, food and water for a prolonged period."

Roads were impassable, residents had limited access to medical care, schools shuttered, government services and private enterprise could no longer operate effectively, landslides caused flooding hazards and wastewater polluted marine environments, he said.

Arriving in November at the Joint Field Office in San Juan – the hub of local, state and federal multi-agency coordination – Lewis joined with DHS-IP staff to brief the leadership from Puerto Rico and FEMA on how recovery investments could be targeted and prioritized.

"Recovery has always had a reactive posture, and we wanted to be more proactive with our approach," he said.

Together, they identified the "sweet spots" where investing money would make infrastructure more resilient – and efficient.

As an example, Lewis pointed to voltage instability, which occurs when demands for electrical power exceed the capability of generation and transmission, causing extremely low voltages. Even before the storms this was a massive problem in Puerto Rico.

For a critical industry like pharmaceutical manufacturing, which drives 30 percent of the state's economy, losing a batch of medicine during a power outage is a major loss. Addressing the voltage instability would not only have a positive impact on the pharmaceutical industry but on water filtration and cell towers as well, making it an appealing choice, he said.

Disaster managers gave the green light for a six-week pilot project in Manatí, a mid-sized municipality on the island's northern coast. The goal was to test the methodology by identifying critical manufacturing facilities and analyzing their dependencies on lifeline infrastructure systems – and then recommending strategies for investment. State and federal officials soon asked for ways in which the methodology could be expanded to other parts of the island.

The next phase of the project began in January 2018 and with it, an opportunity to take almost a decade's worth of knowledge and put it to work in support of Puerto Rico's recovery.

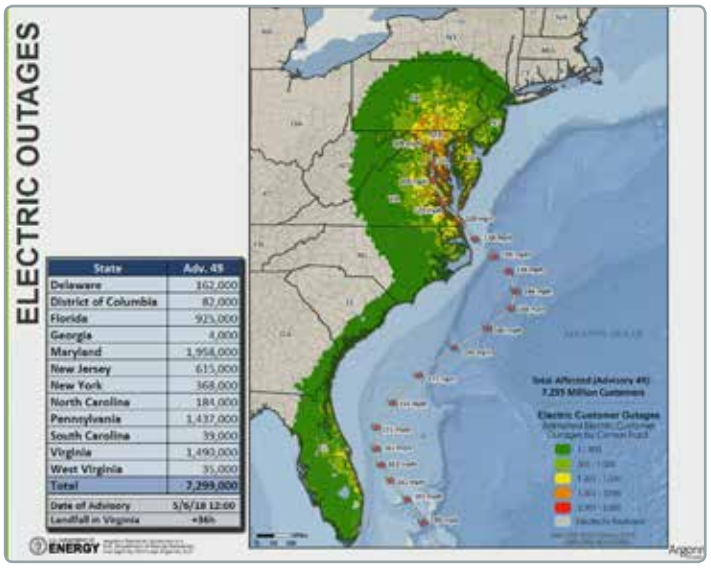
Flipping the framework

Duane Verner is the Resilience Assessment Group Leader in the DIS division at Argonne, and he has been involved with the RRAP since its inception. The program relies upon a "Regional Resiliency Assessment Program Dependency Analysis Framework," written in part by Verner, to provide a common understanding and consistent analytic approach.

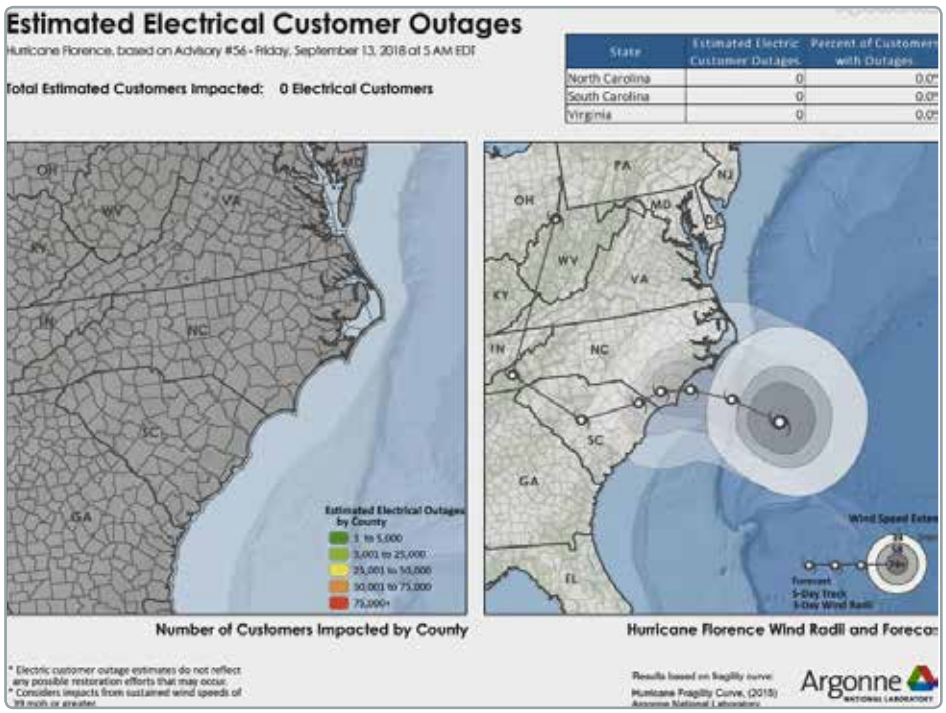
According to Verner, the framework was "flipped on its head" in Puerto Rico. In a typical RRAP, the framework is used to examine the consequences of a particular event occurring. For Puerto Rico, it became a planning tool to understand how to build back the island in a more resilient manner.

"We are using the framework to understand the links and nodes, the dependencies of systems and the interdependencies among systems, bringing to bear a decade's worth of knowledge in this area," Verner said.

In expanding to other parts of the island in this next phase, FEMA asked DHS-IP to perform interdependency assessments in support of long-term economic recovery. Of particular interest were key industrial sectors, such as critical manufacturing, food distribution and maritime port capacity.



This shows a simulation of the faux Hurricane Cora's trajectory and potential electrical outages. This was not a real hurricane and was created for training and research purposes.



This shows Argonne's predictions of Hurricane Florence's trajectory and electric outages in September 2018.

Lewis and his multi-disciplinary team included engineers, economists, GIS analysts, political scientists and IT specialists from Argonne, as well as additional support from DOE's Idaho National Laboratory – totaling more than a dozen people.

Working under the direction of DHS-IP, they helped assess 57 critical manufacturing facilities and industrial assets as part of this process.

According to Lewis, the biggest challenge was to manage the data, understand it and make meaningful use of it – while also protecting sensitive information.

A new web-based data collection and management architecture – the Puerto Rico Infrastructure Interdependency Assessment (PRIIA) toolset – was developed to assess and visualize first- and second-order dependencies and interdependencies and frame key findings for stakeholder consideration.

Earlier this year, DHS-IP released the "Puerto Rico Infrastructure Interdependency Assessment," summarizing its activities from November 2017 through May 2018 and highlighting the importance of understanding infrastructure interdependencies as part of long-term recovery planning.

In addition to Lewis' group, another team at Argonne was asked by DOE to lead the development of modeling tools and analysis spanning five National Laboratories to support Puerto Rico in planning a more resilient electric grid. Their work included a delegation of National Laboratory researchers providing training and technical assistance for Puerto Rico's public utility employees during a series of multi-day working sessions in June and October, and the team continues to contribute to local and federal grid recovery efforts in Puerto Rico. Their work is helping inform solutions to challenges facing critical industries like those identified through Argonne's infrastructure interdependency assessments.

This shows a simulation of the faux Hurricane Cora's trajectory and potential electrical outages. This was not a real hurricane and was created for training and research purposes. (Simulation by Argonne National Laboratory.)

Taking the long view

The report was shared with senior federal officials managing recovery operations in Puerto Rico, and key material about infrastructure interconnectedness was included in the commonwealth governor's economic and disaster recovery plan, which pegged the total costs of the island's long-term rebuilding at $125 billion.

DHS-IP is currently coordinating with FEMA to identify which potential projects identified in the assessment to undertake.

"DHS-IP is one of the leading voices for dependencies and interdependencies in the country," said Leslie-Anne Levy, who leads the DIS Infrastructure Security and Risk Analytics Group and co-manages the RRAP portfolio with Verner. "Drawing connections among infrastructure systems allows recovery managers to see the forest for the trees, to understand their interplay."

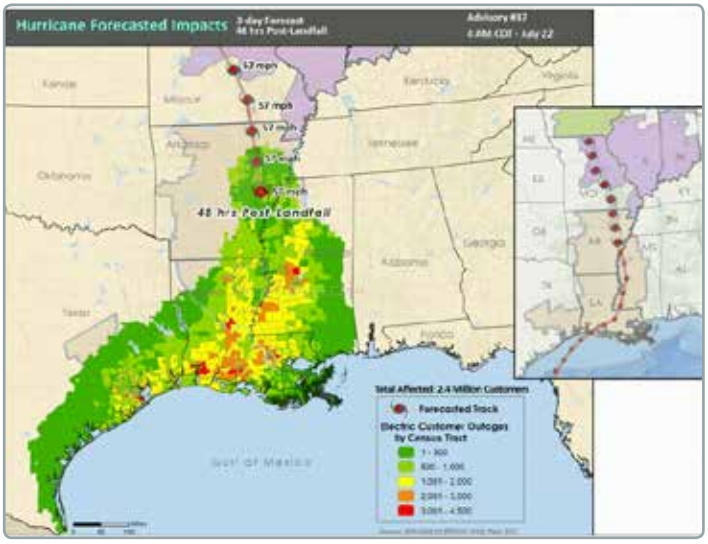
Argonne will continue to support Puerto Rico recovery efforts at least through the spring of 2019. In the coming months, DHS-IP is also looking to extend its work with Argonne to the U.S. Virgin Islands, and apply the toolkit to broader Caribbean infrastructure resilience.

"We are looking to help develop a capability that can be deployed whenever infrastructure dependency is a pressing question," Lewis said. "Resilience is not something you accomplish, it's something you practice. You have to constantly adjust."

The road to rebuilding and recovery

After having supported the recovery in Puerto Rico for more than a year, Lewis, perhaps as much as anyone, understands how much work still remains.

Katrina left New Orleans nearly unrecognizable, he said. Lewis, then a law student at Tulane University, lost everything he didn't



This shows an Argonne-developed hurricane scenario that affects electricity along the Texas and Louisiana coast. This is part of a training session for the Midcontinent Independent System Operator organization.

leave with during the evacuation. It took him years to rebuild and recover.

The storm changed his life and his career path: Rather than take a job in international law as he had initially planned, he instead completed his degree and enrolled in the Master of Science in Threat and Response Management at the University of Chicago, where he now teaches. He joined Argonne in 2010.

"There's not a day that goes by that I don't think about Katrina," he said. "It is why I do what I do."

This summer, Lewis was one of only 23 people across the entire DOE Complex to be recognized by the prestigious Secretary's Awards Program. (Separate awards were also given to Argonne's Linda Hansen, a principal nonproliferation policy analyst in the Strategic Security Sciences Division, and the Argonne team from the Joint Center for Energy Storage Research.)

"To do an interdependency project effectively requires a lot of expertise," Lewis said. "So many people at Argonne were part of this. The validity and reliability of the methods and results are only possible with the diversity of the team we have here."

Argonne National Laboratory seeks solutions to pressing national problems in science and technology. The nation's first national laboratory, Argonne conducts leading-edge basic and applied scientific research in virtually every scientific discipline. Argonne researchers work closely with researchers from hundreds of companies, universities, and federal, state and municipal agencies to help them solve their specific problems, advance America's scientific leadership and prepare the nation for a better future. With employees from more than 60 nations, Argonne is managed by UChicago Argonne, LLC for the U.S. Department of Energy's Office of Science.

The U.S. Department of Energy's Office of Science is the single largest supporter of basic research in the physical sciences in the United States and is working to address some of the most pressing challenges of our time. For more information, visit https://energy.gov/science.

Contraband Crisis in Department of Corrections

"South Carolina Department Of Corrections is Facing a Crisis in Contraband" - Says United States Attorney District of South Carolina, Beth Drake

In April, 2019 United States Attorney Beth Drake announced the indictment and arrest of fourteen former employees of the South Carolina Department of Corrections (SCDC) on federal charges related to accepting bribes and bringing contraband into South Carolina prisons.

Since 2016, the Federal Bureau of Investigation (FBI) has partnered with state law enforcement to investigate the smuggling of contraband into prisons by staff at SCDC. The investigation uncovered a number of SCDC employees who accepted bribes to smuggle into prison various contraband, such as cell phones, narcotics, or tobacco.

July 15th, 2019 a former South Carolina prison guard who was paid $1000 by an inmate to bring a package of drugs containing 86 grams of methamphetamine, 408 grams of marijuana, blunt wraps and cigars into the facility is now an inmate herself!

Janean Lateefah Dunbar, 41, was found guilty by a jury on charges of possession with intent to distribute marijuana, furnishing contraband to an inmate and misconduct in office. She was sentenced to 10 years, suspended to service of six years and five years' probation.

This was one of the longest sentences imposed on a corrections officer in recent years, according to the Department of Corrections.

"I'd like to thank Solicitor Rick Hubbard and his team for prosecuting this very serious matter," corrections director Bryan Stirling said in the release. "Anytime someone brings contraband into an institution and breaks the public trust, there needs to be consequences."

Cyber strategy update shows how UK intelligence is thwarting attack

The NCSC's Active Cyber Defence report for 2019 has been published.

A scam to defraud thousands of UK citizens using a fake email address spoofing a UK airport was one of a wide range of cyber-attacks successfully prevented by the National Cyber Security Centre (NCSC), a report revealed today (Tuesday 16th July).

Details of the criminal campaign are just one case study of many in Active Cyber Defence – The Second Year, the latest comprehensive analysis of the NCSC's world-leading programme to protect the UK from cyber-attacks.

The thwarting of the airport scam was one example in 2018 of how ACD protects the public – in this case preventing potentially thousands of people ending up out of pocket.

The incident occurred last August when criminals tried to send in excess of 200,000 emails purporting to be from a UK airport and using a non-existent gov.uk address in a bid to defraud people.

However, the emails never reached the intended recipients' inboxes because the NCSC's ACD system automatically detected the suspicious domain name and the recipient's mail providers never delivered the spoof messages. The real email account used by the criminals to communicate with victims was also taken down.

A combination of ACD services has helped HMRC's own efforts in massively reducing the criminal use of their brand. HMRC was the 16th most phished brand globally in 2016, but by the end of 2018 it was 146th in the world.

Dr Ian Levy, the NCSC's Technical

Director and author of the ACD report, said:

"These are just two examples of the value of ACD – they protected thousands of UK citizens and further reduced the criminal utility of UK brands. Concerted effort can dissuade criminals and protect UK citizens.

"While this and other successes are encouraging, we know there is more to do, and we would welcome partnerships with people and organisations who wish to contribute to the ACD ecosystem so that together we can further protect UK citizens.

"This second comprehensive analysis we have undertaken of the programme shows that this bold approach to preventing cyber-attacks is continuing to deliver for the British public."

Introduced by the NCSC in 2016, ACD is a bold, interventionist approach that stops millions of cyber-attacks from ever happening. It includes the pioneering programmes Web Check, DMARC, Public Sector DNS and a takedown service.

The ACD technology, which is free at the point of use, intends to protect the majority of the UK from the majority of the harm from the majority of the attacks the majority of the time.

Other key findings for 2018 from the second ACD report include:

• In 2018 the NCSC took down 22,133 phishing campaigns hosted in UK delegated IP space, totalling 142,203 individual attacks;

• 14,124 UK government-related phishing sites were removed;

• Thanks to ACD the number of phishing campaigns against HMRC continues to fall dramatically – with campaigns spoofing HMRC falling from 2,466 in 2017 to 1,332 in 2018. These figures relate to 16,064 spoof sites in 2017 and 6,752 sites in 2018;

• The total number of takedowns of fraudulent websites was 192,256, and across 2018, with 64% of them down in 24 hours;

• The number of individual web checks run has increased almost 100-fold, and we issued a total of 111,853 advisories direct to users in 2018.

Chancellor of the Duchy of Lancaster and Minister for the Cabinet Office David Lidington said:

"The UK is safer since the launch of our cyber strategy in 2016. Over the last three years, and backed by a £1.9 billion investment, we have revolutionised the UK's fight against cyber threats as part of an ambitious programme of action.

"The statistics and examples in this report speak for themselves. They outline the tangible impact that Active Cyber Defence is having, and how it is a key building block in improving cyber security in the UK now, and in the future."

The new report also looks to the future of ACD, highlighting a number of areas in development. These include:

• The work between the NCSC and Action Fraud to design and build a new automated system which allows the public to report suspicious emails easily. The NCSC aims to launch this system to the public later in 2019;

• The development of the NCSC Internet Weather Centre, which will aim to draw on multiple data sources to allow us to really understand the digital landscape of the UK;

• We'll explore developing an Infrastructure Check service: a web-based tool to help public sector and critical national infrastructure providers scan their internet-connected infrastructure for vulnerabilities;

• NCSC researchers have begun exploring additional ways to use the data created as part of the normal operation of the public sector protective DNS service to help our users better understand and protect the technologies in use on their networks.

Active Cyber Defence - The Second Year

You can read the full 2019 report at https://www.ncsc.gov.uk/report/active-cyber-defence-report-2019.

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

I recently read a very good article on the history of suicide terrorism within the aviation industry and how targeting has evolved from terrorists smuggling bombs onto planes, to using aircraft as a missile, to gun and explosives attacks in the public areas of airports.

It is 25 years (19th July 1994) since Alas Chiricanas flight 901 exploded in mid-air after departing from Colon City, Panama, on route to Panama City killing all 21 people on board. The U.S. Federal Bureau of Investigation (FBI) named and blamed a passenger for carrying the explosive on-board and he is believed to have detonated the device in the cabin. This would, by many, be regarded as the first suicidal attack against civil aviation perpetrated as a terrorist act.

The threat landscape to our transportation systems is fluid and constantly changing; it is only limited by the imagination of those who wish to cause us harm or indeed those who seek to profit from attacking this sector of our infrastructure.

As soon as we think we have a good understanding of the threats that we may face and have put what are believed to be sufficient mitigation measures in place, the odds are that they are already out of date or methodologies are being designed to circumvent them.

As we all know, the use of suicide terrorism through the 1990s and its increasing influence since 11th September 2001 has created a plethora of problems when considering the appropriate security regimes to have in place at our airports and on our airplanes.

Experience, both good and bad, has shown that effective aviation security, in simple terms, is all about the considerations of a layered approach. It starts with intelligence and analysis of data then moves into detection techniques within the airport environment and has additional layers built in with security interventions, police patrols and other associated activities. Other areas which focus on people, rather than things, have gathered momentum over the past few years, such as behavioural analysis of individuals throughout their journey and towards airport staff and contractors to help identify any insider threat.

These are all well tried and tested procedures, some more so than others, but all have a part to play in attempting to keep people safe. However, we all have to continue to invest in new innovation, to try new techniques and technologies and keep pace with the pressure that comes with aviation continuing to be an attractive target for terrorist groups and with it being a growth industry, where rising passenger numbers threaten to outstrip the growth in airport capacity.

The IACIPP Poll

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

Q. What are the top 2 areas of training you think the industry needs in the next 12 months?

- Cyber security - 33%
- Risk, Crisis & Emergency Management - 29%
- Preparedness for Disasters - 17%
- Terrorism Awareness - 10%
- Identification of Threats and Hazards - 8%
- Behavioural analysis - 6%
- CBRNe - 2%

Now give your opinion on the latest Poll

Where do you see your next major security threat?

- Insider Threat
- Terrorist attack
- Man Made / Ineptitude
- Natural Disaster
- CBRNE threat
- Cyber attack

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

Success, as always, will depend on both the public and private sector continuing to work together and here at the International Association of Critical Infrastructure Protection Professionals (IACIPP) we try to support that effort wherever we can. Our primary purpose is to provide a platform to share ideas, information, innovation, experiences, technology and best practise. We have a network of like-minded people who have the knowledge, experience, skill and determination to contribute to the reduction of vulnerabilities and seek to increase the resilience of Critical Infrastructure and Information.

We also have a great new website that offers a Members Portal for information sharing and connecting with other professionals and have recently introduced discussion forums, one of which is focused on the Transportation Sector and looks to share those new ideas and innovations as mentioned above.

Membership is currently FREE to qualifying individuals and if you are interested in joining us - see www.cip-association.org/join for more details.

Don't forget, October 14th-16th see's IACIPP supporting Critical Infrastructure Protection & Resilience Europe, being co-hosted by the Lombardia Regional Government and held at the excellent Auditorium of the Regional Government Administration Buildings.

There is an outstanding line up of international expert speakers sharing their experiences and knowledge, as well as a great opportunty to network with like minded colleagues from across CI industries. Registration is open at www.cipre-expo.com and as an IACIPP members you may be entitled to a Complimentary Delegate Pass - ensure you apply before 14th September to qualify.

We hope to see you there.

John Donlon QPM FSyl

Chairman IACIPP

International Association of CIP Professionals

Minister Publishes Review of the UK Search and Rescue Helicopter Service

Nusrat Ghani MP, Parliamentary Under Secretary of State for Transport has published the independent review of the UK Search and Rescue Helicopter Service.

"I am delighted to publish this independently produced post-implementation review of the UK search and rescue helicopter service. The service has been in place since 2015 and in that time, has been responsible for the rescue of thousands of lives. As Minister responsible for the service, I am proud of the work of our helicopter crews who routinely put their own lives at risk to rescue others."

"I recognise the high expectations the public has for this service, particularly given the fact that it replaced the much respected military sea king service. I equally recognise the degree to which our stakeholders in the emergency services and the volunteer rescue organisations value our search and rescue helicopters and how critical it is to enable those services to undertake their lifesaving work."

"To assure itself that the UK search and rescue helicopter service is meeting our stakeholders' needs and to evaluate the impact the service has had on the ability to respond to people in distress, the MCA commissioned this review to evaluate the work of the UK search and rescue helicopter service since it has been in operation."

"The review draws upon statistical data and insight from partner rescue organisations to reach its conclusions. The general opinion of the review is that the transition to the UK search and rescue helicopter service was successful. It concludes that the anticipated benefits are either met or on track to be met. It further identifies a number of unanticipated benefits that present opportunities for the future to grow the service to be offer even greater value for money to the public."

"This review will be used to inform the government's plans for the next generation search and rescue aviation capability, work on which has now started."

Assessing Modern Threats and Vulnerabilities in the Sports Landscape

In 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.

Arenas and stadiums, as a subsector of commercial facilities, are vulnerable to a wide array of threats. As technological capabilities continue to expand in stadiums, the significance of protecting this subsector of critical infrastructure also continues to magnify. Both cyber and physical dependencies are present in the operational functions of sporting stadiums and are vulnerable to potential disruptions. The incapacitation of the networks and systems can cause a cascading effect on functionality and overall safety within stadiums, as operations, security, and physical safety all have a direct correlation to the cyber capabilities within a facility. Consequently, the development and implementation of standardizations through risk assesments, with the inclusion of cyber modules, has the potential to reduce the risks of cyberattacks and would help to protect this subsector from the potentially devastating effects of such attacks.

Perimeter security, surveillance, and communications are forms of critical infrastructure protection for stadiums which may depend on cyber capabilities within these facilities. Emergency preparedness needs to continuously include the development of cyber resiliency capabilities to bridge the gaps in overall security for public venues such as stadiums, which remain vulnerable to a growing number of cyber threats. Malicious actors, all with various motivational factors, can potentially gain remote access to such systems as access control, HVAC, communication systems providing visualization cues, cameras, lighting, power, or fire suppression systems within a stadium or arena. During large-scale events such as the Super Bowl, command centers can also become vulnerable to potential cyberattacks. Through the development and deployment of the Sports and Entertainment Risk Assessment tool, the identification of hazards and risk factors can be reflective

of the modern day capabilities within venues, leading to a more proper resilience plan against physical and cyber threats. The analysis and evaluation of identified risks throughout these commercial entities is vital to the operational success of stadiums and arenas.

I. Historical

While not directly associated with having an impact on a particular sporting event or venue, the incident in Dallas, Texas in 2017, wherein hackers turned on 156 emergency sirens, highlights the gaps in security as well as potential capabilities of adversaries or someone trying to cause disruption on a grand scale. Around midnight in April of 2017, all of Dallas's emergency alarm systems went off at the hands of hackers. Though the hacker was allegedly local and the motive allegedly a prank with no further intentions, the incident negatively affected the response times of emergency services. The volume of 911 calls spiked, and callers with unrelated, actual emergencies may not have been able to get through to an operator. The largest influx of calls came between midnight and 12:15am, as 800 incoming calls caused wait times to leap to six minutes, far exceeding the city's goal of answering ninety percent of emergency calls within ten seconds. While this incident did not directly associate with a particular sporting event or venue, it lit a fuse within the city to taking a conscience effort to increasing cybersecurity practices regarding technology infrastructure.

In 2018, a non-credentialed Houston Astros employee was removed from Fenway Park during a Major League Baseball playoff game after he was seen with a camera and continuously texting behind the Boston Red Sox dugout. The man claimed to be a Houston Astros employee but failed to display proper media credentialing. He was eventually let back in to the stadium, but not in to the credentialed area. This event brings attention to the lack of implemented access control measures by the venue and security personnel. Access control measures not only include proper credentialing and access, but the surveillance of those credentials as well. While this incident was more of a misunderstanding, had this individual had malicious intentions, he could have gained access to critical components or systems within the venue before being removed.

Electronic traffic signs were hacked in another Dallas incident, depicting various messages, tampering with transportation communication equipment. With the heavy dependency that venues or large sporting-event have on traffic management, exposing vulnerabilities of such tools and devices can lead to harm and commotion. Thus, proper monitoring of external systems can be beneficial.

In 2014, in a television piece by CBS about security and private wireless capabilities, the network accidentally broadcasted the Wi-Fi password of the operations center of MetLife Stadium to all those watching. The credentials of a private, in-stadium Wi-Fi network was exposed to millions of television watchers just before the National Football League Super Bowl. Following this broadcast, the ID and password broke on to Twitter, which could have potentially led to someone inside the stadium gaining access to the private network. While the accident did not lead to any known detrimental impacts that they were aware of, it shows how easily a cyber incident could occur. There were no bad intentions in this occurrence, but rather an error in broadcasting judgement (potentially negligence); however, it could be a vastly different scenario should an adversary gain the ability to broadcast the private password of a stadium or arena publically. Venues need to identify protocols and procedures to mitigate vulnerabilities for potentially similar incidents.

Another situation involved Charter Spectrum, the second largest cable TV and Internet supplier of its time in the United States. Charter Spectrum encouraged enthusiasts of the Super Bowl to change their passwords to support who they were cheering for. 'GO_NEWENGLAND' or GO_ATLANTA' could have been some very popular passwords to guess leading up to Super Bowl in 2017. Cyberattacks are often associated with a talented group of ill-intended adversaries, but this case highlights that all it takes is an ill-advised suggestion getting into the wrong hands. There is such a varying level of cybersecurity threats, all which would benefit from some level of assessment and an overall implementation of mitigation protocol.

II. How to Assess

With a lack of standardizations in place to comply with policies and procedures for specific commercial sectors, there comes the issue of completing a risk assessment to raise awareness or mitigate any vulnerabilities that

could cause potential harm to various venues. To add complexity, stadiums and arenas are often selected to host large sporting events such as the Super Bowl, wherein a number of jurisdictions and entities all play an active role in the safety and security of the event. An explicit plan for all roles and responsibilities of participating agencies would be beneficial for incident response rates. Emergency response plans cannot be limited to physical aspects; cybersecurity requires insertion and proper planning. Cyber emergencies also have the potential to lead to physical and structural damages.

How to conduct an assessment on a stadium or arena has not been comparatively calibrated or standardly deployed. Many dynamic factors are applicable to a wide array of venues within the subsector of commercial facilities. Varying factors that can influence venue operational security include: locality, criticality of systematic infrastructure, reliance upon information technology, surveillance and monitoring, physical security and detection, and ingress and egress protocols. How security protocols are implemented prior, during, and following an event will be unique to individual entities. Exercises and drills should also be considered, not only to include physically motivated tabletops or functional exercises but cyber aspects as well. Technological staff can play a dynamic role in the preparation aspects of emergency planning. With how intricately technology is intertwined within stadiums and arenas, the security and functionality of networks and systems can be the cyber barricades against attacks from adversaries.

The Department of Homeland Security does offer a variety of publications specific to the Commercial Facilities Sector, including planning guides for stadiums and major events. Evacuation guides for stadiums provide direction for preparing for and responding to the potential need for an evacuation, with the inclusion of a template which can help with creating and implementing this plan. The Protective Measures Guides focuses on managing security protocols at facilities, including sports venue credentialing, bag searches, and patron screenings. There is also a voluntary Framework released from The National Institute of Standards and Technology (NIST), to provide entities such as venues, with how to assess and manage their cybersecurity risks. The Cybersecurity Framework assists organizations to not only gain a deeper understanding of their current cybersecurity assets and risks, but then how to manage the risks which can be associated with these cyber capabilities. The Framework is flexible enough to accommodate varying levels of sports sectors. There are currently no other tools or guidelines like this pertaining to the commercial sector. The reality is that stadiums and venues throughout the country remain a prevalent and exposed target for adversaries, both physically and from a cybersecurity standpoint. Guidelines and assessments are meant to provide direction as well as a baseline of potential risks and vulnerabilities that can occur. The National Infrastructure Protection Plan Commercial Facilities Sector-Specific Plan also works to improve the protection of facilities in an all-hazards environment. The Plan provides insight in to the process of identifying, assessing, and protecting the sector, to promote a collaborative approach to assessing risk and implementing protective programs. This allows various entities to identify assets which require further analysis in regards to criticality and current vulnerabilities. The associated vulnerabilities with cyber

systems remains a prevalent security concern. What is key to this plan is the measurement of progress step, which fosters the development of relationships amongst a vast array of public and private sectors. So while each sports venue is diverse in capabilities and vulnerabilities, all can benefit from establishing a basis for information sharing.

Furthermore, as a result of a collaborative effort between DHS, the National Cybersecurity and Communications Integration Center (NCCIC), and the Stadium Best Practices Working Group, a guide has been developed to provide guidance and recommendations specifically geared towards stadiums and arenas, focusing on improving existing and developing cybersecurity programs. There is currently nothing else similar to this stadium cybersecurity best practices guide. This is a key initiative to identifying, mitigating, and protecting against the growing cybersecurity risks associated within the sports landscape. The guide discusses risks levels associated with critical systems, including industrial control, communications, and enterprise systems, and then identifies best practices based on the NIST Cybersecurity Framework. The first step to assessing risk is through identification of systems within a facility. The deployment of the Sports and Entertainment Risk Assessment tool is designed to provide both an individual assessment as well as a comparative approach to analyzing the capabilities throughout stadiums, arenas, and the commercial sector in order to assess the risks, vulnerabilities, and effectiveness of preparedness, response and recovery, as well as mitigation efficiencies of these entities. The overarching goal is to create a comparative assessment from which venues can grow within their field. A strong reference point for evaluation can stem from characterizing the facility before an assessment, which allows similar venues to compare results and potential gaps in security measures, almost as a type of benchmarking approach. Characterizations can include the use of a venue, number of events hosted, number of attendees, or the overall size of the venue. In cities that have a concentrated area of venues or stadiums, an assessment would be ideal to uncover any inter-venue dependencies or optimal emergency-response measures. Both physical and cyber dependencies can be assessed.

III. Complications of Cyber in Sports

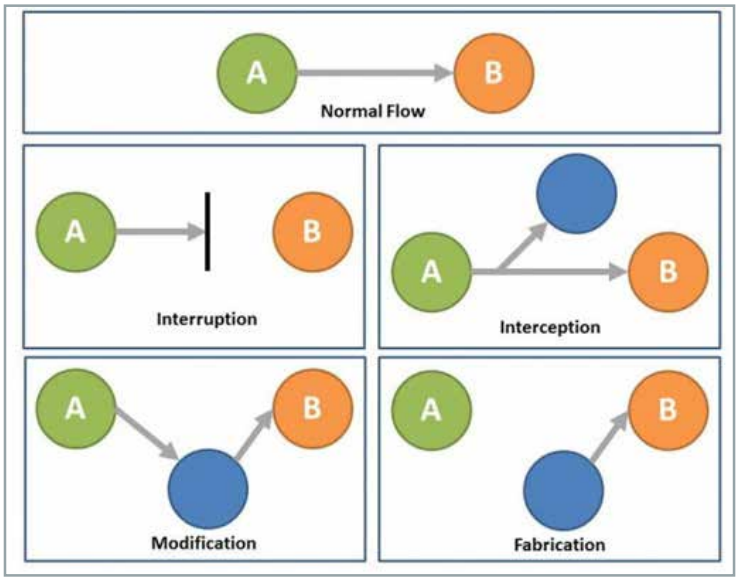
Cyber technology has become a staple in the globalization of sports and will continue to grow as a fundamental aspect of stadiums and arenas. Steps must be taken to assess the resiliency of networks and systems at each unique entity. This leads to potential complications, as there remains a lack of standardizations for cyber and technology. The assessments must also keep pace with the rapidly, ever-evolving technological capabilities that are regularly deployed. The sports world needs direction on how to identify and protect vulnerabilities within their respective organizations, whether it is at the professional, collegiate, or high school level. It is imperative to identify potential vulnerabilities, which then lays the foundation for the development and implementation of response and recovery practices in order to reduce cyber risk.

A risk assessment is a useful tool to utilize when learning the capabilities and improvement areas for a stadium or arena. The complication of a general assessment, however, is the degree of variance between any two stadiums or arenas. Nevertheless, a baseline of cybersecurity best practices for stadiums and arenas are ideally followed and implemented at all sporting levels. As a foundational step toward assessing risks and vulnerabilities, stadium owners and operators must first

define and understand the core functions of technology and cyber throughout the venue. Then, the identification of the venue's critical systems and data must be discussed. Being able to identify the core assets, capabilities, and systems of a venue provides the outline of risk identification. Cybersecurity plans must be established and encompass network security, data security, incident response plans, and management guidelines, especially for employers within the stadium. Currently, however, there are no federal cyber requirements requiring compliance for stadiums and arenas.

In order to optimize the process, the ability to identify cyber dependencies amongst systems within a venue is a first step to conducting a cyber resilience assessment. For example, computer systems within the stadium may rely upon other computer systems to function. This is where a dependency would exist. Cyber dependencies can affect critical business functions for organizations. Furthermore, the National Institute of Standards and Technology (NIST) issued the Framework for Improving Critical Infrastructure Cybersecurity, defining five core functions for improving protection and resilience of critical infrastructure. These core functions are: identification, protection, detection, response, and recovery. This framework identifies the role of cyber dependencies and their criticality within the protection of cyber-related services. Network performance provides functions for communicative efforts amongst users. The figure below illustrates the degradation of data quality by various threats. During normal operations, the flow of data exists between the provider and the user. Threats can lead to the disruption of this flow.

Figure 1 Security Threats



Requiring consideration are not only cyber dependencies but also physical dependencies. If a stadium were to become incapacitated, this could have an effect on such sectors as emergency services, which may rely on the facility as a shelter, or the command post. The Department of Homeland Security assessed large sporting event facilities, and more than 90 percent of stadiums and arenas were dependent on water, wastewater, and electric power for core operations. If there were to be a disruption in these supplies, a lack of these resources would have a detrimental effect on the operational capacity of a venue. The levels of degradation after losing a physical dependency can vary amongst external services. With a loss of dependency on water or communications, the degradation level would lower after about two hours of loss, but not instantaneously. For information technology and electric power, however, the effects would be felt immediately. The line between traditional information technologies (IT) has been merging with operational technology (OT) with regard to networks and physical systems. Cyber dependencies continue to grow, and stadiums and arenas rely on operational technology with such systems as HVAC or water control systems. Stadium operators must be aware that many of these industrial control systems are coming to rely on IT and thus creating a threshold of cyber vulnerabilities. A holistic understanding of what systems and networks comprise a venue is critical before preventative measures may begin. Defense-in-depth is an approach that provides a framework for improving cybersecurity protection when applied to control systems. As IT and industrial control systems continue to merge and become interdependent, control systems themselves become vulnerable to intrusions. Such vulnerability then leads to potential cyber-based attacks on critical infrastructure and its sectors. The Department of Homeland Security's National Cybersecurity and Communications Integration Center and Industrial Control Systems Cyber Emergency Response Team published the recommended practice of creating a defense-in-depth security program for control-system environments in order to reduce the risks within critical infrastructure sectors. Defense-in-depth layers multiple technologies and segment environments, leading to multiple, complex layers of security.

Unlike OSHA or FEMA standards and regulations, there is a limitation when assessing risk in various stadiums, as cybersecurity relies more on guidelines and best practices. Often, regulations can provide a basis for foundational security. Unique to cybersecurity is a landscape of nearly constant shifts, and implementing regulation updates to keep pace with the changes can be problematic. When it comes to assessing cyber and IT risks, focusing on resiliency may offer a better approach than a tactical one. The development of any risk assessment encompasses the idea of being broad enough to allow for application to a wide array of entities.

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

The drone threat – a real and growing danger to 'Critical National Infrastructure'

Drones are rarely out of the headlines these days with "drone incidents" an almost weekly occurrence. Rob Balloch, Senior Vice President Sales and MARSS Group looks at the drone threat and counter measures.

But probably the most well publicised incident was in December last year when a drone sighting around the UK's Gatwick airport caused major disruption for thirty-three hours, affecting approximately 140,000 passengers and 1,000 flights worldwide and costing an estimated £50 million.

A Sky News investigation in February this year found that in the UK, Police reported 2400 drone incidents in 2018, a rise of 40% since 2016, and many of these were flown within airport flightpaths.

Up until now (to the best of our knowledge and the media) the incidents in Europe and North America have been confined to hobbyist type drones, either deliberately or accidentally wandering into restricted airspace. Other incidents have taken place that perhaps don't make major headlines but are equally significant.

In July last year, activist group Greenpeace crashed a drone and a toy plane into the wall of a Nuclear facility in Bugey, near Lyon in France and again in January this year they used a drone to drop a smoke bomb on the roof of another nuclear facility. Alix Mazounie, energy campaigner for Greenpeace said: "Greenpeace has once again demonstrated that French nuclear facilities are not sufficiently protected against the risks of external aggression."

Whilst Greenpeace have clearly demonstrated vulnerabilities, in the Middle East, deliberate destructive attacks on critical national infrastructure (CNI) are now a reality.

In July 2018 Houthis militias claimed to have attacked an ARAMCO refinery in Riyadh using a drone and causing a fire. Whilst the fire was confirmed, ARAMCO denied the cause was a drone. At the time militias also claimed to have attacked Abu Dhabi's international airport in the United Arab Emirates with drones.

On 14th May this year, it was confirmed by Saudi Ministry of Energy that two pumping stations on the East-West pipeline were attacked by drones armed with explosives which caused a fire and minor damage. The pipeline transports Saudi oil from the Eastern Province to Yanbu port.

Since May the situation in the Middle East has escalated, with numerous confirmed drone attacks on airports in both Saudi Arabia and the UAE, the most damaging occurring on 24th June when Saudi Arabia's Abha airport was attacked and one person was killed and 21 people are reported to have been injured. Since then the attacks have continued.

Of course, drones have been used before by IS in Syria and Iraq but this latest escalation in the Middle East is the first sustained attack on any nation's critical infrastructure with a clear intention of damaging and disrupting their economy and that of the world.

While the recent attacks in the Middle East were of a different magnitude and level of sophistication using 'Qasef 1' long range military spec drones, that does not mean we should be complacent and assume that only state actors or their proxies are capable of damaging infrastructure, as amply demonstrated by Greenpeace. Highly capable drones are easily and cheaply available and the vast majority of our infrastructure remains unprotected from that threat.

So, how do you protect your critical national infrastructure?

Here at MARSS, experience has shown that the increasingly complex nature of the threats posed by drones, from large Predator type drones through to the hobbyist drones like those at Gatwick, requires a layered approach.

The MARSS drone detection system uses multiple sensors delivering a wide range of detection, identification and mitigation capability. By integrating technologies such as RF monitoring, S-band air detection radar and infrared cameras into MARSS' command and control system NiDAR, that delivers enhanced 360° perimeter surveillance, long-range awareness and protection.

Application of Artificial Intelligence based analytics developed by MARSS, autonomously and intelligently, classify and respond to multiple objects, triggering an initial alarm, confirming the threat and initialising de-escalation measures to neutralise the threat with the appropriate means.

At the heart of the MARSS Drone Detection System, NIDAR' open architecture can integrate any amount of existing systems and incorporate new technologies and sensors as they reach maturity and become available.

To find out more about MARSS' Drone Detection System download the MARSS White Paper at http://www.worldsecurity-index.com/shareDir/documents/15641513120.pdf

Do Criminal 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

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

Making Coperation Easier with Financial Intelligent Units

Over 100 representatives from 46 Financial Intelligence Units (FIUs) visited Europol today on the margins of the Egmont Group Plenary meeting in The Hague. The financial crime experts were presented with some of the core activities of Europol.

FIUs play an essential role in the fight against money laundering and terrorism financing. Europol hosts the FIU.net, the European tool which enables all EU FIUs to exchange information among themselves and with Europol. The existing cooperation as well as the future creation of a European Financial and Economic Crime Centre at Europol will encourage building even stronger ties between Europol and FIUs with the aim of better supporting Member States and partner countries.

Experts gather to tackle telecom fraud and other scams

Tackling the threats posed by telephone scams and other social engineering fraud was the focus of an INTERPOL meeting on financial crimes.

The 7th Meeting of the INTERPOL Anti-Transnational Financial Crime Working Group brought together experts to discuss the global response to several types of fraud scams which criminal networks are using to swindle unsuspecting victims out of their money.

The three-day meeting, organized by INTERPOL and the Chinese Ministry of Public Security and hosted by the Chongqing Municipal Government, looked at three key topics:

Telecom fraud – criminals set up call centres where the callers use a variety of ruses to trick victims into making payments;

Social engineering fraud – including business e-mail compromise (BEC) scams, romance scams, sextortion, and boiler room or investment fraud;

Money laundering and money mules – the criminals often use money mules to transfer their illicit profits.

Telecom fraud is a growing concern across Asia and beyond. Criminal enterprises set up call centres in various countries, often targeting elderly individuals by pretending to be government officials, police officers or bank managers and requesting the victims make urgent payments.

INTERPOL has coordinated several operations targeting telecom fraud in Asia. Operation First Light in 2016 led to the arrest of more than 1,500 individuals as police shut down more than a dozen illicit call centres in Asia and Europe.

INTERPOL President Kim Jong Yang at the INTEPROL Anti-Transnational Financial Crime Working Group

"The use of technology to commit fraud is not new. But the Internet and social media now enable criminals to expand their geographical reach, to diversify their targets and activities, often without even the need for in-person interactions or a physical presence," said INTERPOL President Kim Jong Yang.

To effectively counter these challenges, he highlighted the importance of establishing robust cooperative relationships to build a law enforcement network with a global reach and knowledge base.

In this respect, the meeting also addressed how the criminal networks use money mules to accept the illicit payments, transfer funds into the criminals' accounts or launder the proceeds. In many cases, these individuals do not even know that they are involved in a criminal activity as they are kept unaware of the source of the payments.

INTERPOL and NCS4: setting international standards on venue security

Violence, disorder, cyberattacks and terrorism at the hands of criminal groups or lone wolf actors are among the security risks associated with major sporting events.

To help address these risks, INTERPOL's Project Stadia and the University of Southern Mississippi's National Center for Spectator Sports Safety and Security (NCS4) have been holding a four-day incident management training course to strengthen law enforcement and first responder standards in sport venue safety and security.

Involving 24 senior participants from 20 countries, the training held at INTERPOL's General Secretariat headquarters will allow senior police officials and incident management team leaders from around the world to better assess potential security threats and prepare plans for evacuation and other protective actions for major international events.

The partnership between INTERPOL and NCS4 has seen the two organizations develop capacity building initiatives, in particular in support of INTERPOL's Project Stadia which is working to implement a comprehensive curriculum to assist member countries meet the demands of hosting major international sporting events.

To capture good practices and lessons learned before, during and after major international sporting events, Project Stadia conducts observation and debriefing programmes with designated security officials from both the public sector and private sector who have direct responsibilities for policing and security operations.

Elbit Systems Subsidiary Selected to Supply a Cyber Intelligence System to the Dutch National Police

Following an extensive and competitive evaluation process Cyber Intelligence Ltd, a subsidiary of Elbit Systems, was selected to provide the Dutch National Police with a Cyber Intelligence system.

Part of Elbit Systems' Intelligence 360 suite of Cyber capabilities, the solution to be supplied is designed to provide high-availability and scalability and enable customization with work-flow, legislation and other custom requirements of the Dutch National Police.

Haim Delmar, General Manager of Elbit Systems C4I & Cyber, commented: "The Netherlands continues to be an important market for us and we are proud to be in a position to contribute to national security and public safety. I believe that our operational experience and technological edge enable us to offer superior solutions to our customers and partners."

Minsait Enhances Protection Against Online Fraud

Minsait, an Indra company, has developed Onesait Behavior Fraud, a state-of-the-art cybersecurity solution for detecting fraud in online payment and transfer transactions that greatly enhances the levels of protection thanks to the application of pioneering artificial intelligence techniques that are capable of replicating the procedures and working methods of specialized banking analysts.

A cyberattack on an airline results in the theft of thousands of credit cards. €12.2 million have been withdrawn from accounts in just a few minutes. This is a real case that took place a year ago, but which is a recurring trend that is generating significant losses in the income statements of banks and companies in many other sectors that operate electronically all over the world.

Onesait Behavior Fraud can put a stop to this type of situation by establishing controls that are far superior to those offered by the anti-fraud tools used until now.

The solution applies automatic and machine learning techniques to ensure fraud detection, even if attackers use new techniques for which there is no known precedent.

The key lies in an algorithm capable of reproducing and automating the complex analysis procedures employed by bank anti-fraud analysts.

The ultimate goal of the Minsait system is to support the work of these specialists, who have to cope with an increasing number of online transactions that run at enormous speeds.

In addition, increasingly demanding regulations and the risk of incurring massive fines rise the pressure.

Onesait Behavior Fraud is responsible for building individualized profiles for each client and it processes large amounts of information about their activity in order to analyze each transaction and verify it. It can thus identify promptly any deviation from habitual behavior.

The system analyzes the operations that clients perform in all contact channels with the company or bank, and not only those in which fraud has traditionally been concentrated (cards and transfers). This omni-channel vision of clients makes it very difficult for attackers to hide their movements.

The Minsait solution completely overcomes the traditional fraud prevention strategy, based on the historical knowledge of the techniques used by scammers to establish business rules for detecting them.

The new system is much more efficient and secure and it allows banks and companies in any sector operating in digital environments to offer an agile and convenient service very much in demand by clients today; one which is essential to survive in the digital world.

Onesait Behavior Fraud was developed from the multipurpose data analytics platform Onesait Platform by Minsait and is integrated into the Onesait Behavior family of products, specialized in learning the behavior of entities and which is currently deployed in critical mission production environments.

The Versatility of 'Mobile' within the Security Sector

The use of mobile technologies, across the globe by the 'security' industry, has evolved immensely over the years -However, within the IT security, defence, law enforcement and border security arenas 'mobile', means different things to different parties.

For instance, on one hand, securing the mobile channel is critical and this aspect is important. On the other, it's a case of working out how to improve communications, security and operational efficiency through using mobile devices in difference scenarios.

One thing that is for certain, though, is that mobile has grown exponentially in popularity and use cases. Forrester, for example, has projected that global mobile device usage is expected to surpass 5.5 billion users by 2022. So, how can the industry ensure that mobile remains secure; and how is it improving the way security and border security functions?

MDM equals IT Governance

Not a day goes by when you don't hear a story about 'some organisation' losing corporate data. Mobile devices, including smartphones, laptops, body-worn devices and barcode scanners, are typically a medium that are vulnerable in this scenario. Therefore IT teams are continually evaluating how they can secure this channel.

This is where mobile device management applications (MDM) become crucial. They enable IT teams to govern their fleets of mobile devices. This includes allowing IT admins to monitor, manage and secure the devices that engage with their networks remotely from a central platform. Using MDM lets IT provision new devices; manage device and software updates; and remotely lock and wipe missing devices, protecting corporate data. In essence, MDM helps firms ensure that IT governance, at a mobile level, is adhered too.

Body-worn Cameras & Law Enforcement

The use of body-worn cameras is a growing trend in law enforcement. They promote higher degrees of transparency and accountability; promote staff professionalism; and help to deter crime and altercations within certain scenarios. Typically, these body-worn cameras function as standalone mobile devices, that store data on the device to be drawn off later. Or, they can be networked to stream data via Wi-Fi or the cellular network. In the future, we expect the dependence on body-worn devices to increase. Integrations with wider job-based workflows (e.g. start 'record' when I'm at a specified location such as for a delivery) and the reliance on AI features will grow too (e.g. face recognition).

Border Control & Security

The number of people travelling globally has increased. Border control agencies are now tasked with providing a swift, efficient, secure and convenient travel experience, as people pass through customs and immigration. To combat these challenges, and scan passports fast, teams often can use mobile devices, integrated with a machine-readable zone (MRZ). 'Mobile scanners' allow staff to move around; they automate and accurately document information for border agencies; and streamline this entire workflow.

The use of mobile technologies is a game changer for many industries. The challenge for the security sector to establish what mobile means to it. How is mobile going to improve my organisation? What software and hardware can I use? How do I secure that channel – and, especially important within the security industry, is my fleet of devices fit for purpose, business rugged and capable of withstanding the rigours of the wider security industry?

Fujifilm releases long range surveillance camera with built-in lens "FUJIFILM SX800"

FUJIFILM Corporation has released "FUJIFILM SX800" ("SX800"), a new long-range surveillance camera equipped with built-in lens. The SX800, developed with the cutting-edge optical technology and image processing technology, features a high-performance built-in FUJINON zoom lens, capable of 40x optical zoom

to offer a focal length range extending to 800mm, the world's longest telephoto coverage. It is an epoch-making surveillance camera that features advanced image stabilization performance, fast and accurate autofocus with AF speed as fast as 0.3 second, and outstanding heat haze / fog reduction function, making it possible to instantaneously capture clear footage of a distant subject.

South Carolina Department Of Corrections Installs 18 Soter RS\ Body Scanners In Their Facilities

ODSECURITY and ODSECURITY North America have recently finished installing Soter RS Body Scanners into 18 different sites within South Carolina Department of Corrections. In this installation, each of the 18 SOTER RS Body scanners are connected to one central data base.

This advanced database allows for the subjects identity to be verified by either an ID number, or by using the OD Fingerprint Reader before the scan commences, thereby managing the cumulative radiation dose per person, ensuring that no one exceeds any recommended dose levels. The central data base, also records; who was scanned, at what dose level, the result, and the category of any find enabling statistics and data to be gathered per installation.

The Soter RS is the worlds most advanced security X-ray system. It is a person X-ray system which combines ultra low radiation with maximum visibility, revealing everything hidden inside human cavities or inside the human body.

It is already used successfully in many prisons worldwide for scanning visitors, inmates and in some facilities, the prison staff themselves.

The Soter RS body scanner can detect any contraband. Indeed, to date is has detected; drugs/narcotics, weapons, cell phones, plastic items, metals, cash, gemstones and other contraband. Basically, if it is hidden, the Soter RS can detect it; whether it is on, or in, the body being scanned.

The Soter RS is the ultimate alternative for intensive strip searches or costly visits to a hospital.

OD Security, the manufacturers of the SOTER RS have installations similar to South Carolina around the world, including Miami and New Hampshire in the USA.

Security Seals Play An Important Role in Fighting Illegal Animal Trade

The global market in illegally traded animals and their parts, including skins, is estimated at 20 billion dollars or more, with over 350 million specimens of all types being sold illegally each year. It is considered the 2nd largest black market after drugs and believed larger than the trade in illegal arms.

Security seals play a role in efforts to bring down this problem, on land and sea. Several organizations including; Fish and Wildlife agencies in the US and many other countries, various UN agencies, CITES affiliated organizations, and the WWF use some type of security or tamper evident seal as a tag to register and identify legally traded items.

American Casting has been supplying seals as secure ID tags for decades to many of these groups. The most commonly used seals are plastic fixed length tags, like our model HS75 and 4001, or pull-up plastic seals like our AP-50 or 9001. However, American Casting & Manufacturing also supply a variety of other security seals that are used in the same effort. Tamper-evident seals are used to securely attach a non-removable serial number and species identification tag on various illegally sold animal or fish parts. This, in turn, helps to identify illegally traded items.

Some items include skins of crocodiles, snakes, alligators, or even protected cats. Tamper-evident seals are also attached to valuable and controlled fish like yellowfin and bluefin tuna, certain shark species, and many more. In many cases, our seals are used on lesser-known species, even the yak hides which are illegally taken and sold in Central Asia.

Aircraft Location and Emergency Response Tracking (ALERT) Service Now Live

World's first-ever, global emergency aircraft locating service provides critical, on-demand data to aviation stakeholders as a public service

Aireon and the Irish Aviation Authority (IAA) announced today that the Aireon Aircraft Location and Emergency Response Tracking (ALERT) service is officially live.

As the first system of its kind in public service, Aireon ALERT provides Air Navigation Service Providers (ANSPs), commercial aircraft operators/airlines, aviation regulators and search and rescue organizations with the last known position of any Automatic Dependent Surveillance-Broadcast (ADS-B) equipped aircraft globally. Much of the world's aircraft are already fitted with this technology, and it will allow for identification of an accurate position for an aircraft that is in an apparent state of distress or experiencing a loss in communication.

Operated by the IAA out of their North Atlantic Communications Centre in Ballygirreen, County Clare, Ireland, Aireon ALERT is enabled by the AireonSM system, the world's first global air traffic surveillance service. The system, which went live on 2 April 2019, monitors all ADS-B-equipped aircraft spanning the entirety of the earth's surface—even over the ocean and in the most remote airspaces. Prior to Aireon becoming operational, only 30 percent of the Earth's surface was monitored through conventional ground systems, leaving over 70 percent without any real-time air traffic surveillance. With Aireon ALERT, registered users now have access to exact location information for aircraft in distress, on-demand, which will dramatically benefit global emergency response efforts.

"This is an exciting day for the IAA and Aireon teams," said Peter Kearney, CEO of IAA. "We have been preparing for this moment for a long time, and we are proud to host and operate the world's first global aircraft locating system. The IAA has always been about innovation and service excellence; our position as a partner in Aireon and in the provision of this global service, further strengthens Ireland's role as a key player in the global aviation industry. As of now, our facility in Ballygirreen is providing the Aireon ALERT service every day, no matter the hour, and we are excited to play such a critical role in delivering this game-changing service to the aviation community. Building on our role as a key player in communications for the North Atlantic, we are proud to be powering Aireon ALERT for the entire globe."

"Now that the Aireon system is operational, we are thrilled to deliver this much-needed public service to the industry," said Don Thoma, CEO of Aireon. "Aireon ALERT can provide the most accurate and precise aircraft locating data for emergency and distress situations, free of charge. As the operator of the world's only global aircraft surveillance system, we recognize our unique position to provide such a critical service to the aviation community, and see it as our duty to provide this data to the proper authorities to assist in emergency situations."

Aireon ALERT users do not need to be customers of Aireon or the IAA to access the service; however it is important that all commercial aircraft operators/airlines, aviation regulators and search and rescue organizations register to ensure they can contact the 24/7/365 operations facility, in the event of an emergency, to obtain the last known position of its aircraft. Once contacted, the Aireon ALERT operator will provide a map of the last 15 minutes of flight for the particular aircraft in distress, with one plot per minute and a 4-dimensional report including altitude, latitude, longitude and time information.

To register for Aireon ALERT, commercial aircraft operators/airlines, aviation regulators and search and rescue organizations should visit https://aireonalert.iaa.ie/alert-register.

DHS S&T Announces $35M Funding Opportunity for New Center of Excellence in Terrorism Prevention and Counterterrorism Research

The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) announced today $35 million in funding opportunities for a new DHS Center of Excellence (COE) for Terrorism Prevention and Counterterrorism Research (TPCR). Accredited United States colleges and universities are invited to submit proposals as the center lead or as an individual partner to work with the lead institution in support of the center's activities.

"By partnering with universities, S&T delivers practical results by developing multidisciplinary, customer-driven solutions while training the next generation of homeland security experts," said William Bryan, Senior Official Performing the Duties of the Under Secretary for Science and Technology. "Once awarded, this COE will leverage emerging technologies and analytic techniques to provide innovative solutions for preventing and countering terrorism."

This funding opportunity is posted at http://www.grants.gov/. The deadline for submitting proposals is September 6, 2019. DHS plans to fund this new COE through a cooperative agreement for 10 years for a total of approximately $35 million.

The TPCR COE will research and develop solutions to support DHS counterterrorism operations. This includes solutions that help prevent terror attacks by countering the radicalization of people and their mobilization to violence. TPCR will also educate a skilled workforce trained in the latest methods to identify and protect the nation from terrorist threats.

The rapidly-evolving, diverse terrorist threat continually exploits technological advances to adapt the nature and expand the reach of its tactics. TPCR will support academic-led innovation that supports DHS in staying a step ahead of emerging terrorist tactics.

DHS is soliciting proposals from multi-disciplinary research and education teams that will work closely with DHS and other subject-matter experts to develop successful innovations to confront the future counterterrorism challenges DHS faces. The teams will need various combinations of academic disciplines, including engineering, data analytics, and mathematics.

The DHS COEs are university consortia that work closely with DHS operating components to research, develop, and transition mission-relevant science and technology, and to educate the next generation of homeland security technical experts. TPCR will be required to engage with DHS operational components and fully understand the operational environment to help better identify technical and training gaps. Each DHS COE is led by a U.S. college or university and has multiple partners from universities, commercial industry, DHS, Federally Funded Research and Development Centers, and other federal, state, and local agencies.

The notice of funding opportunities for the Terrorism Prevention and Counterterrorism Research COE Lead Institution and Partner Institutionare available at grants.gov. S&T will conduct an informational webinar for interested applicants on August 6, 2019 at 3 p.m. EDT. During the call, DHS will discuss the notice of funding opportunity and provide an opportunity for interested applicants to ask questions. The webinar can be accessed at https://share.dhs.gov/rwo6kbeg53be/; it will be recorded and posted on www.grants.gov for future reference.

For additional information about the DHS COEs, visit DHS Centers of Excellence at https://www.dhs.gov/science-and-technology/centers-excellence

Joint Cyber Defense Command Completes Its Training With Indra Cyber Range

The staff of Joint Cyber-Defence Command in Spain has completed the programmed training with the Indra Cyber Range solution to reinforce their ability to conduct and execute military operations in cyberspace.

Unlike other domains, attacks in this area occur continuously without the need for a situation of conflict having been declared. Great powers, criminal organizations and terrorist groups take advantage of any opportunity to spy, attack or obtain an economic benefit.

Much of a country's ability to protect itself and to carry out military deployments depends directly on the preparation of its cyber-intelligence experts. The Spanish Joint Cyber-Defense Command last year chose Indra's solution to prepare collaborative cyber-exercises together with the armies from various Ibero-American countries with the aim of sharing knowledge and responding to global attacks in a coordinated way.

They also used it to carry out advanced training in forensic analysis techniques. These techniques allow information and evidence to be gathered to help solve digital crimes. This intelligence capacity is vital to analyze the strategies followed by the enemy and to limit the anonymity that allows them to operate without impunity.

1st Detect Launches the Tracer 1000™ – the First Mass Spectrometer Explosives Trace Detector

1st Detect Corporation has announced that it is officially launching the TRACER 1000, the world's first European Civil Aviation Conference (ECAC) certified desktop mass spectrometer explosives trace detector (MS-ETD), enabling airports and air cargo facilities worldwide to stay ahead of emerging threats, lower operating costs, and improve screening throughput.

Over a decade ago, the National Research Council's Committee on Assessment of Security Technologies for Transportation identified mass spectrometry as the solution for the shortcomings of ion mobility spectrometry ETDs (IMS-ETD), which is the currently deployed technology. The shortcomings identified included a limited number of detectable threats and a high false alarm rate. The Committee also recognized that cost, complexity, and ruggedness would be the challenges of fielding mass spectrometry-based instruments.

In addition to their extremely limited libraries, IMS technology is known to suffer from false alarms because common household products can be confused with dangerous explosives. This commonly results in passenger delays, unnecessary screening costs, and decreased confidence in ETDs.

The TRACER 1000 is an ETD that has been engineered to meet the needs of the next generation passenger and cargo security checkpoints and replace the antiquated IMS-ETDs that are currently in service with a lower cost of ownership. As terrorists continue to find new ways to threaten global aviation security, the TRACER 1000, with its virtually unlimited and instantly updatable threat library, enables aviation security operators to always stay ahead of the threats. With a lower false alarm rate than the outdated IMS-ETDs, and near-100% uptime, the TRACER 1000 ETD is the logical solution for any passenger checkpoint or cargo facility going forward.

"The aviation security industry has been wanting MS-ETDs for a long time and we are excited to announce the launch of the Tracer 1000 as a true mass-spec technology breakthrough," stated Raj Mellacheruvu, CEO of 1st Detect. "The fundamental virtues of mass spectrometry technology enables us to deliver a product with compelling benefits to checkpoint security operators, including the capability to quickly address a virtually unlimited number of emerging threats, improve screening efficiency, and lower operating costs," he added.

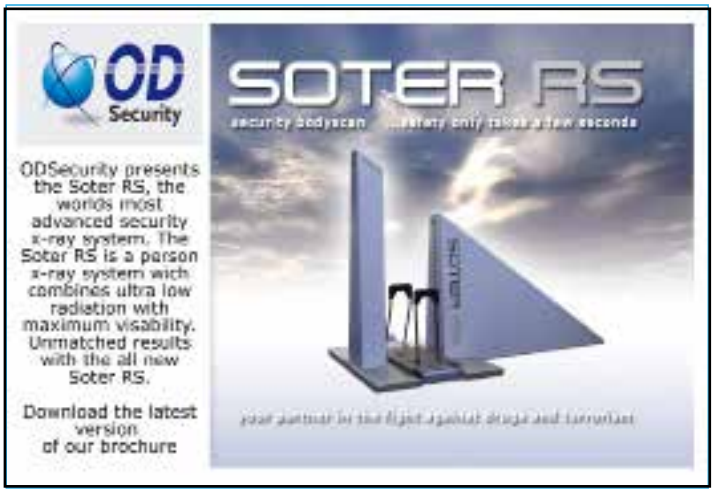
The Tracer 1000 garnered considerable interest following the recent announcement of receiving ECAC certification and has been invited to participate in a number of field trials, all of which have met or exceeded customer expectations.

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.

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.



August 2019

14-16
Secutech Vietnam
Ho Chi Minh City, Viet Nam
www.secutechvietnam.tw.messefrankfurt.com/hochiminhcity/en.html

22
Secure CISO
Toronto, Canada
www.secureciso.com/toronto

27
Skydd Detektor Open 2019
Nykvarn, Sweden
www.detektor.com/scandinavia/sv/SkyddGolfen.asp

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

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

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

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

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

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:

Media Partners: