WORLD SECURITY REPORT

Official Magazine of

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

MAY / JUNE 2019
www.worldsecurity-index.com

FEATURE:
Prisons, Detention Centres, Custodial Institutions are in crisis - The worldwide drug epidemic has hit our prisons
PAGE 9

FEATURE:
Passport free airport experiences take off with the help of facial recognition
PAGE 12

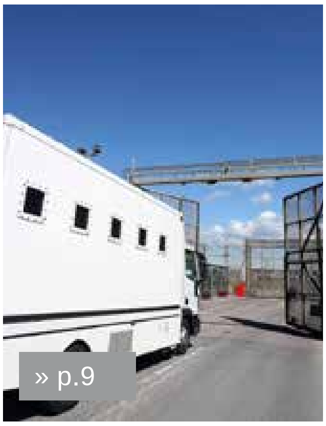
FEATURE:
From video surveillance to real-time video analytics – today's solution to prevent and solve future incidents?
PAGE 16

IS Renews Call for Arson as Method of Attack

i scan with technology from
Rapiscan Systems | AS&E.

CONTENTS

WORLD SECURITY REPORT



CNI UNDER ATTACK

In recent weeks we have seen drone attacks on oil pipelines in Saudi Arabia and attacks on oil tankers in the Gulf. Ansar Allah (Houthi) militias who carried out the drone attack also claim that Dubai airport was attacked by a drone, although this has been denied by the UAE authorities.

In addition, we've seen the uncovering of a plot in Nigeria to mount a sustained campaign to attack its critical infrastructure.

In Saudi Arabia two pumping stations were attacked by drones armed with explosives which caused a fire and some minor damage. The pipeline transports Saudi oil from the Eastern Province to Yanbu port.

Saudi Minister of Energy Mr. Al-Falih affirmed that this act of terrorism and sabotage in addition to recent acts in the Arabian Gulf, do not only target the Kingdom but also the security of world oil supplies and the global economy.

This attack came only days after four oil tankers were attacked by saboteurs off the coastal port of Fujairah in the United Arab Emirates. Saudi Arabia reported that two of its oil tankers were among those attacked, the others being registered in Norway and Sharjah.

A UAE led investigation has told the UN Security Council, in a closed meeting, that divers were used to attack the ships using limpet mines, and that the attacks showed a "high degree of sophistication". The conclusion being that "state actors" are responsible for the attacks.

Meanwhile, Houthi militias have stated they will continue to target military and civilian critical infrastructure in Saudi Arabia and the UAE, in a clear attempt to destabilise both and bring international pressure to bear on the coalition partners by disrupting the global oil trade. As result of the attacks crude oil prices jumped!

In Nigeria's Leadership newspaper, Police reported that they have uncovered a plot to commence massive and coordinated attacks on oil installations across the country.

Spokesman, Frank Mba, a Deputy Commissioner of Police, said in a statement "That the attacks would be carried out in the Niger-Delta region and adjoining states."

He said the elements were claiming to be climate and environmental activists. "These plots, which are politically motivated, and are aimed at sabotaging oil installations with intended negative consequences on national security, economic development and the global oil market"

Nobody is suggesting that the Gulf and Nigerian attacks are in any way linked. But it might suggest that terrorist groups, or their sponsors, are switching on to the fact that they can hurt a regime more effectively by disrupting its economy and that of the world, than they are by the mindless slaughter of its citizens.

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.

IS renews call for arson as method of attack

Islamic State group (IS) has claimed responsibility for a string of arson attacks that burned agricultural lands and crops in Iraq and Syria, urging its militants to intensify their use of this method of attack.

IS has long employed a scorched-earth policy in areas where it has been driven out and has previously recommended arson as a form of jihad.

The new incitement to torch lands came in the latest issue of IS's weekly newspaper al-Naba, which was published on 23 May via IS's channels on the messaging app Telegram.

While the IS article said the arson attacks were to punish land-owners who work for or support the government, local officials have said to extort money from farmers.

'Roll up your sleeves'

The al-Naba article opens with a threatening line, "It looks like it's going to be a hot summer", before urging its militants to "roll up your sleeves" and use arson as a method of attack. IS tells them there are plenty of agricultural fields, orchards, houses and "economic infrastructure" for them to target in Iraq and Syria.

Al-Naba lists a string of attacks in the past week in which fires "engulfed hundreds of hectares" in the Iraqi provinces Diyala, Kirkuk, Nineveh and Salah al-Din, where IS operatives are mostly active.

It says the attacks targeted land owned by Shia or Shia militias as well as by Sunnis who allegedly collaborate with the government.

The article lists "many arson attacks" carried out in the eastern province of Diyala on 16 May and others in neighbouring Salah al-Din, presumably on or around the same day.

Across the border in Syria, IS said its militants on 20 and 22 May set fire to wheat fields owned by "apostates" - mostly a reference to Sunni Muslims - in the north-eastern Hasaka Province.

It justified the attacks by saying the land-owners are known to be "agents" of the Syrian government

and/or work for the local authority in their towns. IS gloated that the destruction of crops came "shortly before the harvest season", denying farmers revenue from wheat and barley sales.

The fires, it claimed, have prompted the Iraqi government to declare "a state of alert" in an effort to resolve the matter.

Previous incitement

IS has on several occasions in the past recommended the use of arson both in the Middle East and in the West.

In an October 2018 edition of al-Naba, IS told its supporters to use arson saying it causes maximum destruction and requires minimal effort to start.

In January 2017, IS's multilingual magazine Rumiyah (now defunct) told supporters in the West that arson was "a quick option for anyone intending to join the just terror campaign".

Rumiyah provided instructions on how to make and use Molotov cocktails and napalm and provided a long list of "ideal targets", including houses, apartment buildings, petrol stations, hospitals, schools, universities and night clubs, in addition to forests near built-up areas.

It added that "multiple simultaneous attacks" were preferred. On the latest fires in Iraq and Syria, IS appeared to indicate that multiple farms were set ablaze on the same day.

أنصار الخلافة
في الميدان ٢
إلى
الإحراق
{مَا قَطَعْتُم مِّن لِّينَةٍ أَوْ تَرَكْتُمُوهَا قَائِمَةً
عَلَى أُصُولِهَا فَبِإِذْنِ اللَّهِ وَلِيُخْزِيَ الْفَاسِقِينَ}
[الحشر: 5]

The group has in the past boasted about using arson to target the properties of government members or aligned militias and tribal figures in Iraq.

Pro-IS media groups have also repeatedly called for arson as a form of jihad, echoing IS's recommendation.

In June 2017, shortly after a fire engulfed the residential Grenfell Tower in London, pro-IS media group al-Wafaa (now a dissident media group) called for arson attacks in the UK in a document titled "The permissibility of setting English properties on fire".

The article featured a picture of Grenfell Tower in flames and expressed admiration at the sight of fire engulfing "the property of Christians in England". The article did not suggest that jihadists were behind the fire but appeared to refer to the incident to show the potential impact of fires.

IS has also in the past more broadly called for sabotage attacks targeting the economic interests and infrastructure of the government and its "agents" in Iraq and Syria, with focus on oil, gas and energy installations.

Following its scorched-earth strategy, IS in 2016 set fire to several oil fields in Qayyarah near Mosul in northern Iraq before it fled the area. The impact was devastating and it took months to finally put out the fires.

In May 2015, IS caused near-total destruction to Iraq's key oil refinery in Baiji, after being driven out of the facility. The group later bragged about the sabotage in al-Naba, saying it would cost the Iraqi government a fortune to rebuild the refinery.

Farmers complain

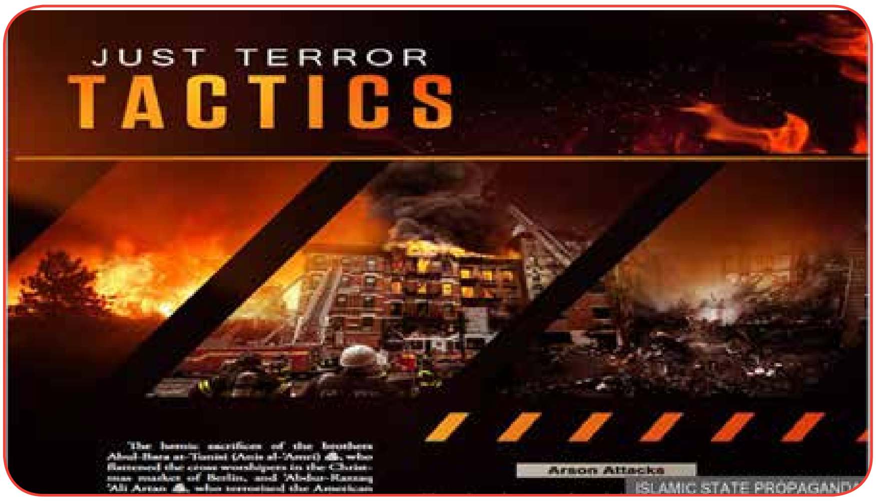
The recent fires have been and the affected farmers widely reported in Iraq and land-owners have demanded the Iraqi authorities compensate them for their losses.

On 18 May, Iraq's Ministry of Commerce accused IS operatives of torching agricultural fields in several provinces.

Salah al-Din governor Ammar Jabr Khalil said IS was carrying out the attacks to extort money from farmers, according to Beirut-based al-Sumaria TV reported.

IS's predecessor, Islamic State of Iraq, had strongly relied on extorting local businesses to fund itself. If a business or a wealthy individual did not pay IS regular sums, their properties and possessions would be destroyed and their lives threatened.

Iraq's Ministry of Agriculture has said it is investigating the fires, which it said appeared to be "systematic".


JUST TERROR
TACTICS
The heroic sacrifices of the brothers Abul-Bara at-Tunisi (Anis al-'Amri), who flattened the cross worshipers in the Christmas market of Berlin, and 'Abdur-Razzaq 'Ali Artan, who terrorized the American
Arson Attacks
ISLAMIC STATE PROPAGANDA

Despite the Iraqi authorities' suspicions that IS is behind the fires, some Iraqi activists and commentators on social media have pointed the finger at "regional powers" who allegedly do not want to see Iraq agriculturally self-sufficient. Others have blamed "Shia militias loyal to Iran".

Article by Mina Al-Lami, Head of the Jihadist Media Unit, BBC Monitoring

Twitter @Minalami

BBC Monitoring tracks, translates and analyses media across the world for governments, corporates and academia.

Twitter @BBCMonitoring

BBC MONITORING

Prisons, Detention Centres, Custodial Institutions are in crisis - The worldwide drug epidemic has hit our prisons

With an increase in people using illicit drugs - According to the latest report UNODC World Drug Report 2018 (United Nations Office on Drugs and Crime) about 275 million people aged 15-64 used an illicit drug in 2016 – and with drug abuse and crime intrinsically linked there will inevitably lead to an effect on our prison numbers.

In recent figures from The Prison Policy Initiative, their The Whole Pie 2019 report states that the American criminal justice system holds almost 2.3 million people, and that of those, 399,500 are held for drug related crime.

Whilst in the UK, The UK Prison Populations Statistics lists the current prison population of approximately 92,500 of which 15% were held for drug related crime.

These figures show simply "drug possession or drug trafficking". Once you consider, theft, robbery or violence against the person (VATP) figures, where the crime could be drug related, then those figures will increase considerably.

These prisoners enter custody with the same drug habit that they had before they perpetrated the crime. They will have the same needs and go to the same lengths to get their fix.

Or those who made money from selling drugs, will find a ready-made market once inside and will have the wherewithal to fulfil those needs – almost like a fox in a chicken coop. UK Ministry of Justice figures reveal that the amount of times drugs were found in prisons rose by 23%. There was also a 15% rise in finds of mobile phones and a 13% rise in SIM cards. Random drug testing between March 2017 and March 2018 revealed that 20.4% of drug tests came back as positive, and that "Spice" was found in 60% of the positive random tests.

We must attack this crisis in three parts;

- we need to deal with the burgeoning drug crisis outside of our establishments

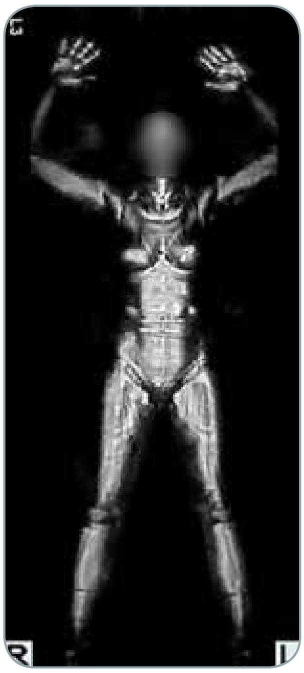
- we need to help our prisoners with an addiction once inside our establishments

- we need to stop the drugs from entering our establishments

We already have a "proven" weapon in our drug detection arsenal.

Speaking in May, at the 24th CDPPS (Conference of Directors of Prison and Probation Services) in Cyprus, CEO of ODSecurity, Jan Steven van Wingerden highlighted the importance and benefits of using a transmission body scanner.

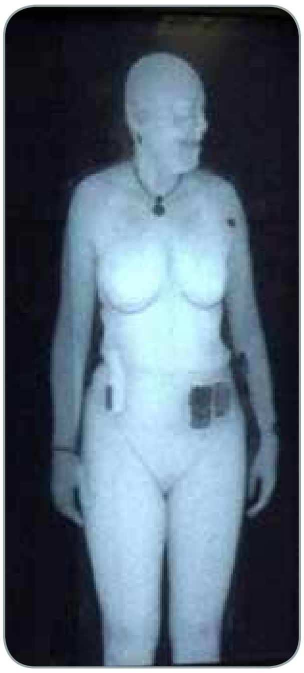
Historically detection methods have developed from the physical pat downs to the intrusive and humiliating strip and body cavity searches to varying levels of electronic and scanning technology.



This shows the quality of an image from a body scanner using "Millimetre Wave" technology.

This is the clarity of image that can be achieved through non-ionizing technology.

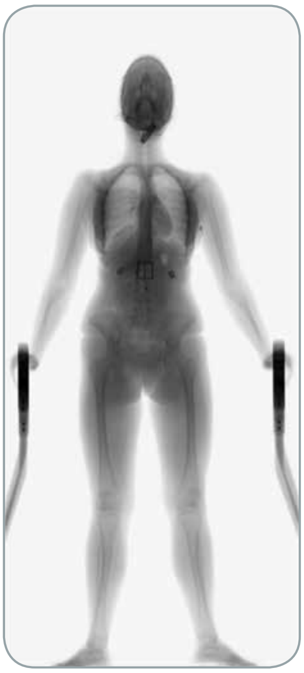
Although showing a clear image of the person it is unclear if this body has anything secreted on the body, and certainly no indication of anything within the body.



This shows the quality of an image from a body scanner using "Backscatter" technology

This is the clarity of image that can be achieved through ionizing technology with levels of between 0,02 – 0,1 uSv

Although clearly showing the "form" of the body being scanned, and clear evidential proof of contraband concealed on the body, there is no indication of anything concealed within the body.



This shows the quality of an image from the ODSecurity Soter RS body scanner which uses "Transmission" technology.

This is the clarity of image that can be achieved through ionizing technology with levels of between 0,1 – 2,0 uSv

This image clearly shows the "form" of the body being scanned, and clear evidential proof of contraband concealed on and within the body.

Each has its own level of effectiveness, but what this situation requires is total effectiveness, not partial.

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.

Concerns over the safety of using X-Ray technology outside of a medical situation has been in the news since 1993, when the use of X-ray technology has been allowed in non-medical uses. The X-ray tube is not a source of radioactive rays!

Radiation doses are measured in "sieverts"

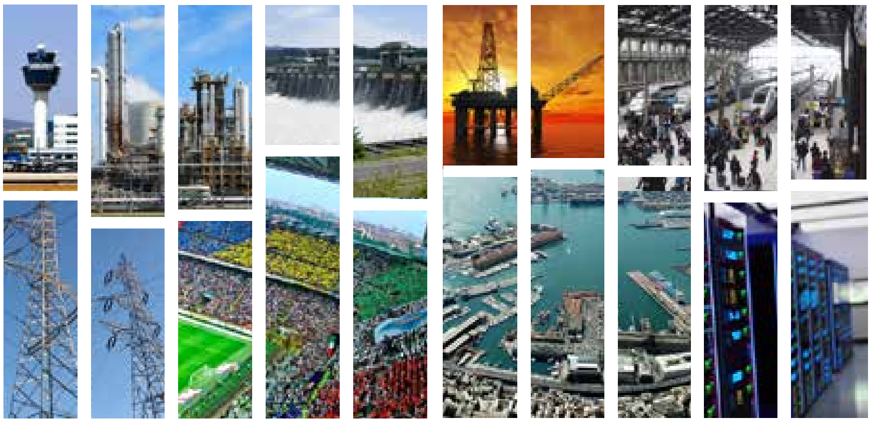
1 sievert would be a massive dose.

Millisieverts – mSv = 1/1000th of 1 sievert

Microsieverts – uSv = 1/1000,000 of 1 sievert

To put these measurements into perspective; a human being just by eating 2 bananas will be exposed to 0,2 uSv. By flying in an aeroplane, you could be exposed to 20 uSv – that is the equivalent of 80 scans using the Soter RS. A typical medical chest CT Scan is 7000 uSv- that is the equivalent of 28,000 scans!

However, these concerns are obvious real concerns of the specifiers and purchasers of body searching equipment, as has been shown in a recent questionnaire of purchasers of the equipment. With this in mind, the safety of full body scanning to prisoners, visitors, and staff have been taken into



14th-16th Oct 2019 | Milan Italy

Co-Organised by:

International Association of CIP Professionals

Regione Lombardia

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

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

REGISTRATION OPEN

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

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.

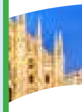
Milan is an ideal location for Critical Infrastructure Protection & Resilience Europe because it is the regional capital of Lombardy, one of Italy's greatest cities, and its industrial and financial powerhouse.

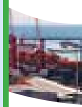
We look forward to welcoming you on 14th-16th October 2019.

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

Confirmed Speakers include:

- Alessandro Lazari, Regional Director Mediterranean, International Association of CIP Professionals
- Piotr Ciepiela, Associate Partner, OT/ IoT Security & Critical Infrastructure Leader, EY
- Ilias Gkotsis, Associate Researcher, Center for Security Studies (KEMEA)
- Vittorio Rosato, Head of Energy Technologies Dept, Smart Energy Division, ENEA, Italy
- Dr Ugo Finardi, Researcher, CNR-IRCrES National Research Council of Italy, Research Institute on Sustainable Economic Growth
- Sandro Bologna, Board Member, Italian Association of Critical Infrastructures' Experts (AIIC)
– Borja García de Soto, Ph.D., Assistant Professor of Civil and Urban Engineering, New York University Abu Dhabi (NYUAD)
– Paul Lucier, VP, Business Development, ISARA Corporation, USA
– Alberto Neri, RESISTO Project Leonardo Technical Coordinator – Cyber Security Division, Leonardo
– Elli Pagourtzi, Researcher, Center for Security Studies (KEMEA), Greece
– Roberto Setola, Associated Professor, University Campus Bio-Medico of Rome
– Stefano Betti, Independent Criminal Justice and Policy Expert, France
– Martin Hromada, Senior Researcher/ Assoc. Prof, Tomas Bata University in Zlín, Faculty of Applied Informatics, Czech Republic





Leading the debate for securing Europe's critical infrastructure

Supporting Organisations:

NS&RC SPF ISIO

Media Partners:

World Security-index.com WORLD SECURITY REPORT

www.cipre-expo.com

consideration during the development process of the Soter RS.

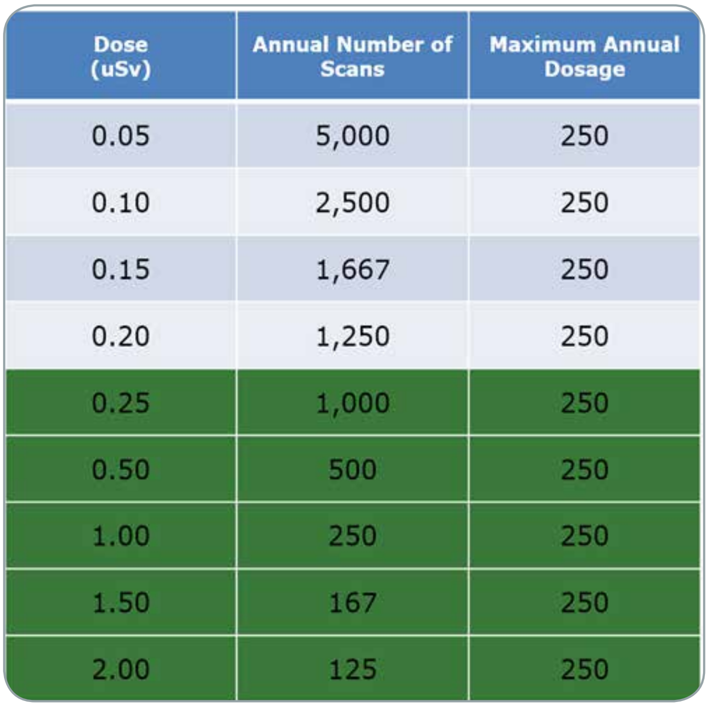
The advanced database allows for the subject's identity to be verified by either an ID number, or using the OD Fingerprint Reader, before the scan commences, thereby managing the cumulative dose per person ensuring that no one exceeds any recommended doses.

In 1993 the National Council on Radiation Protection and Measurements, (NCRP) recommended that the annual dose limit for a member of the general public for continuous or frequent exposure should not exceed an effective dose of 1 mSv excluding exposures from natural background and from medical care. – That equates to roughly 1,000 Soter RS searches per person per year! They would need to be scanned 3 times a day before they reached anywhere near the NCRP recommended levels.

The same council (NCRP) – cites in their Commentary no 16, in December 2003

"It is this administrative control of 0.25 mSv effective dose (or less)) per year for a member of the public (for a single source or set of sources under one control) that this Commentary recommends be used for individuals undergoing security screening procedures with x-ray scanning devices" – That equates to around 250 Soter RS searches per person per year!

Then in 2014 the International Commission on Radiological Protection (ICRP) cites in their Publication 125, (2014). "If a decision is made that its use is justified, the framework for protection as a planned exposure situation should be employed, including optimization of protection with the use of dose constraints and the appropriate provisions for authorization and inspection."



Dose (uSv)	Annual Number of Scans	Maximum Annual Dosage
0.05	5,000	250
0.10	2,500	250
0.15	1,667	250
0.20	1,250	250
0.25	1,000	250
0.50	500	250
1.00	250	250
1.50	167	250
2.00	125	250

Whilst in 2009 the American National Standards Institute (ANSI) and Food and Drug Administration (FDA) in their standard 43.17-2009 Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation, provides a chart showing the dose levels, annual number of scans and maximum annual dosage.

The regulation over the use of body scanners is strict and rightly so, and as you can see from the data above, the Soter RS system falls safely and very comfortably within the recommended safety levels.

The method of contraband detection within our facilities has changed substantially over the years as has the role of of X-ray scanning, but the way we view using X-Ray scanners in prisons also needs to change.

Anecdotally, consider that one prisoner, who is known as a high risk of smuggling contraband, and say that one prisoner has already has his allocated 125 scans (@ 2.00 uSv) for the year, yet you have received qualified and reliable information that he is concealing contraband. Do you scan or don't you? The justification of any use of radiation is that it must have benefits exceeding potential harms. Surely in this case, the needs of the many outweigh the needs of the few.

Security scanning is a controlled process without risk and needs to be accepted within our custodial systems as a positive in the fight against drugs in our systems.

In one case study, Correctional Facilities in Ontario using 16 OD Security Soter scanners performed 136,600 scans during a 6 month period. Of these 4,774 scans were recorded as positive. The finds were, 10 mobile phones, 74 weapons (knives and shives) and the balance 4,690 were of drugs.

If proof were needed that security scanning is needed in our prisons that surely those results speak for themselves.

Contributed by:

Jan Steven van Wingerden
Managing Director
ODSecurity

Passport free airport experiences take off with the help of facial recognition

In a generation which unlocks mobile devices with a smile, the application of biometric data has moved from a foreign concept, to an everyday way of life. People are more in tune with their personal data than ever before, understanding its use as an authentic code to authorisation, but also placing increasing importance on its potential to save time, and simplify mundane tasks. Panasonic's Karen Sangha outlines how facial recognition can help ensure a smoother start to your airport experience.

Famous for the relentless chore of security check-ins and passport control, there is no better place for biometrics than airports. In fact, this has even become an expected location for individuals to utilise facial recognition technology at immigration control, with specially designed RFID chips containing a digital copy of personalised information and biometric identifiers to match the image on a passport, with the identity in real life. Over the past few years, this has amounted to a total of 490 million e-Passports circulating across 100 different countries, with a total of 259 e-passport gates in operation across 14 different UK airports alone.

One example of an airport which has implemented this form of facial recognition technology is the Tokyo International Airport at Haneda. Already the third largest airport in Asia in 2018, the airport implemented Panasonic's FacePro facial recognition technology when it was granted the bid for the 2020 Tokyo Summer Olympics. The expected influx of about 40 million visitors during this time, is expected to place increasing pressure on airport security systems. In fact, with this figure almost double the number of tourists visiting the country in 2016, technology needs to facilitate a new time saving process to avoid doubling time spent in the airport too. The result of the implementation of new facial recognition gates, therefore, was designed to streamline the departure and arrival of nationals, based on the concept of a simple, secure, and safe solution where both first timers and the elderly could pass through the gate without delay, frustration, or confusion. For example, a new type of passport reader was developed that could be positioned in a variety of ways in addition to its predetermined manner. Instructions are then displayed on the screen to ensure smooth and accurate use, enabling the success of a system which is dependent on the quick transition of people that can easily utilise the technology.

With a large number of high quality e-Passports already provided across multiple large-scale airports, to which passengers have become accustomed, airports are therefore looking to the future of its use. Largely, this direction appears to be in favour of a facial recognition driven end-to-end contactless passenger journey. The idea behind the concept is a move away from facial recognition used only at the end of a journey, typically with immigration control, but rather facilitating facial recognition across check-in, bag drops, security lanes, and boarding gates, for a seamless passenger travelling experience. In the short term, the system will work by allowing passengers to log their passport data and individual faces within the facial recognition system upon arrival at the airport. This will enable a seamless, 'paper free' journey through the airport, without the need for passport checks every step of the way.

Already, the new concept of biometrics has been implemented at London Heathrow, ready for the peak of the summer season. With an investment worth £50 million, the facial recognition technology is set to streamline the passenger journey time by up to a third, ensuring easier security control, that is more efficiently managed. Equally, this end-to-end system is being implemented at the world's busiest airport, Hartsfield-Jackson Atlanta International Airport, with the two flagship environments setting a precedent for facial recognition technology that many other airports are likely to follow.

However, with an increased reliance on facial recognition technology, public opinions are bound to turn towards concerns regarding GDPR, and the safety of their stored biometric data. Largely, this is in response to recent data breaches such as those faced by British Airways in 2018, resulting in the theft of personal data of up to 400,000 customers. To reassure consumers, transparency regarding the understanding of how their data is being used, and how it is being protected is necessary. In particular, this requires cyber-attacks to be mitigated by protecting data through secure passwords, encrypted firmware, removal of unused features within an Linux operating system, and more.

Despite increasing fears, however, the potential benefits of facial recognition technology still outweigh the concerns, with IATA research following the implementation of upgraded facial recognition at Heathrow airport showing that 64% of passengers would be prepared to share biometric information in exchange for a smoother journey. Combined with tech overhauls such as self-service baggage check in, X-Ray scanners which do not require the removal of electronics and liquids at baggage control, and electronic body scanners, airports are increasingly designed to meet this requirement.

Despite facial recognition end-to-end journeys being in their infancy, new technologies are already arising to suggest how this journey can be simplified even further, with facial recognition combining with smart technology to customise experiences. For example, the Panasonic One ID platform is designed to enhanced passenger throughput and customer satisfaction, by personalising journeys and improving airport operational efficiency. Facial recognition systems will be linked to digital signage boards so that when passengers pass by flight information displays, their individual flight details are displayed. Similarly, personal mobility units will be activated via a person's face and used by travellers requiring assisted transport, with the wheelchair guiding the passenger across the airport. This is likely to significantly improve the independence and experiences of elderly and disabled passengers, meaning that airports will also become more attractive to a wider range of passengers.

With over 4 billion people taking to the skies in 2018, and numbers only expected to rise, it is apparent that facial recognition technology may be the answer to increasing pressure on to airports, with a new generation of people set to experience a passenger journey in which your face, really is your passport.

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

Since my last article I have been fortunate to attend two major Infrastructure events representing the International Association of Critical Infrastructure Protection Professionals (IACIPP) . The first being as a speaker at the Critical Infrastructure Protection (CIP) Forum in Bucharest in March. This was delivered through the Romanian Government as part of their programme of activities during their Presidency of the Council of the European Union and the agenda was set to explore 'Emerging Technologies Transforming Critical Infrastructure'.

The second as the Conference Chairman at the Critical Infrastructure Protection and Resilience Americas event in Tampa in May. The focus here was on 'Collaborating and Cooperating for Greater Security'.

The CIP forum in Bucharest attracted an array of international speakers from Japan, Malaysia, Nigeria, Israel, the United States and of course from numerous European Countries, all of whom had a significant degree of expertise and experience in the development and utilisation of new technologies to protect critical infrastructure. So it was not at all surprising that the major discussion points were centred around the countering of Cyber Threats in the Infrastructure Sector and the potential benefits that Artificial Intelligence will bring.

The IACIPP is in discussion with the CIP Forum and the organisers of the Critical Infrastructure Protection and Resilience – Europe (CIPRE) conference, to see if we can bring the two entities together, for a joint event in 2020. If this happens it will deliver a unique event, joining both the Eastern and Western European infrastructure community together in a great location with wider international support.

The Tampa conference also had Cyber issues as a significant concern but was designed to deliver a much broader perspective around the issues affecting protection and resilience. It too had excellent Government support from a national, regional and local perspective with agencies such as the Department of Homeland Security (DHS), The Federal Emergency Management Agency (FEMA) and the Office of Emergency Management within Tampa all contributing to a lively and extremely informative 3 days.

Emerging threats to the infrastructure sector were heavily referenced with almost everyone highlighting, that generically, the top five were broadly around:

- Extreme weather (as to be expected within the State of Florida)
- Acts of Terrorism
- Major Accidents or Failures of Critical Infrastructure
- Pandemics and
- Cyber

With the United States being one of the, if not the, most Cyber reliant nations on earth, this was always going to be a topic of interest in Tampa.

The keynote addresses were delivered by Brian Harrell, the Head of the newly formed DHS department - CISA, the Cybersecurity & Infrastructure Security Agency, and Dr Daniel Kaniewski, the Deputy Administrator Resilience for FEMA, both of whom spoke passionately about the efforts being made to combat all forms of Cyber criminality.

They also referenced the absolute need to continue creating greater connectivity across the public and private sectors within the infrastructure community and building lasting partnerships within an ever changing threat landscape.

The need for developed partnerships and information sharing is a continual theme that I see from events across the globe and was clearly evidenced at the conference as a priority for the United States Government. Both the DHS and FEMA have significant programmes in place trying to address the issue and seem to be making good progress with numerous initiatives in place.

Developing partnerships and facilitating the exchange of information is something that we within the IACIPP are

Keynote presenters at Critical Infrastructure Protection & Resilience North America - Dr Daniel Kaniewski, Deputy Administrator Resilience for FEMA; Chauncia Willis, Emergency Management Co-ordinator, City of Tampa; Brian Harrell, Assistant Director, Cybersecurity & Infrastructure Security Agency (CISA).

extremely keen to support. We believe that they are essential elements of the protection and resilience of our critical infrastructure and we are always looking at new ways in which we can assist.

As a result of feedback from our members and from the various events we are involved in, and as we continue to drive the association forward we have recently revamped the IACIPP website - *www.cip-association.org*. - in order to further enhance the available functionalities.

As a developing membership portal it now provides access to information, forums, back issues of World Security Report and previous conference papers from Critical Infrastructure Protection & Resilience Europe, Asia and North America.

The IACIPP Poll

Give your opinion

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

- Cyber security
- Risk, Crisis & Emergency Management
- Preparedness for Disasters
- Terrorism Awareness
- Identification of Threats and Hazards
- Behavioural analysis
- CBRNe

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

We have also introduced discussion groups across a range of topics including, Transport, Energy, Telecoms, Water and Cyber. These have only been up and running a few weeks but we see these as having great potential in putting like minded people together to talk through issues and exchange information.

All of these are small steps in the bigger scheme of things but they have the potential to provide real value to those of us within the infrastructure world.

Check out the website – *www.cip-association.org* and see if this may be something that you might want to be involved in.

I want to leave you with a Cyber related reference from the conference in TAMPA. Brian from DHS/CISA stated that a significant concern for them still related to the use and protection of passwords. His solution to this was really quite simple –

'Everyone should treat their passwords like their underwear -

- Never Share Them
- Change Them Regularly – and
- Please Keep Them Off Your Desk'

Sounds like good advice to me!

From video surveillance to real-time video analytics – today's solution to prevent and solve future incidents?

In some countries today, video surveillance is integrated in citizens' lives, making it easy to leap to the recurring image of Georges Orwell's masterpiece 1984, where Oceania plays the part of a state surrounded by surveillance cameras. At every street corner, every turn, every alleyway, the citizens of Oceania are observed doing the most mundane things.

Although written as a fictional piece, some people may say that 1984 seems to be closer than ever, due to the emergence of video surveillance and other monitoring technology. It seems that for the greater good, citizens are willing to give up certain aspects of their privacy. It's a fact that biometrics are already used to better our lives: we no longer need to type in our password to access our smartphone, as the phone's technology uses our fingerprint to unlock the phone. At some airports, queuing for customs is a thing of the past, as they use facial recognition and biometric technology. Automatic-Plate Recognition software keeps us safe by reducing vehicle crime – the list is endless.

Although video surveillance has not yet been implemented to the same level everywhere globally, the technology is now moving even further. With the emergence of real-time video analytics and facial recognition, many governments and responsible agencies need to ask themselves what the best use of this new technology is. The promise is ambitious: prevent an incident from happening while addressing the public's reluctance to reduce their right for privacy for the greater good.

London Viewing

Writing a piece on video-surveillance without talking about the UK would be imprecise since the country has established itself as a pioneer in the field of video surveillance. If numbers do not lie, the statistics are quite surprising:

- Around 500,000 CCTVs (Closed-Circuit Televisions) in London
- Between 4 and 5.9 million CCTV cameras in the UK
- 9 000 ANPR (Automated Number-Plate Recognition) systems in the UK and cameras in London that photograph each pedestrian almost 300 times a day.

These numbers have been steadily increasing since the UK decided to set up CCTV systems in 1990. At the time, the installation of public and private video surveillance cameras was met with skepticism. Citizens across the UK were reluctant, even if it was for a greater sense of security and peace of mind.

Today, Londoners are quite indifferent to video surveillance, notwithstanding the dramatic increase in the number of cameras between 2012 and 2015 (+ 72%). Cell phones probably play a big role in the Brits' current position on video surveillance, for people all over the world have now grown used to filming and being filmed. Whether it's at Big Ben, or the National History Museum, it is highly likely that a Londoner has been in a situation where they have been filmed by a tourist capturing a souvenir.

Younger generations are also growing up with the use of videos in a very different environment than when CCTVs cameras and systems were initially installed two decades ago. This growth in comfort and trust toward video surveillance can be explained by the fact that safety and security are arguably the most sought-after feelings. Over the past few years, many cities such as Paris, Manchester and recently Sri Lanka, have been the stage of attacks on civilians. In this context, real-time video surveillance together with video analytics can bring a deep sense of reassurance, not only for finding criminals but also for early responses. It does seem that the more cameras you are surrounded by, the better protected you feel against threats. According to the latest available data which dates back to 2013, 78% of Americans said surveillance cameras were a good idea. At the same time in France, 83% of French were favorable to public and private video surveillance. In the UK, it is engraved into people's lives to the extent where it is a moot point to ask the question.

If video surveillance has already conquered some parts of the world, other countries in Europe are still debating the matter, Germany being a prime example. Given the country's history, the Germans' reluctance to video surveillance is quite understandable. After World War II, at a time when Germany was divided into parts, the Eastern part of Germany was under communist sovereignty and millions of east-German citizens were closely monitored by the so-called Stasi (State Security).

Germany's laws on privacy and video surveillance are therefore very strict. For example, they would not allow any video surveillance cameras in places other than banks, stores or train stations, and especially not on the streets. Even in the wake of the December 2016 terrorist attack in Berlin, Germany's officials did not enthusiastically follow Angela Merkel's wish to expand video surveillance. March 2017 marks a crucial day in Germany's history as it is the day when the Bundestag passed a law extending the use of video surveillance. However, local authorities are given the deciding power.

Benefits

Video footage has given police officers and investigators a very credible source of information in cases where incidents had already happened and law enforcement forces were trying to understand criminal patterns.

Following the attacks in Sri Lanka, video surveillance cameras and video analytics helped authorities to identify a person of interest. The very presence of this video footage shows how vital video surveillance and video analytics can be in:

- Analyzing patterns, typical profiles or identifying individuals of interest after an event has happened
- Preventing a potential harmful event from happening in the first place.

In the 1990s, Brits made it a point of keeping children from football stadiums, at a time when hooliganism was on the rise. Several key measures were implemented to combat the presence of ill-intentioned supporters. One of the measures was the introduction of security cameras in stadiums. Children of all ages can now see their favorite teams play.

On December 11 2018, the 400 video surveillance cameras in Strasbourg helped operators and police officers secure areas and follow a perpetrator targeting citizens.

The case that most video surveillance advocators will rely on dates back to 2015 in the United States. As FBI investigators were at a dead-end after the Boston Marathon incident, they turned to video surveillance footage and, by cross-referencing with another source, managed to find the two perpetrators.

Surveillance cameras are of utmost importance in monitoring everyday life of a city. Video surveillance is responsible for ensuring the security of major events, whether they are political (G20 summits, meetings in parliament, etc.) or sports-related (World cups, the Olympics, stadiums, etc.). All of this in an effort to bring citizens what they aspire to most: security and peace of mind.

Securing our lives tends to be the go-to subject for supporters of video surveillance, but one should not forget that there are other scenarios where video surveillance coupled with video analytics helps citizens. In a missing person scenario, video analytics saves law enforcement agencies precious time. They are able to use footage from private or public security cameras, quickly locating the missing individual by narrowing down their location. When the camera setup allows, the police can also follow the person's movements and send in officers to ensure everyone is safe. The responsiveness of video surveillance, especially in crowded areas (malls, main streets, stadiums) makes the scenario of a missing individual much easier to manage.

Criticism to be addressed

Our need for surveillance cameras should not overshadow the fact that it is the admission that we live in a dangerous world. However, does this admission mean that we have to give up on our fundamental and reasonable right to privacy?

Even in the UK, the pioneer in video surveillance, civil liberty groups continue to raise concerns about the extension of its use. According to them, a citizen's right to privacy is impacted by video surveillance and they point out that there have been cases where CCTV footage was abused.

This leads to the arguably most effective argument against CCTV: currently, there are only very few regulations on the use of cameras and the recorded footage. It is indeed a problem one can find in technology overall: it evolves twice as fast as governments. For every beneficial use of technology, there are potential malevolent users. The intense pace at which technology is growing has left laws and lawmakers drastically behind. To ensure countries can benefit from the full potential of video surveillance and real-time video analytics, the industry needs to work alongside public bodies to develop relevant policies.

Basis for success

The future of video analytics shows promise, notably through deep-learning algorithms and A.I. Soon, operators will be able to look for out of the ordinary behaviors. Video analytics systems will be able to analyze normal behaviors, and more interestingly, draw conclusions on what abnormal behavior is. What we are talking about here is possibly one of the biggest breakthroughs in technology at the service of safety: the notion of stopping a crime before it even happens through deep-learning algorithms and behavioral analysis could be a reality.

While real-time video surveillance has been around for many years and is accepted by many, innovative biometric features are what seem to face most reluctance. Yet, they present a significant range of advantages.

Having cameras that film all the time means that whenever something happens, police officers need to watch the entirety of the video footage, which can take several hours. With the advent of facial recognition and A.I. software, the task of analyzing hours of footage manually is now over. Police officers can concentrate on solving crimes. Coupled with video-surveillance cameras, A.I. and facial recognition software represent a credible tool for solving cases, which in turn is beneficial to both citizens and law enforcement. And one critical point is: there will always be a human being involved in the process. Not machines will take any necessary decisions, but trained investigators. Systems can only save time in the decision-making process. Human minds will always be in control.

Understanding and addressing the public's skepticism is critical for the success and full use of the technology's potential. Relevant bodies together with leading technology providers need to:

- Be transparent as to how, why and where real-time data analytics are used
- Communicate on what happens with the analyzed data
- Ensure maximum data security
- Define tight frameworks to minimize the risk of misuse.

The close dialog between decision-makers, users, industry and civil liberty groups will lead to a safer environment for everyone.

About the author:

Craig Cairley has accumulated decades of experience in the implementation of video surveillance and analytics software with a focus on the UK. In his current role as Product Manager Video Analytics for IDEMIA, he is developing the next generation of real-time video analytics software called Augmented Vision.

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

Lack of evaluation in countering violent extremism may boost terror threat

A lack of evaluation of the impact of countering violent extremism (CVE) and counter-terrorism (CT) efforts may actually be increasing the threat and risk of terrorism, a new study points out.

Researchers say that national and international agencies' efforts to counter terrorism and violent extremism have lacked two key ingredients – a clear and coherent theory of how individuals change and consistent evaluation of evidence of their changing attitudes.

Now experts at the University of Birmingham are proposing a new evaluation methodology – the Innovative Moments Coding System (IMCS) – to be explored as a more reliable way of tracking changes in violent extremists' narrative accounts and life stories.

Working with partners at the Universities of Minho and Aveiro, in Portugal, researchers at Birmingham have published their findings in the journal Aggression and Violent Behaviour.

Dr Raquel da Silva, from the International Development Department at the University of Birmingham, commented: "We believe that using the IMCS could provide an in-depth view of how an individual has changed; a useful and reliable indicator in tracking how former militants' life stories change as they leave their radical and extremist views behind.

"There is currently no clarity regarding what change looks like in deradicalisation and risk reduction interventions. Indeed, the lack of evaluation of these interventions might be actually increasing the threat and risk of terrorism, instead of doing the opposite."

Researchers analysed two life-story interviews of former politically violent militants – 'Julia' and 'Jaime' – with contrasting experiences. They used IMCS to analyse their subjects' degree of change and establish the system's reliability and usefulness in tracking such people's life stories.

They note that while radicalised views may open a path to politically motivated violence, these opinions are not criminal or harmful in themselves and do not always lead to certain engagement with a violent organisation.

Moreover, they explore studies that show how unrealistic and counterproductive it is to expect offenders to renounce their commitment to certain political and religious beliefs to prove they are no longer radicalised.

"It is more accurate to expect individuals to stop committing political violence and reject violence as a personal legitimate tactic, than to expect a full make-over of their belief systems," added Dr da Silva.

"We believe that 'self-narrative change' in this context is embodied by thoughts, emotions, actions and experiences that distance the individual from the commission of politically violent acts – demonstrating continued and committed disengagement."

Researchers adapted the IMCS from clinical research and provide evidence for the successful use of this tool to reliably track narrative, non-clinical, change in two cases of former violent militants.

These changes in individuals' actions, thoughts and feelings have been termed Innovative Moments (IMs) and can be categorised at three different levels:

· Level 1 – when the individual distances themselves from the problem;

· Level 2 – when the person starts to voice how they could change; and

· Level 3 – when the individual makes the necessary changes.

Level 1 IMs are crucial at the beginning of the change process, but for lasting change to take place, it is necessary for Level 2 and Level 3 IMs to develop.

Researchers believe that applying IMCS could help to provide an in-depth view of how certain individuals have changed and why other individuals did not showcase such levels of change. IMCS could be used as an assessment tool to describe whether a particular individual benefited from an intervention.

INTERPOL agreement with G5 Sahel strengthens counter-terrorism efforts

The heads of INTERPOL and the G5 Sahel have signed an agreement which will see increased information sharing to better address current and emerging terrorist threats across the region.

The growing number of violent and increasingly sophisticated extremist groups across the Sahel - Burkina Faso, Chad, Mali, Mauritania and Niger - has resulted in the death of thousands of individuals, with hundreds of thousands more displaced.

In particular Burkina Faso has seen the growth of extremist violence over the last few months, most recently on 12 May when an attack on a church in Dablo left six dead, just two days after the release of four hostages in the northern part of the country by French special forces.

To help prevent these threats from gaining power or spreading into other countries, the memorandum of understanding signed by INTERPOL Secretary General Jürgen Stock and Permanent Secretary of the G5 Sahel Maman Sambo Sidikou, will enable technical cooperation, training, capacity building and exchange of expertise.

Funding by Germany's Foreign Office will support expansion of INTERPOL's network and capabilities as well as developing criminal analysis throughout the region.

"The security challenges facing the G5 Sahel countries continue to grow. INTERPOL is stepping up to provide additional assistance to law enforcement across the region, thanks to the financial support from Germany," said Secretary General Stock.

"Whilst the agreement we have signed focuses on these five countries, INTERPOL's global reach will help ensure that any relevant information or expertise from around the world can be accessed and used to support local investigations," added the INTERPOL Chief.

Accompanied by Jean Bosco Kienou, President of the G5 Sahel Committee for Defence and Security and Director General of the Burkina Faso National Police, Permanent Secretary Sidikou welcomed the agreement as an important part of the ongoing efforts to enhance security.

"Uniting the work of the G5 Sahel and INTERPOL will help address terrorism and organized crime which severely impact the day-to-day lives of people throughout the region," said Mr Sidikou.

"The G5 Sahel has huge economic potential, which if it is to be fully realised means we need to help these countries develop and maintain their safety and security," added the Permanent Secretary.

Under the agreement, the G5S Permanent Secretariat will be connected to INTERPOL's secure communications network. This will enable direct sharing of terrorist-related information between the G5, INTERPOL's General Secretariat headquarters, its National Central Bureaus, and the G5 Security Cooperation Platform.

INTERPOL projects, including MiLex (Military to Law Enforcement exchange), Watchmaker (Identifying and tracking individuals involved in the manufacture or use of explosives) and FIRST (Facial, Imaging, Recognition, Searching and Tracking) are also among the key areas for development at the national level across the G5 Sahel countries.

INTERPOL holds meetings on major event security

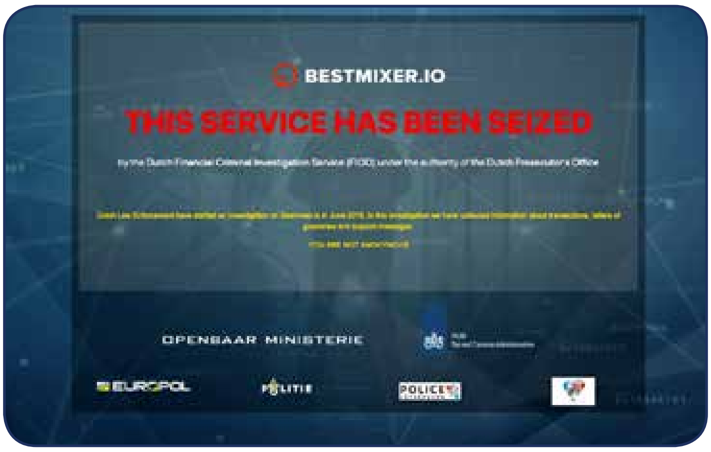
Held under INTERPOL's Project Stadia, the 4th Sports Safety and Security Experts Group focused on integrating the public and private security sectors at large international events. Experts from seven countries – Australia, Brazil, France, Portugal, Qatar, the UK and the US – as well as FIFA attended the three-day (21 – 23 April) meeting.

During the meeting, the participants shared best practices to address and mitigate potential threats facing major events.

The importance of coordination between police and private security providers was stressed, from selection criteria and training to logistics and operational coordination.

This was followed by a two-day (24 and 25 April) workshop on high-risk matches. Countries from Africa, Europe and South America detailed how they have prepared for sporting events with a high risk of security issues, such as violent spectators.

Multi-Million Euro Cryptocurrency Laundering Service Bestmixer.io Taken Down



BESTMIXER.IO

THIS SERVICE HAS BEEN SEIZED

by the Dutch Financial Criminal Investigation Service (FIOD) under the authority of the Dutch Prosecutor's Office

Dutch Law Enforcement have started an investigation on Bestmixer.io in June 2018. In this investigation we have collected information about transactions, letters of guarantee and support messages

YOU ARE NOT ANONYMOUS

The Dutch Fiscal Information and Investigation Service (FIOD), in close cooperation with Europol and the authorities in Luxembourg, clamped down on one of the world's leading cryptocurrency mixing service Bestmixer.io.

Initiated back in June 2018 by the FIOD with the support of the internet security company McAfee, this investigation resulted in the seizure of six servers in the Netherlands and Luxembourg.

ONE OF THE LARGEST MIXING SERVICES

Bestmixer.io was one of the three largest mixing services for cryptocurrencies and offered services for mixing the cryptocurrencies bitcoins, bitcoin cash and litecoins. The service started in May 2018 and achieved a turnover of at least $200 million (approx. 27,000 bitcoins) in a year's time and guaranteed that the customers would remain anonymous.

NATURE OF THE SERVICE

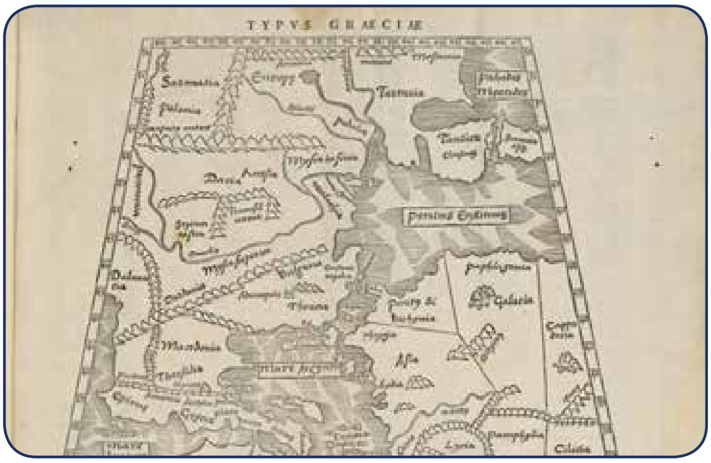
A cryptocurrency tumbler or cryptocurrency mixing service is a service offered to mix potentially identifiable or 'tainted' cryptocurrency funds with others, so as to obscure the trail back to the fund's original source.

The investigation so far into this case has shown that many of the mixed cryptocurrencies on Bestmixer.io had a criminal origin or destination. In these cases, the mixer was probably used to conceal and launder criminal flows of money.

FOLLOW-UP

The Dutch FIOD has gathered information on all the interactions on this platform in the past year. This includes IP-addresses, transaction details, bitcoin addresses and chat messages. This information will now be analysed by the FIOD in cooperation with Europol and intelligence packages will be shared with other countries.

3 Arrested for Looting Archives of Libraries Throughout Europe



With the support of Europol, the French National Police (OCBC - National Unit in charge of Cultural goods trafficking) and the Spanish Guardia Civil (UCO) have dismantled an organised crime group suspected of stealing maps in the archival collections of libraries throughout Europe.

On 20 May, 6 properties were searched simultaneously in France and Spain and 3 suspects arrested. 3 vehicles and €6 000 in cash have also been seized.

The modus operandi was well defined: one of the member of the organised crime group would enter a library pretending to be a researcher interested in consulting the archives. The individual would then distract the attention of the librarian, making the most of this opportunity to cut sheet out of XVIth century books, mainly old maps. These maps were then sold for several tens of thousands of euros on the criminal market for cultural goods.

Europol provided analytical support to prepare for the action, and deployed a mobile office on-the-spot in Montpellier (France) to extract and analyse mobile phone data on the action day itself.

Heald's Matador Range Excels in Double Crash Tests

Heald has announced the success of two crash tests for its award-winning, sliding bollard system, the Matador. The firm manufacture a range of products and solutions to protect high profile buildings and pedestrianised areas from the threat of vehicle attacks.

Heald's HT3-Matador 4 which has already been previously crash tested to IWA standards has achieved a new record with an IWA crash test against a 7.2 tonne N2A specification truck travelling at 80 kph (50 mph).

The IWA crash test is the world standard in crash testing and has been prepared by the Centre for Protection of National Infrastructure (CPNI) and British Standards Institution (BSI) with input from the US Department of State and combines aspects of PAS68 and ASTM (American standard) crash testing requirements.

Whereas the latest configuration, the HT2-Matador 6, which consists of four central moving bollards and two fixed bollards to accommodate access for large vehicles or tight turning circles has also succeeded in its PAS68 crash test, halting a 7.5 tonne truck travelling at 64 kph (40 mph).

As Heald continue to innovate the patent-protected Matador range, which has recently seen the launch of an electro-mechanically operated range removing the need for oil to operate and up to a 60% reduction in electrical running costs, they have continued to invest in crash testing to provide the market with a trusted solution to mitigate the risk of vehicle attacks. To date, Heald's Matador Range has been crash tested four times, with each test covering a variety of standards. After each test, the Matador continued to function, mitigating the risk of secondary attacks.

Due to its sliding bollard feature, the Matador range can be shallow or surface mounted making the product ideal for install in locations where excavation can be challenging due to existing infrastructure such as underground cabling and drainage. The surface mount option is ideal for short term events such as festivals and Christmas markets due to its rapid installation, while still providing the same levels of protection as its shallow mount counterpart.

Matador installations include a government facility in Melbourne, Australia and secures the perimeter of one of Norway's airports, New Orleans historic French Quarter and the Stavros Niarchos Cultural Centre in Greece. Surface mounted Matadors have also secured the World Snooker Championships and the London Olympics.

Commenting on the crash tests, Heald Managing Director, Debbie Heald MBE said "As part of our commitment to providing products which push the boundaries we are committed to putting our Matador up against some of the most stringent tests on the market to ensure we can provide products which protect from the most extreme threats. The latest crash tests cement Heald's Matador as one of the world's most effective HVM bollards".

When the unexpected happens, where will you turn? The FoneTrac travel safety app can help

It only takes a few short moments to change your life. One minute, you can be enjoying the luxury of breakfast with loved ones or the beauty of a worship service. The next, you're in shock and dealing with a horrible tragedy. For many in Sri Lanka over Easter 2019, this nightmare became reality.

Travel always has an element of danger to it. That's partially what makes it fun…to step outside the comforts of home and experience something new. However, nobody wants to face unnecessary danger or have to deal with circumstances like a natural disaster or terrorism. To help business executives, employees or even students and teachers traveling over the summer to stay safe GlobalSecur® Travel Safety introduced their FoneTrac travel safety app.

FoneTrac is a unique travel safety app that enables users to gain instant access in an emergency to security professionals. Wherever you are around the world, you can get the help needed to know how to get out of a dangerous situation. It doesn't matter what time zone you're in…FoneTrac's security team is backed by UnitedHealthcare Global's extensive 24/7 network.

In addition, unlike many other security apps out there, FoneTrac doesn't track users on a continual basis. This might sound counterintuitive, but it's actually designed with your privacy in mind. To record your location, simply log into the app and, with the touch of a button, you can "check in." This lets the security team (as well as family, friends or your boss) know that you're safe. Of course, in an emergency, you can send a "panic alert" and call the FoneTrac professionals for help.

PPSS Group Launch Cut Resistant Neck Guards To Help Protect Homeland Security Professionals

PPSS Group have launched SlashPRO® Cut Resistant Neck Guards in order to help further improve the personal safety of homeland security and other public facing professionals.

This latest addition to this widely respected brand of slash resistant clothing certainly makes sense, understanding that the side of the neck and throat contains both the Carotid Artery and Jugular Vein. If either is cut by an attacker one will most likely suffer from rapid blood loss, subsequent shock and most likely death.

PPSS Group have identified a noticeable increase in the demand for such product, especially from several homeland security agencies, such as prison, police, immigration, customs, border forces and other government agencies. Many of these agencies have reported incidents, which saw their officers being brutally attacked. Many attacks had targeted the officers' throats and necks.

Robert Kaiser, CEO of PPSS Group said: "Many government employees or security professionals have been attacked from behind. This may well be the case because they, for whatever reasons, either trusted the attacker to a reasonable level, or because the attackers put themselves intentionally into such position in order to cause max injury or even death."

"No matter how hard we try, we simply cannot eliminate their operational risks. However, what we can do is continue our research and development and relentlessly explore all possible options to further improve the personal safety of those who serve our countries and protect us."

Mobile Surveillance in the cloud? Soliton announces new cloud solutions

There was a time law enforcement and defence organizations were adamant about cloud. And that given its apparent insecurity it would never be utilized as a platform of choice. But times are evolving.

The Lincolnshire Police broke the mould in 2018 by installing the UK's first cloud-based Command and Control Room Solution, developed by Motorola Solutions. Totally in the cloud. Cloud solutions have long been recognised as a way of massively saving resources and using a subscription model to use services that can be more cost effective. Naturally security has to be addressed and with special secure data centres, private lines, encryption and a raft of IT security solutions to prevent cyber attack and access control, it has come of age that cloud-based solutions can be as secure as your own data centre within a closed network.

Soliton Systems are specialists in both IT Security and mobile surveillance and have just launched their first cloud-based solutions for live streaming specifically for the law enforcement and mobile surveillance market. Their small mobile H.265 encoders allows live streaming from the field from moving devices such as action cams worn on-person, vehicles, boats, trains, boats and drones. They can live stream over multiple 4G networks simultaneously, Wi-Fi or satellite, which can be an open public network, but they support full encryption of the video to make the video impenetrable. They are designed to work in the most challenging of situations including congested areas or where signal strength is low. At the receiving end their new cloud solutions can either create an ONVIF compliant video stream that can be fed to an existing Video Management System (VMS). Or for organisations without a VMS platform, their new Cloud View platform gives organisations the ability to record from any location and then view multiple streams from any location in the world through a secure standard browser interface.

In addition, their recent award winning Zao Android App has been integrated into the new Airbus Tactilon Dabat device which gives the opportunity to have an encrypted live stream from an Android device which can then be viewed in the cloud allowing police offices to broadcast securely in full HD for the first time from their communications devices back to a virtualised command and control centre.

Cloud has become ubiquitous across the corporate and broadcast world, but it seems the last bastion of resistance is inevitably coming to terms with the benefits of cloud.

Marlow Ropes Introduce FRR (Fast Rope Rack) into Global Defence and Law Enforcement Markets

Innovators in the field of rope technology, Marlow Ropes Ltd designed and developed the original Fast Rope in conjunction with the British Special Forces. These ropes are now in use by traditional Special Forces and SWAT teams across the globe.

Marlow are delighted to introduce the Fast Rope Rack (FRR) a lightweight stainless steel device to be used in conjunction with 40mm fast rope and to aid the rapid insertion of units. This innovative British-made device is light (1.83kg), quick and easy to install and Ideal for the insertion of non-Fast Rope qualified personnel including Medics, Interpreters, Guides and Bomb Disposal Specialists. It also offers a perfect solution when descending with a dog. The FRR has various fitting options to help with the deployment of equipment considered too heavy for insertion in normal Fast Roping conditions.

The unique construction of the Marlow Fast Rope allows comfortable control throughout the descent and makes it easier to slow down and break. The suppleness of the material means that the rope is not hard on the hands as less force is required than with other ropes. Oil and general spillage do not affect the speed of descent as Marlow Fast Ropes absorb liquids.

Other additions include, a new and improved Fast Rope bag, a Fast Rope DLT cover, alongside our range of Fast Roping gloves and hardware.

Marlow Ropes' reputation for quality and technical innovation continues and the Company continues to forge a path of progress and growth in the international markets in which it operates.

Advancements in Explosive Entry Safety: Safe Connection Set

Explosive Dynamic Entry has long been a critical tool in military special operations and urban fighting. It provides an element of speed and violence that makes it a superior tactic in gaining entry quickly and efficiently. However, for Law Enforcement the preferred method of gaining entry has been CS gas or tear gas as it is frequently called. CS gas was abandoned by the military because it was hard to control, hard to contain, hard to fight in, had adverse effects on non-combatants, especially the young, the old, and the infirm. In addition, CS gas provided very little—if any—tactical advantage. In recent years, Law Enforcement operations have evolved to look very similar to military urban warfare. As a result, we have seen that criminals have better weapons and better equipment to include the ability to fight in a CS environment. In other words, there is no tactical advantage to employing CS for law enforcement. As a result, more law enforcement departments are transitioning to explosive dynamic entry. However, explosive entry can be very dangerous for operators to transport, employ, and un-employ. Also, if you are in proximity of the explosion, it can have a catastrophic effect on both users and bystanders. For this reason, companies have recently partnered with military and law enforcement training centers to develop breaching support products that can mitigate some of the danger associated with explosive dynamic entry, such as lowering the net explosive weight of charges and making them safer, faster, and simpler to transport, employ, and disarm.

Over the years, a few products have been developed to make it easier to employ and control explosive breaching systems. Unfortunately, none of them until recently have made an impact on safe DISARM or the net explosive weight of the systems. The Safe Connection System is a two-piece clip-in/clip-out priming system that gives operators increased control over the ARM/DISARM of charges while also reducing the overall net explosive weight. This new capability allows operators to quickly and safely pair different charges and firing systems while operating in the field. The Safe Connection System also lowers Net Explosive Weight (NEW) by eliminating the need for 18" of detonation chord usually required for a "det chord loop." This makes explosive breaching safer for both operators and bystanders within the blast radius.

Piracy in Commercial Sea Lanes Remains Ever Present Danger

May has been a very busy and dangerous month in the commercial sea lanes with a number of worrying incidents reported by the IMB Piracy Reporting Centre.

In one incident in Callao Anchorage, Peru, around four to five robbers wearing face masks boarded an anchored LNG tanker via the hawse pipe. They took hostage the duty crew on routine rounds. Alarm was raised, the ship's whistle sounded and crew mustered. On hearing the alarm, the robbers took the duty crew's radio, pushed him and escaped in their boat. The incident was reported to Port Control and a patrol boat was dispatched to the anchorage area.

A few days before in the Lome Anchorage, Togo, armed persons boarded and hijacked an anchored chemical tanker and took its crew hostage. The Togo Navy received a call from the owners that their tanker had been attacked and immediately responded by dispatching patrol boats to investigate. The tanker was intercepted 25nm from the anchorage area and forced to return to Lome port. The crew were reported safe and the armed persons were captured and handed over to the Authorities.

On the 12th May, around 4nm East of Pulau Mapur, Indonesia, four robbers armed with long knives boarded a general cargo ship underway. They took hostage the duty AB and entered into the Master's cabin. They tied up the AB and the Master and escaped with their personal cash and effects.

On the 5th of May approximately 48nm SW of Luba, Equatorial Guinea, pirates onboard a previously hijacked tug approached and boarded a heavy load carrier ship underway. Alarm sounded and the crew retreated into the citadel. Regional Authorities notified. A nearby Spanish Naval vessel and the Equatorial Guinean Navy responded to the incident resulting in the pirates escaping and the crews released. The tug and the ship were escorted by the Equatorial Guinean Navy to a safe port for further investigations.

These are just a few of the many incidents in May so far and clearly show that despite international efforts, piracy remains an ever present danger.

MARSS Automated Climber Detection – CLiMBERguard automatically detects, tracks and classifies intruders scaling the side of a vessel or structure, immediately alerting operators to the climber and its location.

CLiMBERguard has been developed from the MARSS man-overboard detection technology to provide higher probability of detection and low false alarm rates for vessel security.

Heras wins tender for protecting TenneT HV substations

Heras will be providing security solutions for high-voltage substations operated by the nationwide Dutch HV substation grid operator TenneT. This includes the installation and maintenance of fences that deter and delay unwanted access.

Dirk-Jan Westendorp, Heras' Country Manager for the Netherlands: "With the energy sector being a vital part of our society, any breakdowns and malfunctions can cause serious disruption to public life. In addition, problems involving our power supply can pose a threat to our national security. It is essential that these high-voltage substations are protected round the clock and to the maximum extent, so as to keep the risk of breakdowns and malfunctions to a minimum."

Heras will be implementing effective, deterrent and delaying security measures for the various high-voltage substations in order to provide maximum protection against access by unauthorised and/or unwanted individuals. Westendorp: "Being awarded this contract is confirmation for us that Heras has a proven track record and that this is recognised as such. We look forward to working closely with TenneT in using our expertise and providing the appropriate security solutions for protecting vital infrastructure in the Netherlands."

Videalert Launches New Electric Mobile Enforcement Vehicle

Videalert, one of the UK's leading suppliers of intelligent traffic management and enforcement solutions, has announced the immediate availability of a new all electric Mobile Enforcement Vehicle (MEV). This multi-purpose MEV will enable councils to enforce a wide range of moving traffic, parking and clean air zone contraventions whilst demonstrating their commitment to reducing emissions.

Videalert has selected the Renault Zoe as the preferred vehicle for this all electric enforcement solution although other brands can be used if required. Each MEV will be equipped with two roof-mounted ANPR cameras and two colour cameras to capture contextual video evidence. These ONVIF-compliant HD cameras will deliver superior capture rates of up to 98% to dramatically increase productivity and reduce the total cost of ownership. Significantly, this capture rate is achieved with just a single pass at normal road speeds.

Used in conjunction with the latest video analytics, the Videalert electric MEV will deliver the highest productivity at the lowest operating cost in any traffic environment. The on-board systems are totally automatic requiring no manual operation.

Smiths Detection technology to be deployed in multi-member-state security initiative sponsored by the European Commission

Smiths Detection's advanced explosives and chemical trace-detection technology is to be deployed in a broad security initiative that was launched by the European Commission. Smiths Detection has leased equipment to be used in coordinated, operational trials in public spaces – including transport and other high-risk targets – in multiple European Union Member States.

The launch of this new security initiative coincides with the inauguration of the European Commission's new law-enforcement training centre – also officially opened on 20th May 2019 in the presence of Commissioner for Security Sir Julian King – which will feature several of Smith products such as Smiths Detection's LCD personal chemical detectors.

In the face of evolving threats, the European Commission is continuing its support for Member States in implementation of the 2017 EU Action Plan on Strengthening Protection of Public Spaces and EU CBRN Action Plan in detecting threats and reducing the vulnerability of public spaces to mitigate the consequences of terrorist attack.

Accordingly, the European Commission (DG HOME) has launched jointly with security authorities in Belgium, Netherlands, Luxembourg and Spain a protection trial, which has been designed to offer the law-enforcement community an opportunity to experience different technologies and introduce the use of such technologies in different public areas.

The EU protection trial will be initiated during the EU Heads of State Summit taking place in Brussels on 28 May 2019. Three different types of trace detectors are included in the lease: TRACE-PRO for revealing traces of explosives on people, vehicles and surfaces; LCD personal chemical detectors; and the portable, desktop IONSCAN 600, which detects and identifies trace amounts of both explosives and narcotics.

"This initiative fosters public-private cooperation to enhance the protection of public spaces, while still allowing freedom of movement with very limited levels of disruption to people's daily lives," commented Tony Tielen, VP Europe, Africa and Marketing, Smiths Detection. "We are delighted to be participating in this ground-breaking project and working in partnership to improve public protection. This project allows Smiths Detection's trace equipment to be fully tested in a truly operational context, assessing both its value and impact when utilised in a range of field situations."

Various security units in different operational environments and conditions will be involved, from counter-terrorism investigator units to front-line police officers operating in public spaces. The units involved are the Belgian Federal Police; the Dutch Marechaussee; the Luxembourg Police and Luxembourg Civil Aviation Security (DAC); and the Spanish Guardia Civil (GAR).

World Security Report

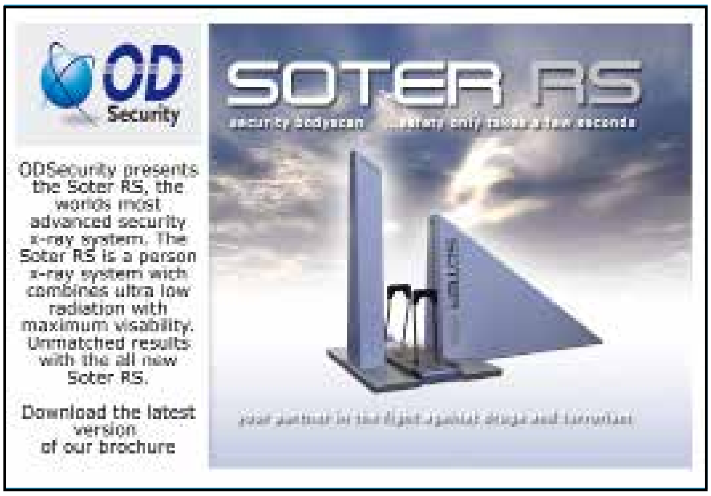
World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 130,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, security and armed forces and civilian services and looks at how they are dealing with them.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

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

www.clantect.com

Border Security Report

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


OD Security
SOTER RS
security bodyscan ... safety only takes a few seconds
your partner in the fight against drugs and terrorism

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

Download the latest version of our brochure

Wagtail International leading specialists in detection dogs and dog handler training

Click here to view our profile

International Procurement Services (IPS)
Electronic Countermeasures Equipment
Sweep Teams
Training
IPS
www.SECURITYSEARCH.Co.Uk

June 2019

18-20
IFSEC
London, UK
www.ifsec.events/international

25-26
Police Security Expo
Atlantic City, USA
www.police-security.com

26-27
Security Expo Munich
Munich, Germany
www.sicherheitsexpo.de/en

July 2019

14-16
China Defence & Police
Nan Fung International Convention & Exhibition Center, China
www.defenpolchina.com

16-18
International Cyber Security and Intelligence Conference & Exhibition
Brampton, Ontario, Canada
www.icsicanada.org

19-20
Police Expo India
New Delhi, India
www.internationalpoliceexpo.com

19-20
Fire, Safety and Disaster Management Expo
New Delhi, India
www.fsdexpo.in

24-26
Security Exhibition & Conference Australia
Sydney, Australia
www.securityexpo.com.au

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

October 2019

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