

INCORPORATING

**BORDER SECURITY
REPORT**

WORLD SECURITY REPORT

Official Magazine of



International Association of
CIP Professionals

JULY / AUGUST 2018

www.worldsecurity-index.com

FEATURE:

**Super Recognisers offer
unique and force multiplying
skills**

PAGE 9

FEATURE:

**Stark Reality of Phones in
Prisons**

PAGE 15

FEATURE:

Closing the Surveillance Gap

PAGE 17



**HEMS, DISASTER RELIEF OPERATIONS
AND EQUIPMENT PRE-POSITIONING**



**critical
infrastructure**
PROTECTION AND
RESILIENCE EUROPE

**critical
infrastructure**
PROTECTION AND
RESILIENCE EUROPE

2nd-4th October 2018

The Hague, Netherlands

www.cipre-expo.com

REGISTER ONLINE TODAY

Working together for enhancing security

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.”

**Cyber
Security
Week**
powered by The Hague Security Delta

Critical Infrastructure Protection and Resilience Europe launches Preliminary Conference Programme

Delivering an outstanding conference programme of international expert speakers contributing to the valuable discussion on protecting Europe's critical infrastructure.

Part of the City of The Hague's 2018 **Cyber Security Week**, Critical Infrastructure Protection and Resilience Europe will include topics of discussion such as:

• Risk and Resilience in CIP and CIIP • PPP Role in CIP • Emergency Preparedness and Response in CNI • Cyber Security Legislation, Best Practice & Standards • Cyber Defence Strategies • Cyber Technologies to Prevent and Protect • SCADA Systems and IT/OT Integration • Emerging and Future Threats on CNI • Space Based CNI • Human Factors, Organisation Risk and Management Culture • Risk Management in Transport, Telecoms and Energy CIP

Download the Preliminary Conference Programme guide at www.cipre-expo.com/PSG

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.

Further details and Online Registration at www.cipre-expo.com

Confirmed Speaker include:

- Silvio Mascagna, Member of the Security Union Cabinet, European Commission
- Andrew Palmer, Border Security Lead, Gatwick Airport
- Bharat Thakrar, Head of Business / Cyber Security Resilience, BT Global Services
- Mirjam van Burgel, Researcher Tele-Vulnerability, Radiocommunications Agency Netherlands
- Catherine Piana, Director General, CoESS – Confederation of European Security Services
- Mia Wannowitz, Research Associate, United Nations University, Institute for Environment and Human Security (UNU-EHS)
- Eva Stock, Research Consultant, German Federal Office of Civil Protection and Disaster Assistance
- Ivana Cesarec, Senior Advisor for Prevention Activities National Protection and Rescue Directorate Republic of Croatia
- Alexandru Georgescu, Researcher, ROMSPACE
- Assistant Professor Robert Mikac, Faculty of Political Sciences, University of Zagreb, Croatia

For further details and speaker line up visit www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Hosted by:



Media Partners:



CONTENTS

WORLD SECURITY REPORT



5 HEMS, DISASTER RELIEF OPERATIONS AND EQUIPMENT PRE-POSITIONING

UK's Midland Air Ambulance Charity have developed and implemented a new concept.

9 SUPER RECOGNISERS OFFER UNIQUE AND FORCE MULTIPLYING SKILLS

Is the relatively new science of Super Recognition the new and innovative way of fighting and preventing crime?

11 REFLECTIONS FROM CIPRA

A review of this years Critical Infrastructure Protection & Resilience Asia hosted in Kuching, Sarawak, Malaysia.

14 SOCIAL MEDIA MONITORING AS A CRISIS MANAGEMENT TOOL

With the advent of social media, an entirely new and publicly-accessible intelligence source has become available.

16 ASSOCIATION NEWS

News and updates from the International Association of CIP Professionals.

17 STARK REALITY OF PHONES IN PRISONS

The HM Prison and Probation Service in the UK has just published their long-awaited report.

19 CLOSING THE SURVEILLANCE GAP

Sonardyne look at the changing nature of conflicts and need for 'Local Situational Awareness Systems'.

22 AGENCY NEWS

A review of the latest news, views, stories, challenges and issues from enforcement agencies.

25 INDUSTRY NEWS

Latest news, views and innovations from the industry.



WHERE US GUN CONTROL LAWS AND INTERNATIONAL SECURITY COLLIDE



I'm an advocate of strict gun control and believe that the evidence is absolutely conclusive that there is a direct correlation between lax gun control in the US and the huge numbers of mass shootings and gun crime. But, I also believed that the issue is something for US citizens alone to decide and has nothing to do with the rest of us.

Well, this month that situation has changed, and US gun control has just become an international issue.

Why, because early this month US company, Defense Distributed, the non-profit gun group that hit the headlines for posting plans for 3D printed

weapons such as their own, the single shot 'Liberator', has settled a case with the federal government allowing it to upload technical data on nearly any commercially available firearm.

These guns are known "ghost guns," because they have no serial numbers and are untraceable and potentially undetectable. The Liberator for instance has only one metal working part. That's the firing pin than can be made from material easily picked up at the local hardware store and as easily hidden or disguised.

Now it is not known yet whether there will be any international licensing restrictions on the downloading of these weapon plans, but even if there is, we all know how easy they are to circumvent.

So, now we have a situation where the US Second Amendment has direct implications for international security, especially aviation. We will watch the debate now with renewed interest!

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

Contributing Editorial:

Neil Walker

E: neilw@torchmarketing.co.uk

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.



Copyright of KNM Media and Torch Marketing.

2nd-4th Oct
2018
The Hague,
Netherlands

critical infrastructure
PROTECTION AND
RESILIENCE EUROPE

www.cipre-expo.com

critical infrastructure
PROTECTION AND
RESILIENCE AMERICAS

4th-6th Dec 2018
Tampa
Florida, USA

www.ciprna-expo.com

19th-21st Mar 2019
Casablanca
Morocco

World Border
Security Congress

www.world-border-congress.com

HEMS, Disaster Relief Operations and Equipment Pre-Positioning



The UK's Midland Air Ambulance Charity (MAAC) have developed and implemented a new concept in Extending Day and Night flying Operations for Helicopter Emergency Medical Services (HEMS) that could have major implications, not just for HEMS operations but for disaster relief operations right around the world.

They call them **Community Emergency Lit Landing Sites** or 'CELLS'.

West Midlands is one of the largest regions of the UK with population 5.6 million and has a mixture of rural and urban territory including the UK's second largest city, Birmingham.

The question for MAAC was how they could increase night flying and poor visibility HEMS operations (especially to rural areas with poor local infrastructure) safely and at an affordable cost.

Well, the first obvious question for night operations is why not simply use night vision goggles?

After carrying out a study they

concluded that the initial outlay on equipment is very expensive, critical golden hour time must be taken to plan ad-hoc night missions and a requirement for ongoing training for pilots and crew, means ongoing recurrent expense. So, NVG's were rejected.

The concept they came up with instead was CELLS; which are pre-designated and pre-surveyed helipads operated by local people. These CELLS are strategically sited across the entire region to ensure maximum HEMS coverage day or night with maximum operational safety but at minimal cost.

The idea is that local people such as volunteer groups co-ordinated by the emergency services, respond to emergency calls to mark out the pre-surveyed 'Landing Zone' with portable lights so helicopters can land safely. Local road ambulances are directed to the CELLS where the patient is transferred from the road ambulance to the helicopter for fast transfer to an appropriate emergency unit.

Landing sites are chosen for their geographic distribution using analysis of emergency calls, as well as other criteria such as population

density and transfer times to Trauma and Cardiac units (in this case anything over 40 minutes).

Consequently, CELLS are mainly in rural areas with limited road networks, and can be located anywhere, such as hospitals without emergency facilities, health clinics, doctors' surgeries, police and fire stations, power stations, football clubs, sports centres, theme parks, schools and public parks.

It was an important requirement that CELLS needed to be independent of critical infrastructure such as power, terrestrial communications, roads etc. and need minimal training for operators.

The company chosen for the development of the equipment CELLS required was FEC Heliports Equipment.

FEC have a track record of delivering portable helipad lights as well as other helipad equipment to air ambulance, government agencies, the military and bodies like the UN.

For this project, in addition to their portable helipad lights, FEC developed a lockable case that can be wall or pole mounted with inbuilt charging stations for the lights. They also developed an illuminated wind sock and obstruction light all of which can be powered by wind or solar power, so that the station is independent of local power supplies and infrastructure. They called it the



HEMS Station which serves as a secure cabinet for the storage and charging of up to ten portable helipad lights keeping them ready for immediate deployment. The whole installation is fenced with access for volunteers via a key pad.

CELLS are now in operation right across the West Midlands and more are being rolled out as funds become available. Other regions around the UK are also planning to adopt this approach.

So, what are the implications for disaster relief operations?

Pre-positioning of equipment is not a new concept. The American military have been doing it for years. It means having all the equipment you need to achieve your military objective is pre-positioned in bases at geopolitical hot spots around the world. Maintenance of the equipment is carried out by the minimum number of personnel. All you need is to turn up with your combat troops as and when the need arises. Obviously, that's a massive over simplification but in principal, that's how it works.

Well, the same principal could and should apply to disaster relief operations. Time and again when natural disasters strike, isolated rural communities are cut off from communication and vital help for days, sometimes even weeks. Local resources are overwhelmed and whole communities must wait for additional resources to arrive from overseas governments and NGO's before rescue and relief missions can be mounted.

Often it is only when the first helicopter arrives in the area that the authorities and the outside world get any idea of the scale of the local casualties and are then able to assess what sort of supplies



and help are required. Depending on how degraded the local infrastructure is, it is helicopters again that are key to delivering initial relief supplies, rescue equipment and evacuation.

What is clear from experience is that in almost any type of disaster, whether it is flooding, earthquake, tsunami, forest fires, dam collapse or something man-made, in the initial phase helicopters are critical to the immediate response.

Therefore, it makes sense to build emergency response and resilience around helicopter operations. Day and night!

That's where the MAAC CELL concept comes into its own. By carefully selecting and surveying CELL sites for those communities most at risk and co-locating emergency relief supplies and equipment at a CELL site, not only can you provide local communities with daily HEMS coverage for their more routine emergencies, but you equip them with the means to help themselves in the event of a major disaster. The same CELL equipment can be used as marking an air strip for fixed wing aircraft, space permitting.

And it doesn't have to be expensive. Everything you need is available commercially off the shelf and at affordable prices. All you would need is a HEMS-Station



(£20,000), 40ft shipping container/s (between £4,000 and £6,000 each) the relief supplies to go in it and enough fencing to surround it.

Of course, none of this matters if you can't communicate with the outside world in the first place. But again, recent developments in mobile communications make this much more doable and affordable. Everyone has a mobile phone today, even in most of the world's poorest countries the number of mobile phones per head of population is in the high 80's and 90's percent. But of course, those mobile phones are useless if the GSM infrastructure, which is very vulnerable, goes down.

Companies like Thuraya produce what they call a Satsleeve (£480), which turns most common mobile phones into a satellite phone or the Satsleeve hotspot that you simply connect your smartphone

via Wi-Fi to the satellite unit. The sound is now routed through the smartphone, allowing users to make their calls directly from the smartphone or phones.

US company make the goTenna Pro (£380 per unit), which provides the portability and accessibility of traditional voice radios, but instead of voice, it focuses on offering digital communications for smartphones and their applications. It creates long-range multi-hop wireless networks without any infrastructure for smartphones. It provides text communication only via free apps like WhatsApp or messenger and can be used for group communication or between individuals. But importantly it provides geolocation of every member of the network, which is vital for rescue operations.

Then of course you fill the rest of

your container with all the things you need to keep people alive until help arrives like first aid kits, emergency generators, fuel, tenting, thermal blankets, water purification kits, dried and tinned emergency rations, solar chargers, batteries, work gloves, crank radios and torches etc.

Obviously, the CELL site locations, the mix of equipment and supplies will depend on local conditions and perceived threats, but it is not inconceivable to envisage everything you need to deliver a CELLS in a container for not much more than around £50k. A small price compared to delivering the same supplies after the event.

But the real beauty of this approach is that CELLS can make a tangible difference to the everyday lives of people in isolated communities by providing that safe day and night landing zones and landing strips for aircraft, as well as an emergency lifeline in times of major disaster.

(NB all prices are approximate)



critical infrastructure PROTECTION AND RESILIENCE AMERICAS

December 4th-6th, 2018
Tampa, Florida, USA

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.

Registration Now Open

Register today and benefit from Early Bird delegate fees

For further details visit www.ciprna-expo.com/registration

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. This directive supersedes Homeland Security Presidential Directive 7.

We must be prepared!

All Federal department and agency heads are responsible for the identification, prioritization, assessment, remediation, and security of their respective internal critical infrastructure that supports primary mission essential functions. Such infrastructure need to be addressed in the plans and executed to the requirements of the National Continuity Policy.

Join us in Tampa, Florida for the premier event for operators and government establishments tasked with the regions Critical Infrastructure Protection and Resilience.

The conference will look at developing on the theme of previous events in helping to create better understanding of the issues and the threats, to help facilitate the work to develop frameworks, good risk management, strategic planning and implementation.

For more information and online registration visit www.ciprna-expo.com

**Leading the debate for securing America's
critical infrastructure**

Confirmed speakers include:

- Chauncia Willis, Emergency Coordinator, City of Tampa
- Brian Harrell, Managing Director, Enterprise Protective Services, Duke Energy Corporation
- Fred Ruanavar, Chief DISA/DoDIN
- Michael Cotton, National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Science (ITS)
- Jessica Yuzwa, Project Administrator, Franklin County Office of Homeland Security and Regional Communications, Ohio
- David Alania, International Expert/ Adviser, Georgia
- Jeff Gaynor, President, American Resilience
- Deborah Kobza, President, International Association of Certified ISAOs (IACI)
- Michael Hamilton, Founder and President, Critical Informatics
- Peter Murphy, Director and Co-founder, Noetic Corporation
- John Esquivel, Senior Director, AECOM
- Christian Morin, VP Cloud Services & CSO, Genetec

For speaker line-up visit
www.ciprna-expo.com

To discuss exhibiting and sponsorship contact:

Paul McPherson
Exhibit Sales Manager
E: paulm@torchmarketing.co.uk
T: +1-240-463-1700

Owned & Organised by:

Supporting Organisations:

Media Partners:



Super Recognisers offer unique and force multiplying skills



The relatively new science of Super Recognition has lately received considerable publicity as the need to find new and innovative ways of fighting and preventing crime becomes ever more urgent. As crime rates rise, and detection/prosecution rates fall, as international organised crime becomes ever more profitable and as the threat from extremism fails to recede, Super Recognisers are being mobilised, bringing their unique and force multiplying skills to bear.

Many academics are of the opinion that Super Recognisers have now an increasingly important role to play in defence, security and policing operations. There has been a small, select section of trained police officers who are Super Recognisers based at Scotland Yard for around the past 8 years – they came into their own following the London 2011 riots. The German Police have recently set up a similar team and it is understood that Australian and Brazilian police are studying the concept in earnest at this time. More nations are likely to follow the British lead as the advantages and opportunities of such skills are realised.

Research suggests that Super Recognisers represent under 1% of the global population. They are the polar opposite of those individuals who suffer from prosopagnosia, commonly known as face blindness. Their memory skills cannot simply be taught, they are present from birth, but they can be enhanced by training. The increased availability of online tests enabled via the world wide web has allowed many more individuals from around the globe to try out their prowess at facial recognition – over 4 million individuals have now been screened. Examples include the Cambridge Facial Recognition Test (CFRT). As well

as being outstandingly good at remembering and recalling faces, notwithstanding aging or disguise, they are highly adept at behavioural analysis, able to spot likely offenders even before they commit their crime.

New autonomous facial recognition software (FRS) is being developed and deployed in many countries and these will undoubtedly have a positive effect on preventing and solving crime. Super Recognisers provide the essential human input to such technology – they add value to FRS which can cue Recognisers onto persons of interest but also provide the confirmation to AI system

alerts which uniquely only the human eye and human judgement can deliver. They can reduce error rates and give confidence to civil rights campaigners who have concerns about AI systems and potential losses of privacy.

Like any new science, standards and codes of conduct need to be established if the new techniques are to be accepted by the judiciary, the law enforcement community and society at large. To this end, the Association of Super Recognisers (ASR) is being established to set and maintain ambitious standards and to provide confidence to community leaders and politicians alike. The ASR website will provide a forum for debate, the exchange of experiences and the general development of the cohort of Super Recognisers wherever they may be working. Affiliate and licentiate levels of admission are available depending on experience, qualifications and training. The ASR will include a group of academic advisors who will monitor the development of the skillset and ensure that the trade is underpinned by the very latest research and development. Background screening and training as expert witnesses will further enhance the credibility of this new and exciting branch of crime fighting science.

Super Recognisers have numerous roles to play. They can be deployed either overtly or covertly, on the ground amongst the crowds at a race meeting or in CCTV monitoring or control room for a major demonstration, perhaps monitoring a shopping precinct where thieves and shoplifters are known to ply their illicit skills. Such operations may take place at a music festival to deal with known ticket touts or even drug dealers. They may be deployed at football stadiums to identify and deal with those who may have had banning orders issued against them or who are known troublemakers. They are invaluable at border crossings, air and sea ports of disembarkation to reinforce e-passport and conventional immigration operations. In the surveillance age, much of the video and imagery recorded is never even looked at, let alone is it ever analysed. This is what Super

Recognisers do, making the best use of the investment in high definition cameras and recorded as contemporary CCTV systems proliferate and offer low light, 24 hours, poor weather performance. By using techniques such as linked series analysis, Recognisers can identify individuals who may have committed numerous crimes, each time using a different disguise or appearance. They can piece together a jigsaw of crimes committed in different police authority areas by examining imagery from different forces and agencies and picking out those who are common to many scenes of crime no matter how geographically separate. There has never been a more crucial time for sharing imagery and footage of known, wanted criminals on a national and international basis if the battle against evil is to be won.

The ASR recently held its first ever awards ceremony at the prestigious Apothecaries Hall in the City of London. Lord Lingfield, the Chairman, presented certificates and announced the first Fellows of the Association followed by a lunch for families and friends of the recipients.

For more details go to www.associationofsuperrecognisers.org



Reflections from this year's Critical Infrastructure Protection and Resilience Asia



At this year's Critical Infrastructure Protection and Resilience, Asia in Kuching, Malaysia, over 3 days 140 delegates participated in a training session delivered by Cyber Security Malaysia and listened to 30 presentations on both physical and cyber security from a distinguished panel of speakers from right around the world.

The programme covered everything from emerging threats, both physical and cyber, to big data. Inter-agency and international co-operation once again featured heavily as it always does wherever we host these events but cyber loomed large on the minds of many as the world struggles to find the right tools to protect society from this modern scourge.

The conference was opened by Yang Berhormat Tan Sri Datuk Amar Dr. James Jemut Masing Deputy Chief Minister and Minister for Infrastructure Development and Transportation Sarawak.

He stated that critical infrastructure protection is a major issue for



governments the world over and in Malaysia it is a key priority. That's why Malaysia has invested considerable time effort and public funds developing the organisations, tools and policies to protect our citizens.

According to the research by Malaysia Communication and Multimedia Commission (MCMC), from 32 million peoples in Malaysia, 24.5 million users (76.9%) have an access to Internet. In 2017, the Malaysia's Internet penetration had risen to 85.7 per cent from just 70.0 per cent in 2015. It shows information technology and communication (ICT) is experiencing rapid growth in Malaysia.

In 2017, CyberSecurity Malaysia received a total of 7,962 cyber security incidents reported to Cyber999 Help Centre. From Jan until June 2018, there are 3,280 incidents reported. The top four incidents reported are fraud (2,158

incidents), intrusion (514 incidents), malicious code (192 incidents) and cyber harassments (170 incidents).

The National Cyber Security Policy (NCSP) is one of the most important measures taken to secure the cyberspace and forms the foundation of Malaysia e-Sovereignty.

The implementation of NCSP is under the supervision of the National Cyber Security Agency (NACSA), National Security Council. NCSP is a comprehensive initiative to tackle cyber threats, especially in the protection of the 10 critical sectors in Malaysia which are Defence and Security, Transportation, Banking and Finance, Health Services, Emergency Services, Energy, Water, Information and Communication, Government Services, Food and Agriculture.

For my part, in my own presentation I looked at a number of innovative concepts and technologies that I feel address some specific issues facing the global critical infrastructure protection and resilience community.

Legacy Systems

The first issue I looked at was securing critical infrastructure protection integrating legacy systems, which is one the most pressing problems facing CNI operators.

Be it CCTV, radar, RF, ground sensors, motion sensors, thermal imaging, electro-optics or sonar, unless it is a new installation virtually every CNI site will have a whole range of security systems that have been installed and operated over a number of years and represent a considerable investment that cannot easily be replaced.

These systems usually have their own operating systems that don't necessarily talk to one another making integrating them into a single command and control system a major problem.

So how do you get these systems to work as one?

One company MARSS, say they have the answer with their system, NiDAR. MARSS developed the NiDAR system over 10 years of research and collaboration with the European Union, European defence agencies, NATO and academia.

MARSS say that the NiDAR command and control system will integrate many sensor or surveillance systems and uses proprietary software with open-source and artificial intelligence to deliver real time analysis and increased situational awareness.

NiDAR uses advanced algorithms developed in cooperation with NATO to determine the risk of threats in the surveillance area. It does this by analysing behaviour patterns such as shape, size, history, background checks



and external factors such as weather and location.

Anomalies are highlighted to the operator for further investigation.

A common issue with traditional port or coastal protection systems are the high false alarm rates, to such an extent that systems are often deactivated by operators.

NiDAR approaches this challenge by assessing the risk posed from each contact in the surveillance area based on the multiple Risk Evaluator (RE) Modules. Its sophisticated engine combines the results of multiple RE modules to determine a Target Risk Level based upon which it alerts the operator.

NiDAR the system provides both short and long-range air, surface and underwater detection

NiDAR Risk Evaluator sensitivity can be tuned according to a 3-tiered security environment level (based on US Coast Guard MARSEC levels) set by the supervisor.

NiDAR can also integrate all your mobile assets into the system, including fast patrol boats, light patrol vehicles and even drones.

This means that mobile assets become an integral part of the system, extending the coverage of the surveillance area and whilst



keeping team members informed of the tactical situation at all times.

NiDAR has been installed at key government, CNI sites, high value merchant vessels, VIP homes and even super yachts.

MARSS also produce their own multi-sensor.

It's called RADiRguard and is an all in one sensor, which includes radio monitoring, radar, CCTV and IR.

It provides enhanced situational awareness and increased reaction time, as detection takes place in advance of reaching the fence, tracking continuously over the fence and inside the perimeter.

Typical multiple RADiRguard Pods are interlinked to make up a full perimeter system

The multiple sensors provide internal and external surveillance and the behavioural analytics ensure minimum false alarms

Precise tracking means that the systems behavioural analytics can detect anomalies and notify security staff, such as cars doing multiple drive pasts, turning around

unexpectedly or slowing down and stopping in the surveillance zone.

Security Screening

Next, we looked at a pilot scheme for Security Screening run by the Singapore Navy for the Changi Naval Base.

Historically, Security Screening and Access control at the Changi Naval Base involved between 25 and up to 35 people.

Performing the clearances for individuals and vehicles at the gate resulted in unnecessary delays and congestion.

It was obvious that this was a waste of manpower, time and resources, so they decided to run a pilot scheme using biometrics and smart technology.

It was decided to test three biometric technologies; facial recognition, finger print and iris recognition.

The company selected for the trial was IDEMIA. And the products tested were:

Biometric Capture Technology •

MorphoFace • IAD • MorphoWave
Biometric Matching Accuracy •
1:1 • 1:N Digital ID Creation and
Authentication • SmartFlow suite •
Licence2Go (digital licences)

Volunteer naval staff at the base were biometrically scanned and asked to perform numerous test accesses to the base over a period of 40 days.

Over the 40 days, they carried out about 2,500 trial runs on the biometric systems to test the accuracy of its data collection. Trials were also carried out on twins and similar-looking people, which the system easily differentiated. The team even made a rubber cast of a trial participant's face and tested it on the facial recognition scanner, which detected it without problem.

Regular non-naval visitors to the base such as support staff, delivery drivers were able to renew their passes and register vehicles via a telephone app. Saving time and money.

Having tested all three biometric technologies, the Singapore navy selected two for speed and accuracy. Facial and IRIS recognition.

Staff requirement for this activity at Changi Naval Base will be reduced to five based on the lessons learned from the pilot.

The global CIP community will be reconvening in The Hague, October 2nd to 4th for Critical Infrastructure Protection and Resilience Europe and in Tampa, Florida, 4th to 6th December for Critical Infrastructure Protection and Resilience North America. So, the only way to join the discussion is be there.

Social Media Monitoring as a Crisis Management Tool



The kind of information collected for adversary analysis has changed significantly. With the advent of social media, an entirely new and publicly-accessible intelligence source has become available.

Today, when managing a crisis situation, it is becoming increasingly common to use social media channels as essential sources of information. The very nature of social media – the fast-paced, instant and global reach – makes it the ideal source from which to monitor, analyse and even predict developments in communities, networks or groups of people with regards to a social issue, a public sentiment or specific event that may pose an organisational risk.

Whilst social media channels are not in themselves a new development, what has amplified their importance to crisis management teams is the concurrent emergence of technological solutions that have the ability to collect and analyse large amounts of data.

Trained analysts are able to evaluate and interpret the data sourced from social media platforms such as Twitter, Facebook and Reddit to build more precise and current adversary profiles and incident models.

A case study that can help to illustrate the advantage of using social media monitoring to inform an organisation's approach to crisis management is the current political unrest in Nicaragua. What began as small-scale protests against changes to the social security system in April 2018 has since grown into nationwide and large-scale anti-government protests. By late July, the Nicaraguan Association for Human Rights had counted over 440 fatalities, at least 700 disappearances and illegal detentions, and countless

persons injured during protests and altercations.

Amid the unrest, many Nicaraguan citizens as well as numerous civil society groups, NGOs and news outlets have been very active on social media. Monitoring, analysing and evaluating their use of social media can help to create a more comprehensive understanding of the specific risks faced by organisational assets. The networks in which social media users are active can reveal the group membership of individuals or help gauge the size and strength of a group. The level of online discussion regarding an event can also indicate the amount of attention or controversy there is related to the event and, based on these conversations or

comments, analysts can estimate the size of a protest or if violence should be expected.

In the Nicaragua case study, social media monitoring ahead of a large, scheduled protest, the Marcha de las Flores on 30 June, was used to assess the potential crowd size and level of expected violence. First, online comments by individuals, NGOs, civil society organisations and news outlets were evaluated to gauge the general interest in the event. Second, by analysing conversations in monitored networks of identified potential actors (both groups and individuals) analysts were able to measure the potential for violence at the march. Based on this collective analysis, a more comprehensive threat picture could be generated, and organisations were better able to comprehend the risks to their in-country assets and operations.

This case illustrates how the utilisation of new technology and contemporary sources of information such as social



media monitoring can prove integral to organisations operating in volatile or unstable environments. In the future, social media monitoring and evaluation is likely to continue to grow in importance as more sophisticated analytical software with access to an enormous amount of online data shall increase its potential and importance.

NYA RISK



ICS Cybersecurity. Safety. Compliance.

You Cannot Secure What You Cannot See

Gain configuration visibility into
proprietary ICS cyber assets

cyber.pas.com





Playing your part in the protection and resilience of our infrastructure and information

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

I have just returned from the delightful city of Kuching, the capital of the State of Sarawak in Malaysia where the International Association of Critical Infrastructure Protection Professionals were supporting the Critical Infrastructure Protection and Resilience Asia (CIPRA) conference and I was honored to have had the opportunity to Chair the event.

As we are all aware, there is an increasing reliance on the delivery of the services provided by a nation's critical national infrastructure. It serves as the backbone of economy, security and health. It provides the clean water that we drink, the power to our homes, the transportation that moves us around, the communication systems we rely on and much more.

So, it follows, that the loss or interruption of any critical part of national infrastructure or information could have a significant impact on the operational ability of a country, a severe detrimental effect to its economic wellbeing and impact on the safety and security of a region or nation.

It is therefore vital that Governments, the private sector, academic institutions and like minded individuals seek out opportunities to share good practise, explore new innovations, and to develop discussion to ensure a continued focus on the reduction of vulnerabilities within infrastructure and an increase in their overall resilience.

Conferences, such as this are, in my opinion, an ideal platform for bringing people together to focus in on the ever evolving threats that we all face and to discuss what is being done internationally to address such threats.

The event in Kuching ran over 3 days. Day one was a specialized training day on Cyber defense strategies: tools, techniques, response and procedures led by CyberSecurity Malaysia. They are an agency under Malaysia's Ministry of Science, Technology and Innovation set up to be the national cyber security specialist centre for Malaysia.

CyberSecurity Malaysia, along with the National Cyber Security Agency (NACSA) were major contributors to the full conference agenda, which saw some excellent presentations by some distinguished and experienced speakers from across the globe.

The Deputy Chief Minister for Sarawak gave the keynote address where he clearly articulated the commitment of

government in terms of time, effort and money in developing organisations, tools and polices to protect critical infrastructure and information within the region. He focused in on cyber concerns being at the very top of the Malaysian governments agenda.

It was probably not surprising, given the current climate of threats, that cyber activity was a major topic of discussion. Several speakers touched on other threat factors, such as, natural disasters and terrorism but without doubt the major concern around critical national infrastructure and information within Malaysia and the wider region at this time relates to the threats they perceive through malicious cyber acts both by terrorists and the wider criminal fraternity.

Cyber activity is the 'issue of the day' for Malaysia, but as we all know it is also challenge for all nations globally. When you start to look at the startling speed at which technology continues to advance we can clearly see the benefits that it will bring to our societies but also the potential for those who would wish to exploit new opportunities to create disruption and seek out financial gain.

Some of the figures that were quoted by various speakers at the event clearly demonstrates the speed of that development. We were told that there were currently 25 billion connected devices to the Internet – set to rise to 50 billion by 2020 and 100 billion by 2025 and that the estimated cybercrime costs to the global economy is estimated at around \$450 billion.

With the advent of all things being connected we will undoubtedly see greater attack surfaces and increased vulnerabilities developing around our infrastructure.

It is, therefore, vital that all who have a part to play in the protection and resilience of our infrastructure and information continue to meet, discuss and share experiences to ensure our understanding and response to current and future threats develop at a greater pace than those who would seek to do us harm.

So, if you are involved in critical infrastructure protection, please don't hesitate to get in touch via info@cip-association.org.

Stark Reality of Phones in Prisons



The HM Prison and Probation Service in the UK has just published their long-awaited report into what drives the demand for illicit mobile phones by prisoners, with the hope to potentially identify effective ways of preventing their use.

The results of this report starkly highlight the differing views of the Security Staff within the prisons and that of the prisoners themselves and emphasises the need to strictly control the access of phones into the UK prisons.

The report was conducted in Spring/Summer of 2014 and consisted of a survey of all prison establishments across England and Wales, semi-structured interviews with 20 Heads of Security and 67 prisoners across 20 prisons, a review of literature on the use of illicit mobile phones in prison, and a small scale limited content analysis of material found on confiscated mobile phones.

Heads of security cited that “the trafficking of illicit mobile phones as one of the major risks they faced in maintaining prison discipline and providing a decent and secure environment” and that “Mobile phones were seen by both the security function and prisoners as a major component of the illicit prison economy, with mobile phones acting as a key facilitator of drug dealing and use within establishments. ”

The report found that although a variety of mobile phones

were being used within establishments, the smaller, easier to conceal phones seemed to be the most sought-after models, as smart phones with greater functionality were at a greater risk of detection and confiscation.

Prisoners themselves commented that mobile phones were a feature of prison life and economy, regardless of type of prison, although they did comment on the fact that higher security prisons were harder to traffic phones into.

Although, nine out of ten prisons surveyed agreed that illicit mobile phones were used for drug dealing within the prison and Heads of Security said that illicit phones were being used by organised criminals to continue to run criminal business from inside the prison, and that they also created instability and exposed vulnerable prisoners and their families to bullying, exploitation and extortion. The flip side is that they were also being used by other lower profile prisoners simply to keep in contact with partners and family. Prisoners themselves also agreed that “the presence of mobile phones in prisons also worked to moderate the potential for violent confrontation between prisoners” and that given the situation where prisoners were “increasingly

locked up for extended periods, access to mobile phones acted to defuse the resulting tension and resentment, which might otherwise lead to confrontation with staff.”

The report detailed that “both mobile phones and in-cell phones enabled prisoners to sustain richer and more meaningful relationships with family members and that those able to maintain effective relationships with family and friends were better able to cope with their sentence, more realistic about resettlement and more motivated on desistance.”

A range of different methods are being used in establishments to search for illicit mobile phones and SIM cards. At the time of the research, physical searching was one of the most commonly cited methods to aid detection of illicit mobile phones.

However, the view from the Heads of Security was that mobile phones were not about to go away any time soon this was echoed by prisoners who opined that both the economic and human drivers of the demand for mobile cell phones means that it would not be possible to stop mobile phones entering UK prisons in significant numbers. And that “the demand for phones were so strong that there would continue to be a constant flow of mobile phones into prison, even as prisons became more effective in preventing entry.”

So, the stark realities remain that to aid Prisoners rehabilitation and to lower recidivism rates it is important to ensure prisoners have access to mobile phones, but on the flip side, if prisoners have mobile phones then they can continue with the very crimes that they are currently in prison for. It is almost a chicken and egg situation.

This report coincided nicely with an announcement by the UK Justice Secretary, David Gauke as he launched a fresh crackdown on crime in Prisons.

A £30 million prison improvement package which includes a £7million investment in safety. This will fund a range of new security measures, including airport-security style scanners, improved searching techniques and phone-blocking technology together with £7m on in-cell telephones for more prisons. Currently most prisoners queue for public phones on the landings, which can be the trigger for violence or fuel demand for illicit mobile phones. Some UK modern prisons have in-cell phones with strict security measures, meaning calls to family can take place in private.

If the new measures are to work, and prisoners who need private access to a phone network, then the illicit mobile phones making their way into UK prisons needs to be stopped.

One system that is currently operational in prisons in over 30 countries is the SOTER RS Body Scanner.

The SOTER RS Body Scanner is an ultra-low radiation full body scanner which can find contraband that has been hidden on a person, and more frequently, in, a person.

Jan Steven Van Wingerden, CEO of ODSecurity, manufacturers of the SOTER RS Body Scanner said, “One of the strengths of our system is that regardless of how small an item is, and whether it has been ingested or inserted, the SOTER will find it. We pride ourselves on our products ability to find items that cannot be detected by conventional metal detectors or strip searches. It is important when searching for contraband that you can differentiate between human and other materials, to limit false positives, and wasted time. SOTER RS comes with its own software, and any hidden object, regardless of what material it is made from is found within 10 seconds!”

He continued, “SOTER has had terrific success in many prisons and correctional facilities the world over. Of course, due to the nature of the establishment, figures however can rarely be published. A report from Canada on our equipment can be read here; <https://wordpress.com/view/custodyanddetentionsecurity.com>”

Closing the Surveillance Gap



The changing nature of conflicts has seen different threat profiles for military and commercial waterside and on-water assets. Asymmetric warfare and the increased threat of terrorism is driving new requirements for surveillance systems that include short range capabilities as well as long range sensing systems; these 'Local Situational Awareness Systems' (LSAS) are becoming critical for the protection of military and high value/important civil facilities.

The requirement for LSAS has also resulted in surveillance systems becoming more sophisticated with the use of advanced sensors such as short-range high definition radars combined with long range and thermal cameras that use video analytics for the detection, classification and tracking of potential intruders.

It is important that such systems deliver complete coverage of the environment around the asset, including the underwater domain. Potential attacks by divers and/or underwater vehicles, including AUV's and UUV's, will cause a disproportionate impact if successful in

attacking the military facilities, vessels or critical national infrastructure, and so must be protected against.

Recent advances in intruder detection sonar systems provide Navies and security services with the capability to



Figure 1 – Divers near a waterside asset

monitor the underwater environment and so have full situational awareness, both above and below water, when combined with other sensors. These systems will detect the presence of underwater intruders, classify and track the intruders alerting operators to potential threats to the protected facility.

These intruder detection systems must provide reliable performance in detecting threats at the required range such that appropriate action to interdict the threat can be taken. The reliable detection of underwater threats in the acoustically hostile



Figure 2 – Diver Delivery Vehicle (DDV)

environment of a seaport, harbour or critical national infrastructure using sonar is a notoriously difficult challenge to overcome. Constant vessel traffic, noise from active depth sounders and a complex thermal structure characterise the environment. However, intruder detection sonars have proven to work in these complex environments, Sonardyne's Sentinel IDS has tracked divers to ranges in excess of 950m in good conditions and can achieve ranges of over 600m in all but the most challenging environments.

To understand the complex environment, maximise the sonar's performance and ensure users know the detection and tracking ranges that they are going to get from their sonars, Sonardyne has developed a modelling tool that takes in multiple environmental measurements and observations and produces a graphical representation of the predicted ranges for target tracking, as shown in Figure 3.

This tool ensures that the sonar system can be configured and deployed to meet users' operational requirements and provide robust detection of potential threats.

It's essential that an underwater intruder detection system does not cause unnecessary workload by falsely reporting the presence of an intruder. Continuous false alarms can also lead to operator fatigue, whereby alarms are mostly ignored knowing that it will

probably be false.

The system has to automatically remove false alarms to provide ease of use for the security operator while also being simple to operate. Sentinel IDS achieves this by using Automatic Detection and Tracking (ADT).

The ADT is a multistage processing technique that ensures operators are alerted to potential threats while minimising false alarms. The process is discussed below.

Target classification is a key process to minimising false alerts and the following characteristics form part of the decision-making process for alert generation:

Behavioural Filtering; target speed, trail length, signal to noise ratio, asset range rate of direction change and purposefulness

Sentinel's Acoustic Signature Classification (ASC) process uses characteristics of the passive sonar signature to classify the type of threat into the following threat types; SCUBA diver, closed circuit diver or machine.

The results of the tracking and classification stages are used to set the system alert level.

The classification filters are

implemented in 4 stages:

Stage 1 – selects tracks for display based on some of the filters described on the previous slide. Used to set an initial alert level.

Stage 2 – repeats the filters in stage 1 with more stringent settings. Used to raise the alert status one level higher.

Stage 3 – raises alert level further based on the purposefulness of the track.

Stage 4 – monitors the hostility of a track towards any defined Asset, either by virtue of their trajectory or proximity. Will raise the alert status to the highest level.

The multi-level alerts mean that the operator should start to monitor a track at Stage 3.

If the ADT system is showing a track, it's because something is there, and moving in a way that passes the classification filters.

The filter settings are designed to minimise showing tracks of moving objects that do not present a threat (e.g. biologicals such as shoals of fish, sharks, marine mammals, or boat wakes) but occasionally a biological may move like a threatening target long enough to raise an alert.

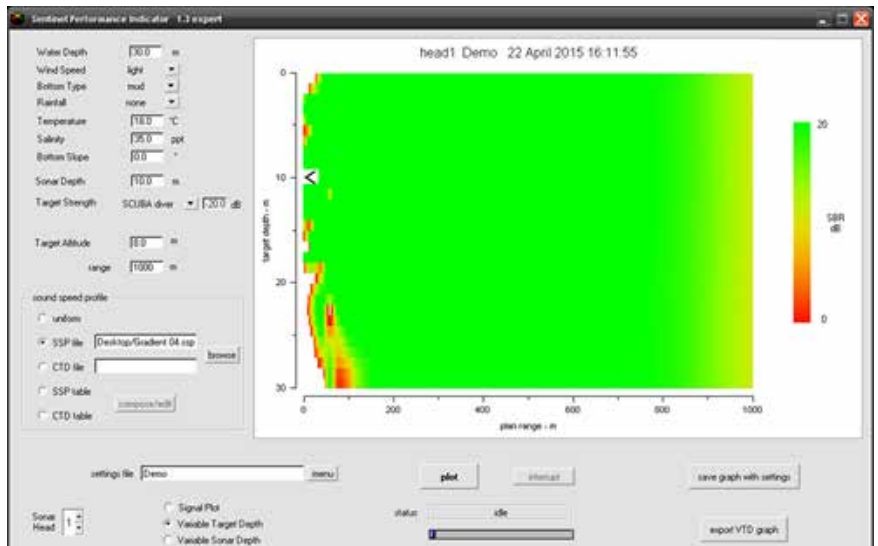


Figure 3 – Sentinel Performance Indicator (SPI)

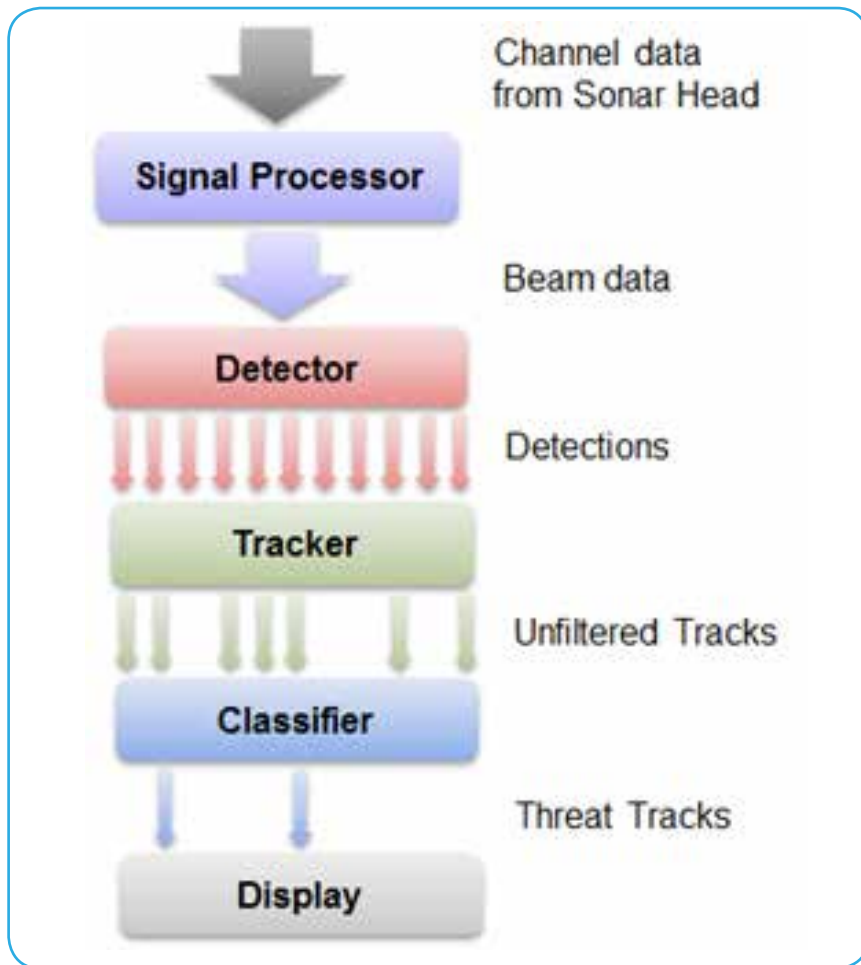


Figure 4 – ADT Process

Once detection has occurred slow to cue camera systems can be focused on the location of the potential threat providing increased situational awareness. Integration of intruder detection sonar with command and control system will provide enhanced threat detection giving advanced warning providing time to react and mobilise response teams to enable interdiction. The response plan would be developed as part of the local site CONOPS.

Scalable and Flexible Deployment Options

The types of water side or vessel that need a surveillance capability can be extremely varied, from large ports and harbours through to small vessels. Having an IDS with a scalable architecture and deployment options for the different applications gives a

number of advantages. It means the same sonar technology can be used in all applications. There is a reduced training and flexibility of operating and maintenance. Commonality of spares and a reduced logistics footprint

Sonardyne's Sentinel is an example of such a system and can be deployed in numerous configurations, including:

- Single head portable system for use from a vessel. The sonar head can be deployed on a cable below the vessel hull, or on a portable tripod on the seabed. The IDS can either be standalone, or the vessel can be 'fitted for, but not with' so cabling is in place and the sonar output can be fed into the ships CMS or surveillance system. Sonardyne have recently supplied portable systems for use on OPVs
- Vessel mounted through hull

deployment system. The IDS can be mounted on a through hull deployment system that enables very rapid deployment on the vessel.

- Single or multi-sonar head systems for deployment on shore side facilities. Multiple sonar heads can be connected into a single system to provide a single surveillance picture of the underwater environment. Sonardyne's Sentinel enhances the multi sonar capability by providing 'track stitching' which maintains the track of a target as it moves from the coverage of one sonar to another.

COTS diver detection systems are available and operational today. System design needs to be based on all of the user's requirements. It is important to understand the environment before designing and installing the system. An integrated surveillance system that does not have a diver detection system has a serious vulnerability.

Andrew Wood
Sales Manager – Maritime Security
Sonardyne

ATEFI signs Strategic Agreement with AMERIPOL

The Latin American Association of Operators Electronic Funds Transfer and Information Services (ATEFI) has signed an Agreement of Understanding and Mutual Cooperation with The Police Community of the Americas (AMERIPOL). This public-private sector Agreement, signed in Buenos Aires (Argentina), enables ATEFI and AMERIPOL, through collaboration and mutual professional training, to carry out preventive and

investigative actions through forensic analysis of fraud and cybercrime cases.

In May 2016 EAST and ATEFI joined forces to further strengthen inter-regional cooperation in combating all types of payment crime including payment card fraud, hi-tech crime and ATM cyber and physical attacks and in October 2015 EAST participated in a two-day meeting in Bogota (Colombia) to discuss payment card fraud overseas

and money withdrawals in Latin America. This meeting, attended by AMERIPOL, was organised by Europol in cooperation with the Colombian authorities (Policia Nacional and its Liaison Bureau at Europol) with the financial support of the Romanian authorities.

This new public-private sector initiative in Latin America is welcomed by the industry in Europe as another step forward in global efforts to tackle

transnational payment fraud and financial crime. EAST has worked with Europol since 2004, a partnership that was strengthened in June 2015 by the signing of a Memorandum of Understanding (MoU), and in June 2017 EAST and ASEANAPOL formalised collaboration. ASEANAPOL is the National Police organisation for the Association of Southeast Asian Nations (ASEAN).

Economic Development Ministry, SBU to create a list of critical infrastructure

The CBRN 46 project to The Ministry of Economic Development and Trade jointly with the Security Service of Ukraine (SBU) have created an interdepartmental expert group on critical infrastructure protection.

“The Economic Development Ministry and SBU have established an interdepartmental expert group on critical

infrastructure protection, which will become a platform for creating a national list of critical infrastructure facilities, as well as defining bases for categorization and certification of these facilities. The expert group will also develop proposals for the first vice prime minister regarding new tools for protecting critical infrastructure facilities,” the press service of the

Economic Development Ministry reports.

The ministry noted that the expert group will coordinate the activities of state government bodies.

Deputy Economic Development Minister Yuriy Brovchenko has been appointed as chairman of the group. The expert group will also include other representatives of the Economic Development

Ministry, as well as the Security Service of Ukraine, State Fiscal Service, State Emergency Service, Infrastructure Ministry, Energy and Coal Ministry, Agrarian Policy Ministry, National Bank of Ukraine, Antimonopoly Committee of Ukraine, Foreign Ministry, Ministry for Temporary Occupied Territories, State Water Resources Agency and State Environmental Inspection.

Tough new rules to protect UK's critical infrastructure come into force

New measures to protect the nation's critical infrastructure and digital services from cyber attacks and computer network failure came into force.

Bosses of firms in health, water, energy, transport and digital infrastructure will now be expected to have robust safeguards in place against cyber threats and

report breaches and network outages to regulators within 72 hours or they face fines of up to £17 million.

The new law announced by Digital Minister Margot James will help reduce the number of damaging cyber attacks affecting the UK.

The National Cyber Security

Centre, set up by the government in October 2016 as part of GCHQ, has already responded to more than 950 significant incidents, including WannaCry.

It will also give new regulators powers to assess critical industries and make sure plans are in place to prevent attacks.

The regulator will have the power to issue legally-binding instructions to improve security, and – if necessary – impose significant fines.

The legislation will also cover other threats affecting IT such as hardware failures and environmental hazards.

Countering terrorist use of the Internet



INTERPOL

INTERPOL has conducted two advanced training courses for officers in Southeast Asia on countering the use of the Internet for terrorist purposes.

The training courses gathered law enforcement officers and investigators from 10 countries

across the region. Activities focused on boosting their abilities to:

- Identify and detect potential terrorism suspects online;
- Address challenges related to the admissibility of digital evidence in counter-terrorism cases;
- Develop a dialogue between the private sector and law enforcement to advance their investigations.

The first course was held under the auspices of INTERPOL's Project Trace, a

three-year capacity building programme funded by the Government of Canada. With a clear focus on detecting, preventing, investigating and ultimately prosecuting terrorism-related crimes, participants learned how to collect, analyse and share information found online.

The second session, entitled "Enhancing Member State Capacities to use Social Media to Prevent and Counter the Foreign Terrorist Fighters Phenomenon" was funded by the Government of

Japan and UNCCT. Through practical exercises, it sought to deepen understanding of the FTF phenomenon via the collection of social media information to support counter-terrorism investigations.

These training courses were a key deliverable of INTERPOL's global counter-terrorism strategy, which seeks to counter terrorist threats on digital platforms by reinforcing social media analysis capabilities of member countries in Southeast Asia.

Tackling future policing challenges with AI, robotics

The latest robots, virtual communication tools and facial recognition software were on display at the INTERPOL Global Complex for Innovation this week, as experts from different sectors gathered to consider practical applications of these new technologies for law enforcement.

Technological advances in the fields of artificial intelligence and robotics – from facial recognition to 'futurecasting' technology – can have many implications for police worldwide, both positive and negative. In the hands of criminals, these technologies can pose digital and physical threats, while at the same time these tools offer new opportunities to police in combating crime.

The first global meeting to examine the opportunities and risks of AI and robotics for law enforcement was organized

by INTERPOL's Innovation Centre and the United Nations Interregional Crime and Justice Research Institute (UNICRI), through its Centre for Artificial Intelligence and Robotics.

The two-day conference brought together some 50 participants from law enforcement in 13 countries and partners from the private sector and academia to exchange expertise on the latest developments in the fields of AI and robotics,

understand how they can be used by law enforcement to support their activities, and gain insight on potential challenges.

Discussions on ways that police could adopt these emerging solutions looked at the use of AI for conducting virtual autopsies; crime prediction systems to support police to optimize resources; behaviour detection tools; techniques to autonomously research, analyse and respond to international mutual

legal assistance requests; blockchain-based traceability approaches that respect privacy; and autonomous patrol vehicles.

The participants also considered ethical challenges such innovations could present to police, such as ensuring AI is fair, explainable and transparent and balancing the need for security with the right to privacy. They underlined the need to have further discussions on ethics and privacy, and a call was made for a follow-up meeting on this topic.

"Innovation is not a matter for police alone. Strong partnerships between all stakeholders with expertise is necessary to ensure police can quickly adapt to future challenges and formulate inventive solutions," said Anita Hazenberg, Director of INTERPOL's Innovation Centre.



Online Scammers Captured After Causing EUR 18m of Damage in More Than 35,000 Cases



After six years of preparation and coordination, the international Operation Warenagent has seen the arrest of 15 individuals, thought to be members of a network responsible for online fraud causing EUR 18 million worth of damage. The operation was conducted by the German Prosecutor's Office of Dresden, the Saxon State Office of Criminal Investigation, the Lithuanian Police and the Lithuanian Prosecutor's Office, with help from Europol and Eurojust at the international level.

During the investigation, the Department of Organised Crime together with the Cybercrime Competence Center Sachsen (SN4C) and the judicial assistance of

Lithuania met in The Hague to form a Joint Investigation Team (JIT) with the support of Europol and Eurojust. Overall five coordination meetings took place at Eurojust. The information gathered, alongside frequent information exchange and

analysis by Europol, led the investigators to identify and locate the key target in Cyprus.

From the 12 to 15 June 2018, 31 house searches were carried out in Cyprus, Estonia, Finland, Germany, Latvia, Lithuania, Switzerland, Ukraine and the United Kingdom. On the action days the head of a criminal organisation was detained in Cyprus, alongside four criminals in Latvia and Finland respectively, two in the United Kingdom, and one each in Estonia, Lithuania, Switzerland and Ukraine. Over the course of the investigation itself, four individuals were detained in Germany.



Two Criminal Groups Dismantled for Laundering EUR 2.5m Through Smurfing and Cryptocurrencies

Europol has supported the Spanish Guardia Civil and the National Police of Colombia in dismantling two criminal organisations involved in large-scale money laundering. It is estimated that the EUR 2.5 million have been laundered by using different methods, such as smurfing and cryptocurrency exchanges.

23 members of the group were arrested – mainly from Spain, Colombia and Venezuela -, and another 9 investigated. 12 house searches were carried out - 10 in Spain and 2 in Colombia-, and 2 vehicles seized, alongside mobile phones, computers and banking and financial documents. Also, numerous virtual wallets used by the criminal organisation to launder the cash were frozen by law enforcement authorities.

Europol supported the operation by facilitating information exchange and by deploying four experts to Spain equipped with a mobile office and a Universal Forensic Extraction Devices (UFED) . This allowed for real-time cross-checks of the data gathered during the course of the actions against Europol's databases, as well as the extraction of data from the mobile and computer devices The investigation began in January 2017 when

Colombian authorities warned about a Colombian family with links to drug trafficking that was operating in the Spanish city of Zaragoza. The Spanish Guardia Civil verified the existence of a criminal organisation operating in Spain and dedicated to laundering the money earned by other criminal groups who were operating in various locations in Spain and France. The criminal network picked up the illicit proceeds, split them and sent them in small

remittances – a criminal method known as smurfing.

Among the criminal groups they collected the money from, investigators also identified a second network operating in Madrid (Spain). This second network was also involved in collecting large sums of cash from other criminal groups linked to illicit activities such as drug trafficking or crimes against the heritage in Spain. The group used cryptocurrency exchanges to convert large amounts of money from cash into cryptocurrencies, like Bitcoins and Altcoins, and later transferred them to other virtual wallets controlled by the Colombian organisation, which allowed the return of the illicit proceeds to South America, thus hiding the origin of the money, seized for its posterior analysis.



Southeast Asia joins forces against CBRN threats

The CBRN 46 project to improve the response to NRBC risks in the region has ended. Now the objective is for the results to be maintained in the participating countries

The closing event of the CBRN 46 project has brought together around 70 experts and authorities from Brunei, Cambodia, Laos, Malaysia, Myanmar, Singapore, Thailand and Vietnam in the management of these risks. Through the



initiative of the European Union Centres of Excellence (CBRN CoE), the response capacity of the countries of Southeast Asia has been improved in the face

of nuclear, radiological, biological and chemical threats.

The final project meeting, funded by the European

Union and led by FIAPP, focused on regional cooperation to maintain the capacities and practices acquired during the project in the participating countries. At the inauguration, the director of the Department of Cooperation of the Laos Ministry of Science and Technology underlined the importance of international cooperation in the response and management of deliberate or accidental risks from NRBC materials.

Sepura TETRA radios enhance operations at Mexico City International Airport

Mexico City International Airport's (AICM) TETRA network is now fully operational following its initial roll out in the first quarter of 2018. Officially known as Benito Juárez International Airport - the international hub serves Mexico City and the surrounding areas. It is one of Latin America's busiest airports, with over 100,000 passengers passing through each day. Statistics from 2017 showed a 7.2% increase of passengers (45 million passengers in total) compared to 2016. More than 2,500 employees are based on site.

The airport previously had an analogue trunked system that suffered from operational limitations: outdated technology which could not be upgraded; poor audio quality; insufficient coverage, lack of data capability and limitations on voice call functionality. The system also had no interconnection gateways and insufficient security to protect the network from cyber threats. Due to rapid

increases in airport traffic, the airport operators needed to upgrade their communications system to one that matched international standards for robustness, reliability and security. The airport's decision to switch to TETRA would allow for enhanced existing operations and future growth in user numbers and functionality.

AICM's TETRA system includes three base station sites with interconnection to analogue gateways which allow the new TETRA network to connect to legacy radio technologies. This key functionality enables dispatchers to listen to all radio communications from one integrated communications system, improving efficiency and security across the site. The system is also interconnected to the airport's PABX telephone system allowing radio users to perform calls to fixed landlines or mobile phones from their TETRA radio, ensuring simplicity of communication and reducing

the expenditure on further communication devices. Crucially, the network has successfully achieved 99.9% coverage to meet one of the airport's key operational requirements.

The new network increased site security through air interface encryption and authentication, ensuring communications are secure. The airport also now has GPS monitoring of emergency and runway service vehicles, enabling dispatchers to locate users working on the external side of docking gates, where they were previously out of sight.

Spread across the two airport terminals, AICM's system will utilise over 500 Sepura SC20 hand-portable radios, alongside over 130 SRG3900 desk- and vehicle-mounted mobile radios. The SC20 terminals were chosen for their combination of ruggedness, ease of use and audio quality – especially important in the extremely noisy airport environment – and the SRG3900 mobile

devices complemented these by enabling DMO gateway functionality to extend coverage to lower user density areas which still required coverage. A further key advantage of the Sepura terminals was the ability to add future functionality.

Airport operators are already seeing the benefits of the spectrum efficiency inherent in a TETRA system. Despite a high density of users, TETRA systems offer greater talk group capacity, which facilitates better resource management. In addition, operational benefits have been delivered through significantly reduced call queue times. The new system also offers redundancy, ensuring communications are not compromised in the event of failure. Users themselves benefit from improved voice quality, enhanced security and added functionality, including Water Porting technology, whereby water is expelled from the microphone and speakers, ensuring consistently good audio quality.

Critical Infrastructure & Government GSOCs Drive IPSecurityCenter™ V5.7

CNL Software announced the release of IPSecurityCenter™ V5.7. The release includes many feature enhancements that increase performance and reduce operational response times in large-scale, multi-sited and mission critical deployments of IPSecurityCenter. These improvements also benefit those in the transportation, corporate security and public safety markets.

With over a decade of development IPSecurityCenter leads the Global Security Operations Center (GSOC) market for PSIM with its flexibility, features, performance and sophistication. This latest release improves CNL Software’s unique ability to manage across multiple SOCs & GSOCs, keeping in the entire operation in harmony using enterprise wide visualization to support the overall security mission for critical infrastructure and large-scale government homeland security programs.

“We continue to invest



heavily in developing the features that customers, partners and industry leaders inspire us to create” commented Simon Knightley, CTO at CNL Software. “We listen to our customers and understand what is important to them. Their ideas help us to innovate new ways to support them in making the GSOC a faster and more effective hub for all mission critical security and life safety related activity. They want their control rooms to see more, act faster and collaborate better throughout the whole organization, which we help them to achieve using IPSecurityCenter V5.7.”

The V5.7 release differentiates CNL Software from other PSIM vendors and establishes IPSecurityCenter as the first choice PSIM solution for large scale, Government security programs, critical infrastructure and facilities protection. Some of the main enhancements within the release include;

- More scalable for larger deployments - Enhancements support greater control over large scale federated solutions, driving tightly managed GSOC operations.
- Faster and more responsive

- Improvements include faster access to historic alarm data with fewer clicks and rapid access to video from remote locations.

• Support for 64-bit video - ensuring IPSecurityCenter leverages the latest developments in video-technology and multi-thread processing for faster and more scalable solutions.

• General Data Protection Regulation (GDPR) ready security platform - Enhancements ensure that IPSecurityCenter is ready for the most demanding compliance processes, with security features such two-factor authentication to ensure there are no unauthorized changes to the system.

• Improved decision support - Developments include new visually stunning interactive dashboards that allow operators to access key performance indicators in real time using customizable device that can highlight alarm, human, and machine data.

Northgate Public Services acquires i2N Ltd to expand its justice offering

NEC Corporation and Northgate Public Services (NPS) have announced that NPS acquired i2N, which supplies specialist software to the UK’s Ministry of Justice’s HM Prison and Probation Service and the Youth Justice Board. The deal will significantly increase NPS’ offering across the entire criminal justice process.

NPS is the market leader for policing IT solutions in the UK with 15 forces currently using NPS’ crime, custody and intelligence management system, CONNECT. Recent contract wins with West Midlands Police and the Metropolitan Police Service mean that over 50% of police officers in England will be using NPS technology.

The i2N acquisition presents an opportunity for greater visibility across the criminal justice system enabling users throughout the process to work collaboratively to deliver better outcomes and reduce reoffending.

Stephen Callaghan, chief executive officer of NPS, which is owned by the NEC Corporation, Japan, said,

“We see a good synergy between NPS and i2N in the area of local authority youth offender management.

NPS provides a range of product and services to 168 local authorities in the UK. This acquisition will boost our offer in the important justice sector whilst providing a strong opportunity for growth for i2N.”

Headwall is combining its hyperspectral imaging sensors with LiDAR.

They are combining the instruments aboard the DJI Matrice 600 Pro UAV but later this year we will have evolved the offering to actually fuse/synthesize the data streams from both instruments. For a range of remote sensing applications, the ability to collect full hyperspectral data PLUS LiDAR simultaneously is a big advantage since



flying is made much more efficient. The hyperspectral data provides a full spectrum for every spatial pixel in the field of view. That's 270 spectral bands x 640 spatial. The LiDAR provides terrain elevation, so, for example, plant health can be determined based on height and volume.

Cyber report details tricks used by hackers to target critical infrastructure

A cybersecurity firm says it uncovered the methods and tools hackers use to target critical infrastructure organizations, activity it observed by creating a website that masqueraded as a major electricity provider.

Cyberreason on Monday released a report on its "Honeypot Project," which is designed so that the firm's researchers could learn more about the tactics and techniques hackers employ while trying to compromise control systems.

The fake website, known as a honeypot in cyber-speak, was made to resemble a large, well-known electricity provider that served customers in both the United States and United Kingdom.

Cyberreason found that the hackers acted quickly.

"Just two days after the honeypot went live, attackers had discovered it, prepared the asset for sale on the dark Web and sold it to another



criminal entity who was also interested in [industrial control system] environments," according to the report.

The first set of hackers found ways around firewalls and other security measures by employing a tool called 'xrdp' to gain access to Remote Desktop Protocol (RDP) servers in environments.

The software helped the hackers get around certain administrator restrictions in Windows and quietly gain access to an environment using a compromised user's credentials. They

also created backdoors for the new owners to eventually use.

The criminals appear to have bought xrdp from one of the largest underground criminal marketplaces known as xDedic, a digital black market.

By the time the new owners began to become active, they appeared only interested in gaining control of the operational technology (OT) environment, which operated utility providers' hardware systems like pumps, monitors, and

breakers, according to the report.

"Whoever controls the OT environment determines who gets utilities like electricity, natural gas and water," Cyberreason found.

But Cyberreason said these "specialized" hackers did not appear to be part of the "upper echelon of attackers," because they made some mistakes along the way.

"Despite the attackers' sophisticated techniques, they made some amateur moves that indicate their approach needs some refinement," Ross Rustici, Cyberreason's senior director of intelligence, said in a statement.

The ongoing project, which went live on July 17, had been underway for a week when the Department of Homeland Security announced that Russians have targeted the control systems of hundreds of electricity providers.

Leonardo DR mini II

Now even lighter and more comfortable – the new Leonardo DR mini II In May 2018, OR Technology presents the second generation of the portable X-ray case Leonardo DR mini. The Leonardo DR mini II surpasses its predecessor in its equipment at lower weight. At only 8.9 kg, the Leonardo DR mini II is one of the world's lightest portable X-ray case systems. The high-quality plastic processing and the well planned space concept form the basis for a practical case for any outdoor use. If necessary, the case shell can be easily cleaned with water. The



mobile compact package fits behind every car seat. The practical suitcase solution is quickly ready to go and easy to use. All components are integrated in the X-ray case.

The 17" laptop can easily be removed from its holder in the case and used as a tablet for presentation purposes. The notebook is equipped with the dicomPACS@DX-R

acquisition and diagnostic software. The wireless CsI X-ray detector is transported space-saving in the case inside and guarantees best image quality even at low X-ray doses. Everything is stored perfectly. The Leonardo DR mini II supports its users in outpatient digital radiology in the areas of human medicine such as home care, disaster control, emergency medicine on ships, yachts and oil platforms as well as in medical services. In veterinary medicine, the suitcase solution can be used in a veterinary practice, equine clinic or university facilities.

Indra Develops System to Give Direct Earth Observation Satellite Access to Organisations

Under a contract with the European Space Agency (ESA), Indra is developing an innovative terminal designed to enable governments, organizations and companies to directly and autonomously retrieve data from earth observation satellites and get extremely high-resolution images virtually in real time.

They will only need two main elements: an antenna to download the telemetry sent by satellites and this innovative Direct Access Terminal (DAT), which will process the data received to generate images with maximum celerity. After signing agreements with satellite operators, users will be allowed to independently connect to satellites, thus rendering the entire process of retrieving information of interest more agile and a matter of minutes from the

data acquisition.

It was conceived so that any organization or company seeking to monitor a situation in any part of the world can do so whenever it wants. The enormously valuable images can have resolution sizes that are in many cases smaller than one meter per pixel: this is the case of ESA's several radar satellites (SAR) that reach up to 0,25 meters per pixel. Radars allow to collect images at night and regardless of cloud cover or weather conditions that might otherwise reduce visibility.

The degree of detail of those images suffices to identify a vessel at sea or vehicle anywhere on the planet. They can help detect and monitor spreading wildfires. They can delimit zones affected by flooding or buildings that have been damaged

following an earthquake.

Among the seemingly endless possibilities, they are the most effective and quickest way to examine the conditions of crops across a country and estimate cereal harvest yields for the year, or containers stored in customs-free zones at ports.

Indra's system reduces the elements necessary to access this powerful observation capability to the absolute minimum. This capability had thus far only been within the reach of satellite operators equipped with expensive and sophisticated infrastructures that include control stations deployed around the globe and huge data processing centers. Indra's terminal nevertheless lets end users get access to only the functional features they really need.

Indra's terminal has been initially conceived to receive data from Spain's PAZ radar satellite and the twin systems, TerraSAR-X and TanDEM-X, which will soon begin operating jointly as a single constellation capable of observing any point on the Earth.

Indra has designed the system to be easily adaptable for receiving and processing data from other satellites. This renders Indra's system as one of the most advanced and versatile solutions on the market. In less than 15 minutes from the data acquisition, users can get the image of the constellation that they need. The system's daily surveillance capability will cover an area of approximately 300,000 km², which is equivalent to 60% of the size of Spain.

EVERY installs Boon Edam security Speed Gates



As one of the largest IT companies in Scandinavia, EVERY provides comprehensive computing, IT consulting, and business solutions to Nordic companies, financial institutions, public sector entities, and health authorities. While security at EVERY facilities is paramount, so is maintaining a leadership brand and accommodating a high flow of staff and visitors.

Entrances of EVERY facilities must provide a high level of

security given the value and sensitivity of the work they do, as well as the presence of clients' intellectual property and other data. Management was looking for entry designs that would not only provide a secure entry way, but would also display excellence in design, innovation and quality – elevating and supporting the overall perception of the firm for both staff and visitors.

The EVERY security team quickly zeroed in on Boon

Edam as a premium entrance provider. When they heard that many Boon Edam entrances could be customized to meet aesthetic objectives or to match desired colors and finishes, they were compelled to come and see the samples in person.

Bravida, the system integrator who installed the Lifeline Speedlane Swing speed gates integrated them with cutting edge access control technology that communicated with

security personnel. The combination of this physical and technological access control delivered a highly effective solution that met EVERY's needs for both staff and visitor access control.

"The reception area of an IT company like EVERY was an ideal application for the Lifeline Swing speed gates," explains Daan Van Beusekom, Product Manager Security Access, Royal Boon Edam. "The sleek, high-tech design of the turnstiles support EVERY's brand positioning, and they provide a high-throughput, secure solution that meet EVERY's demanding access requirements. The turnstiles also integrate with leading access control systems, making it easy to tie them in with EVERY's existing security strategies and systems."

MARSS completes installation of NiDAR perimeter security system onboard superyacht

MARSS has successfully completed the retrofit of its NiDAR perimeter security system onboard a large yacht undergoing a winter refit.

The system integrates the vessels radars and upgraded cameras using smart software to provide long range awareness of objects operating in the vicinity of the vessel.

NiDAR provides automated monitoring, detection, tracking, classification and alerts with information, live tracks and real time video



feeds presented on an intuitive user interface.

The Captain of the vessel said: "From my first introduction to MARSS I have been impressed. Having started off on the back foot looking

to replace a useless piece of security equipment, I wanted to see a lot of data, testing, comparisons and real world live demonstrations of any proposed equipment. MARSS complied with all requests professionally and came out

shining. I am very happy with NiDAR. It does what is says on the tin with minimal fuss and is intuitive to operate. Training new users is easy, no matter if they are trained Security Guards, Officers or Junior Crew. The system is easily integrated into the Bridge Operations and adds a layer of security and awareness rather than distracts from the necessary good practices for watch-keeping and lookout. I am most happy to recommend MARSS as a company and NiDAR as a surveillance package."

Bruker have launched the first commercial 24 hour advisory support network for managing CBRNe incidents



CBRNet™ provides a network that links CBRNe sensors and their operators with decision makers.

It provides 24 hour advisory support to clients in the form of advisers in the specialist areas of scientific, technical and operational expertise.

CBRNet™ is the industry's first fully integrated and networked end-to-end solution addressing the challenge managing CBRNe incidents. Specialist advisers, based in Bruker centers of excellence, will be available at all times to provide support in the management of CBRNe operations.

Bruker scientists have teamed with leading experts from around the world to develop CBRNet™ capability.

- The software house Bruhn Newtech has adapted its specialist software, widely used amongst NATO nations, to provide the information technology to support the Central Monitoring, Advice and Global Incident Capability

(CMAGIC) .

- Cubic Mission Solutions provides the networking and communications technology that allows clients to choose between their own preferred communications bearers and CBRNet™ recommended solutions.

CBRNet™ will allow users to connect all of the most commonly used CBRNe sensors already available from manufacturers on the market. Detection Data will be provided to decision makers in the form of a "Recognised CBRNe Picture" providing the capacity to view via a map interface the location and performance of individual detection equipment.

CBRNet™ will offer Bruker customers 7 new products and services that, together, can be tailored to meet the specific needs of each user.

- SafeZone, the CMAGIC™ Information System. SafeZone provides advanced software capabilities to support all the other components of

CBRNet™. It links decision makers with the sensors and specialist CBRNet advisers.

- Advice 24/7/365. Specialist advisers are available at all times in CBRNet™ Operations Facilities. Securely connected to user Decision Makers, these advisers support all areas, from training and fleet management, to the provision of scientific, technical and operational support.

- Planning. CBRNet™ specialists are available to support users developing plans to meet specific operational challenges, whether it be designing the protection of a new railway network, protecting a major sports festival or hosting an international gathering.

- Training. CBRNet™ is designed to support training at both the individual and collective levels.

- Fleet Management. The CBRNet™ Fleet Management package offers solutions to problems of logistic supply, preventative maintenance,

repair and asset tracking.

- CBRNet™ Deploy. CBRNet™ Deploy is Bruker's unique solution to the challenge of hosting short term events that require temporary CBRNe solutions, for example, major international sports events or international conferences, each of which require a surge in capability for a limited period of time. With CBRNet™ Deploy, users can call on a selection of CBRNet™ products and services to support a short duration operation. Sensors, people, planning, training, and of course, SafeZone, are all available to meet the challenge.

Sebastian Meyer-Plath, Managing Director of Bruker Detection, announced the launch of CBRNet™ saying:

"CBRNet™ represents a huge leap forward in our ability to help our customers meet the growing challenge of CBRNe threats. Whether as a military challenge, as a part of the terrorist threat, or as a consequence of industrial accident or natural disaster, recent history shows numerous examples of the challenge presented by chemical, biological and radiological threats. Bruker's CBRNet™ brings the best possible data and services to aid decision making at the right time. We are proud to be at the forefront of solutions to this real challenge."

(ISC)² extends global computer-based testing certification agreement with Pearson VUE

(ISC)², the world's largest non-profit membership association for certified cybersecurity professionals, has extended its multi-year agreement with Pearson VUE, the global leader in computer-based testing.

As part of the continued partnership, Pearson VUE's team of measurement scientists will work with (ISC)² subject matter experts to develop valid, fair and reliable exam content in the ever-changing field of information security.

The exams – including the acclaimed Certified Information Systems Security Professional (CISSP) certification, newly modified to a Computerized Adaptive Testing format – are being delivered via Pearson VUE's network of highly secure test centers in 180 countries around the world. Candidates benefit from the convenience of on-demand testing and the ability to schedule their exam at a local test center at a time and date of their choice.

"The extension of our partnership with (ISC)² is great news for both Pearson VUE and security specialists around the world," said Bob Whelan, president of Pearson Assessments. "Access to this exam will continue to enrich lives and careers, as we continue to provide increasingly sophisticated computer-based assessment solutions in the dynamic field of information security."

"As demand for cybersecurity certification continues to grow, Pearson

VUE offers excellent value and quality for (ISC)² exam candidates around the world with its unmatched breadth in test delivery reach," said Dr. Casey Marks, vice president of professional programs at (ISC)². "By extending our relationship, we will continue to offer a consistent testing environment and the convenience of local test centers to security professionals pursuing our certifications worldwide."

Other variants boost espionage capability, says threat assessment expert Jeremy Samide

Trojan malware is among today's most frequently deployed cyber threats. Calisto has just reemerged as a Mac backdoor, while Quasar and Sobaken impact Windows users and are being used primarily for government and corporate espionage.

Additionally, Vermin, an open-source, Remote Access Trojan or RAT has been targeting victims in Ukraine, while DanaBot—a new banking Trojan—targets users in Australia.

"These new RATs support 24 implemented and several optional commands, including audio recording, keylogging and password theft. Attackers use Virtual Network Computing or VNC to create and control

remote hosts, steal private and sensitive information and communicate the data covertly via Tor," observes Jeremy Samide, CEO of Stealthcare, an international cybersecurity and threat assessment firm with offices in Cleveland, Los Angeles and Toronto.

Calisto infects Mac

As with most Trojan variants, Vermin and DanaBot target Windows users exclusively, however Mac users are now at risk from Calisto, the Mac backdoor that reemerged last week after lying dormant since 2016. "The operator's motives are unclear as this backdoor provides total access to the infected machine, offering myriad possible courses of action.

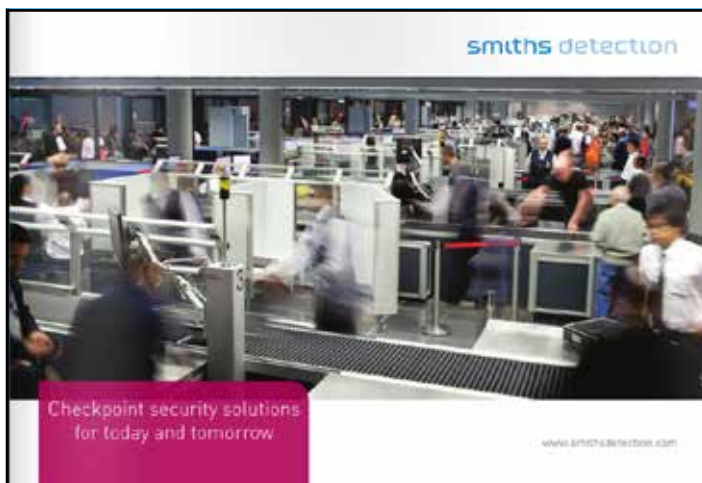
Calisto also contains several unfinished functionalities suggesting it is still in active development," according to the latest weekly Stealthcare Alert that warns clients of emerging threats. "Calisto's functions include loading and unloading the kernel extensions for handling USB drives, data theft from user directories, and self-destruction together with the destruction of the Operating System."

With cyberattacks becoming more pervasive and sophisticated, Stealthcare has changed cybersecurity from defense to an aggressive stance that relies on early warning and threat assessment, as well as artificial and human intelligence. Stealthcare's

proprietary platform Zero Day Live, warns clients of emerging threats and provides countermeasures.

Samide adds, "Playing defense is not enough. When we developed Zero Day Live, it became the first complete cyber threat intelligence aggregation platform to spot emerging trends, uncover actionable information, and report on high-value intelligence. The platform enables our clients to respond quickly to impending cyberattacks." Stealthcare researchers and technical staff also provide ongoing assistance that includes human threat assessment and, if need be, disaster recovery as well as tactics to ward off future attacks.

smiths detection



Checkpoint security solutions for today and tomorrow

www.smithsdetection.com

World Security Report



World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 150,000 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.



HIDDEN TECHNOLOGY
systems international ltd.

Discrete tracking devices for personal protection and vehicle security.

Fast, accurate locations using 3G, GPRS, SMS and RF.

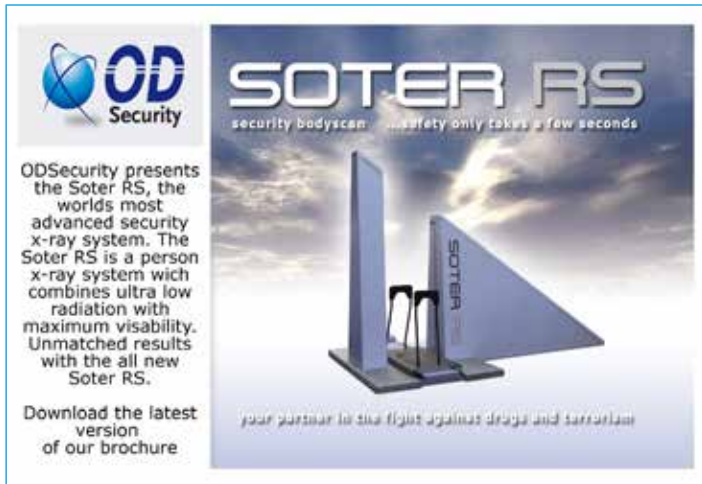
In use by Police, Military and Government organizations worldwide.

www.hiddentec.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

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

Download the latest version of our brochure

your partner in the fight against drugs and terrorism



2003-2013
WAGTAIL
UK LIMITED
SPECIALIST DOG SERVICES
10 YEARS

Wagtail International
leading specialists in detection dogs and dog handler training

Click here to view our profile



DEFENCELL

PROFILE 300 & DC BARRIERS
HOSTILE VEHICLE MITIGATION

www.defencell.com

International Procurement Services (IPS)



Electronic Countermeasures
Equipment Sweep Teams
Training

www.SECURITYSEARCH.Co.Uk

August 2018

16-18

Secutech Vietnam
Ho Chi Minh City, Vietnam
www.secutechvietnam.com

27-31

Asia Risk & Resilience Conference
Singapore
www.arrconference.com

September 2018

4-5

SmartSec Cyber Security & Blockchain Conference
Manama, Bahrain
smartsecme.com

4-5

Indonesia Security Summit
Jakarta, Indonesia
www.indonesiasecuritysummit.com

14-16

Blockchain & Future Tech Expo
Dallas, Texas, USA
www.bftexpo.com

23-24

Arab Security Conference
Cairo, Egypt
www.arabsecurityconference.com

24-26

International Conference on Critical Information
Infrastructures Security (CRITIS)
Kaunas, Lithuania
www.lei.lt/critis2018

25-28

Security Essen
Essen, Germany
www.security-essen.de



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

October 2018

2-4

Critical Infrastructure Protection & Resilience Europe
The Hague, Netherlands
www.cipre-expo.com

15-18

International Conference on the Internet of Things
Santa Barbara, California, USA
iot-conference.org

December 2018

4-6

Critical Infrastructure Protection & Resilience North
America
Tampa, Florida, USA
www.ciprna-expo.com

ADVERTISING SALES

Sam Baird
(UK, Germany, Austria, Switzerland, Israel & ROW)
E: sam@whitehillmedia.com
T: +44 7770 237 646

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

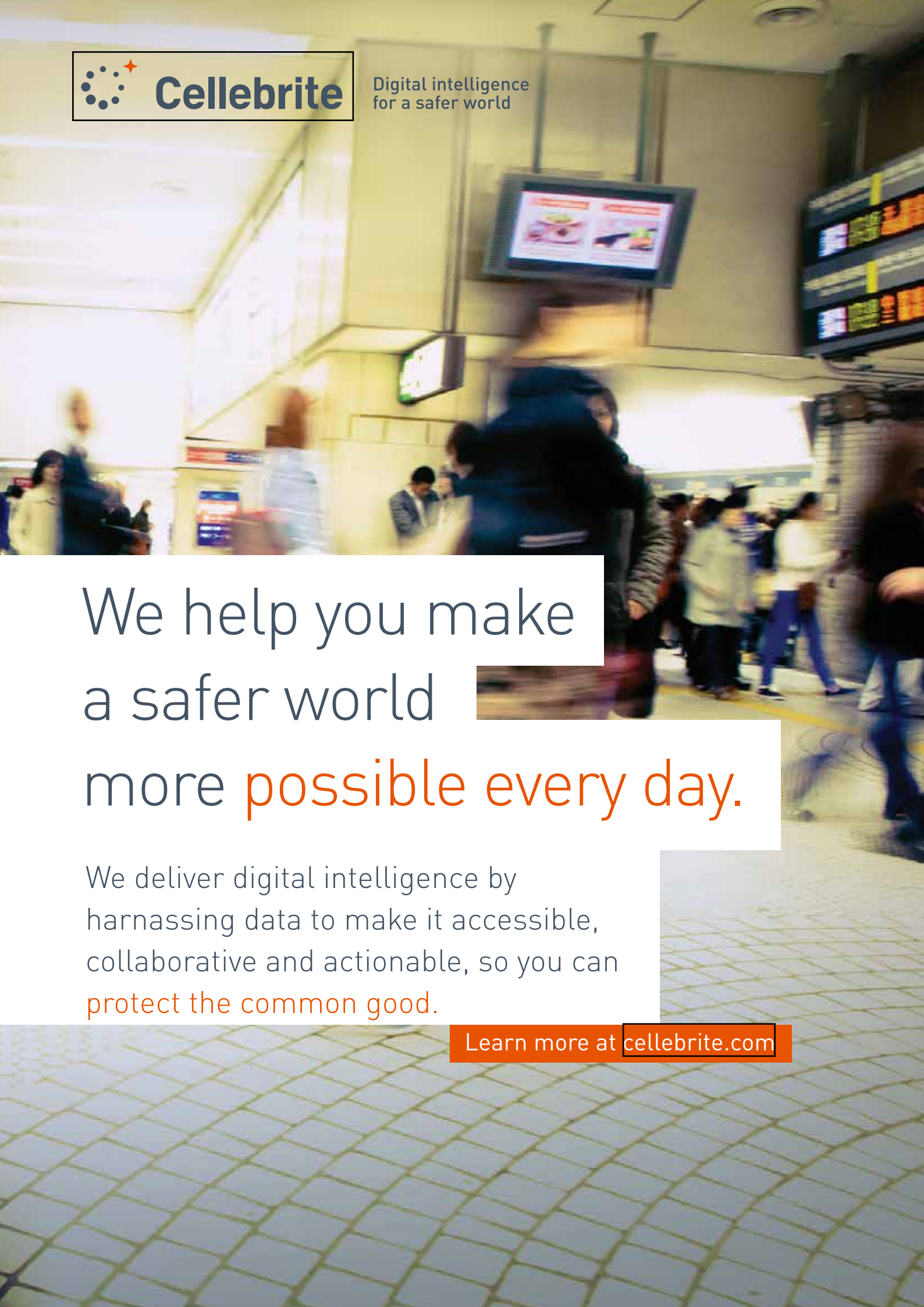
Paul McPherson
(Americas)
E: baulm@torchmarketing.co.uk
T: +1-240-463-1700

Annabel McQueen
(Benelux)
E: annabel.mcqueen.am@gmail.com
T: +44 20 8249 6152



Cellebrite

Digital intelligence
for a safer world

A blurred background image of an airport terminal with people walking and digital screens.

We help you make
a safer world
more possible every day.

We deliver digital intelligence by
harnessing data to make it accessible,
collaborative and actionable, so you can
protect the common good.

Learn more at [cellebrite.com](https://www.cellebrite.com)

BORDER SECURITY REPORT

VOLUME 11
JULY / AUGUST 2018

FOR THE WORLD'S BORDER PROTECTION, MANAGEMENT AND SECURITY INDUSTRY
POLICY-MAKERS AND PRACTITIONERS

COVER STORY

RETURNING JIHADISTS AND EUROPE'S FRONTIERS



SPECIAL REPORT



Technology and Border Security in Europe p.23

AGENCY NEWS



A global review of the latest news and challenges from border agencies and agencies at the border. p.18

SHORT REPORT



Ghana Immigration Service Unveils Strategic Action Plans p.4

INDUSTRY NEWS



Latest news, views and innovations from the industry. p.28

CONTACTS

Editorial:

Tony Kingham

E: tony.kingham@knmmedia.com**Contributing Editorial:**

Neil Walker

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

Neil Walker

E: neilw@torchmarketing.co.uk**Subscriptions:**

Tony Kingham

E: tony.kingham@knmmedia.com

Border Security Report is a bi-monthly electronic magazine and is the 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.



Copyright of KNM Media and Torch Marketing.

Drones, borders and drugs

US Homeland Security Secretary, Kirstjen Nielsen recently took a trip to the U.S.-Canada border to learn about the threat drones pose to border security, especially how drones are used to smuggle drugs across the border.

It's not surprising that the threat is being taken seriously at the highest level because drones are a real game changer in the world of cross border smuggling and drug trafficking in particular.

A quick search on google and you can find a long-range cargo drone for less than \$3,000, that is capable of carrying two kilograms of drugs up to 20 miles. With a street price of heroin at approximately \$100,000 per kilo, it makes the drone a disposable item.

So just taking the capabilities of that one drone, it means that you would have to extend the control or patrol zone around the border, up to 20 miles on either side. That means for the US Canada border 5,525 miles, a control zone of 110,500 square miles. And of course, that's just for that one drone, there are plenty of others out there with ever increasing capability.

To police a control zone that big simply isn't possible which makes the only feasible option some sort of technical solution to stop drones as they attempt to cross the border.

The last few years have seen a proliferation of anti-drone systems using a variety of technologies but to date they are mostly for localised deployments, not extended borders. This issue needs a solution and quick!

Tony Kingham
Editor

READ THE FULL VERSION

The digital version of Border Security Report contains all the additional articles and news listed in the contents page below. The full digital version is available for download at

www.world-border-congress.com/BSR

CONTENTS

BORDER SECURITY REPORT



5 RETURNING JIHADISTS AND EUROPE'S FRONTIERS

Tony Kingham looks at the challenges and problems of foreign fighters returning from the Middle East to Europe.

8 AGENCY REPORTS

Latest news and reports reports from key agencies INTERPOL, OSCE, EUROPOL and the IOM.

12 GLOBAL REVIEW OF MIGRANT SMUGGLING DATA AND RESEARCH

IOM launched of its newest publication Migrant Smuggling Data and Research.



18 AGENCY NEWS

A global review of the latest news, views, stories, challenges and issues from border agencies and agencies at the border.



23 TECHNOLOGY AND BORDER SECURITY IN EUROPE

Cellebrite look at how and why technology will continue to be at the center of all discussion related to border security.

25 WORLD BORDER SECURITY CONGRESS

A look at the annual international border security gathering being hosted in Casablanca, Morocco on 19th-21st March 2019.



27 INDUSTRY NEWS

Latest news, views and innovations from the industry.

Ghana Immigration Service Unveils Strategic Action Plans

The Ghana Immigration Service (GIS) has launched a five-year Strategic Plan (2018- 2022) to position the Service to deliver effectively on its mandate in migration management in the country.

The development of the Plan had financial assistance from the EU and ECOWAS and facilitated by International Centre for Migration Policy Development (ICMPD).

The Plan operates around six thematic areas including; human resource development; strengthening laws and policies for effective migration management; enhancing both internal and external stakeholder engagements.

Other areas are making ICT services compliant in all its work processes by developing ICT Infrastructure and acquiring information security management certifications (ISO 9001 & ISO 27001); providing state-of-the-art equipment and infrastructure, including staff accommodation, training centres and new Headquarters to enhance the services of the GIS.

Mr Kwame Asuah Takyi, Comptroller-General of GIS, said the plan identified key challenges from the implementation of the previous plan (2011-2015), conducted a SWOT analysis of the Service, factors in emerging issues and the changing dynamics within the GIS work environment.

'It also proposes interventions that will position the GIS to deliver effectively on its mandate in migration management,' he said, adding that the plan is aligned to the National Migration Policy for Ghana and the Medium-Term National Development Policy Framework (MTNDPF) - An Agenda for Jobs; creating prosperity and equal opportunity for all (2018-2021).

The Strategic Plan, he said, was estimated to cost the Service 473.5 million of which equipment and infrastructure accounted for about 83 per cent of the total cost.

Mr Takyi said the success of the Plan would depend largely on the timely availability of funds to implement it and called on all stakeholders to come on board to ensure its successful implementation.

He expressed his gratitude to the partners for their support and the planning committee, GIS Council and

Management for their dedication.

In a speech read on his behalf by Mr Henry Quartey, Deputy Minister of the Interior, Mr Ambrose Dery, Minister of the Interior said: 'Historically, Ghana has played host to many non-nationals mainly from other African countries to facilitate their development efforts during the early post-colonial era.'

He said: 'The trend continued as Ghana, in addition to the promotion of pan-Africanism, enjoyed relative economic prosperity soon after independence. Over the years, immigrants into this country, particularly those from the West African sub-region, easily merge with the nationals and join the internal mobility of workers.

'The nation cannot therefore sit aloof with no proactive measures instituted to ensure orderly and safe migration that will be of benefit to the country of origin and the country of destination,' he added.

Mr Dery said the GIS, as the first line of defence to the country, had over the period not relented on its efforts in ensuring safe and orderly migration for national development though with inadequate resources.

'I know and certainly appreciate the personal sacrifices that you and your families have made to protect Ghana's frontiers and for that we remain extremely grateful. We will therefore ensure as a government that the Service gets its fair share of the national cake in terms of resources to make you more effective and efficient as the guardians of the Nation's borders.

'I can attest to the fact that this is a Plan of wide stakeholder consultation with meaningful inputs from all stakeholders, thereby ensuring the buy-in of all for effective coordination and implementation of all the activities outlined in the Plan. I know there is no limit to what an organisation can achieve, where there is unity of purpose,' he added.

He said a Strategic Plan presented a change and modernisation agenda for an organisation in all its functional areas and that called for attitudinal and cultural change and a persistent focus on delivering priorities from the rank and file of the Service to ensure success in the implementation of the Plan.

RETURNING JIHADISTS AND EUROPE'S FRONTIERS

Tony Kingham looks at the challenges and problems of foreign fighters returning from the Middle East to Europe.

Manuel Navarrete, head of Europol's Counter Terrorism Centre, estimates that of the 5,000 Europeans (mostly from Britain, France, Germany and Belgium) who joined the Islamic State, 1,500 have now returned to their home nations.

Hundreds of these returning jihadists from the so-called 'Caliphate' are

believed to already be behind bars across Europe.

But behind bars or not these individuals still pose a huge security threat.

Of course, it is better to have them behind bars but that does not solve the problem. Prisons that are short of space and resources are notorious as



radicalisation hubs for new recruits and training grounds for would-be terrorists.

Look at the recent case of Benjamin Herman a white, middle class, Catholic teenager who became an avowed Moslem and jihadist whilst mixing with jihadist whilst in prison for petty crime. In Liege, only a few months after leaving prison went on to kill three people and wounded more whilst shouting "Allah Akbar".

But, at least in prison we know where they are, and have the opportunity to address the problem directly, whether that's through de-radicalisation or permanent incarceration.

However, if Mr Navarrete calculations are correct, that leaves around 3,500 European jihadists unaccounted for.

Now hopefully, many these will have fulfilled their wish to die fighting for the Caliphate, but we can't be sure how many.

Some are, as we know in jail in Kurdish controlled Syria and Iraq and elsewhere in the region and thankfully their chances of release are slim. Some may have travelled to places like Malaysia or the Philippines and some are said to be laying low in places like Turkey.

But whichever way you look at it, there are likely to be hundreds of former fighters unaccounted for looking to make their way back home to Europe, whether that is to try to resume some sort of normal life or to carry on the fight. Even the ones that have headed elsewhere pose a potential threat for years to come, not just for their host

country but for Europe as well.

Then of course you have to add to this calculation those fighters who are not Europe citizens that are and will try to infiltrate Europe posing as refugees with the express aim of carrying out terrorist atrocities.

So, what can be done to stop them. Well toughening up the borders is really the only answer and despite a reluctance at the European Commission level to impose stricter controls for political and ideological reasons, circumstances have overtaken the EU with individual member states putting up fences and imposing stricter border control unilaterally.

Now the EC is really in a game of catch up. Which means instead of leaving those European states that are neighbouring failing states, to deal with the problem themselves, but instead starting to take on the responsibility of Europe's external borders centrally and provide the funds, personnel and equipment necessary to do the job properly.

To be fair that has already started with Frontex staff being deployed in Southern Europe and Mediterranean and the purchase of additional assets such as patrol boats, aircraft and even drones that are likely to be purchased.

But in every crisis, there is an opportunity.

There has been an historic reluctance for some member states to sanction any sort of European agency or force that could be conceived as federal.

Well, with the imminent departure of the United Kingdom from the EU, the biggest stumbling block to that has been removed.

It has long been the ambition of the EU to develop a European Army or defence force. But for lots of good reasons, not just the British but other European nations, with their own unique histories and international perspectives have been reluctant to hand defence of the state to an outside body. After all, is not the defence of the state every governments first duty.

But, I would say that in the case of the EU's external borders, the argument for a fully functioning European border agency with all the necessary structure, legal powers, personnel and equipment to take on the job is not only desirable, but necessary.

The logic is simple. With free movement of people within the EU being one of the principle rights and freedoms, it is in every member States interest for the external borders of the EU to be properly managed and policed.

It is also therefore logical that all member States contribute financially and materially to that border management.

This became evident at the beginning of the migrant crisis in 2015 when countries like Italy and Greece in particular, faced a huge wave of migration at a time when they themselves were still in the middle of their own financial crisis.

The rest of Europe and Britain in most vocally, maintained that responsibility for borders was a national issue and that “under the Dublin regulation”, refugees should seek asylum in the country that was their first point of entry into the EU. So, despite appeals for help from the Southern European States, very little help was forthcoming.

As the crisis escalated, the authorities in Balkan States

too were overwhelmed and as a result millions of refugees (and terrorists) made their way into and across Europe.

The handling of this crisis was Europe’s biggest failure since its formation. The consequences of which Europeans will live with us for generations.

To be fair, at the time the only organisations capable of handling the crisis were the national armed forces of individual member States, over which the EU had no jurisdiction.

Therein is the problem and the solution. The EU should grasp this issue and instead of playing catch up, take the lead in this issue.

Europe needs Frontex to be effective and Frontex needs it to have the tools and systems to do the job of protecting the EU’s external borders. It’s too late to stop hundreds jihadis that are already here and the many that are probably already on their way.

But it is not too late to start preparing for the next crisis, whatever and whenever that is!

Frontex strengthens surveillance in Croatia



Frontex surveillance airplane has started monitoring the EU’s external borders in the Western Balkans area as part of Frontex Multipurpose Aerial Surveillance (MAS). This is a swift and tailored response to the request made by Croatian authorities to monitor the migration flows and help Croatia, as well as the neighbouring Western Balkan countries, address the challenges on the ground.

MAS uses surveillance planes that stream video and other data directly to the Frontex Situation Centre (FSC) at the agency’s headquarters in Warsaw where a team

of experts analyses the data to provide quick feedback to relevant national authorities. It is an example of a new service that Frontex can offer with its autonomous technical equipment. Experts from Croatian authorities are present on board of the airplane, ensuring compliance with national procedures.

The airplane will perform up to 100 hours of aerial surveillance per month.

Overall, the number of illegal border-crossings on the Western Balkan route in the first half of 2018 amounted to 2100, which is about 60% lower than last year.

However, Frontex data indicates continued pressure along the Greece-Albania-Montenegro-Bosnia and Herzegovina-Croatia sub-route, which is indicative of migrants trying to bypass existing security measures along the main route via Serbia. The agency already supports Croatia with 10 officers who assist the national authorities with detecting document fraud and stolen vehicles.

7 Arrested in Spain for Smuggling Migrants to France



With the support of Europol's European Migrant Smuggling Centre (EMSC), the Spanish National Police has dismantled an organised crime group suspected of facilitating large-scale migrant smuggling between French-speaking African countries and France. It is estimated that this criminal network has facilitated the entry into Spain of almost 300 irregular migrants, before arranging for their subsequent smuggling to France.

During an action day end of July, six suspects were

arrested in Guipuzcoa (Northern Spain) and one in Madrid. Eight migrants awaiting to be smuggled to France were also rescued from a safe house in Guipuzcoa. Europol supported the investigation with analytical capabilities in-house and the deployment of an expert to San Sebastian (Spain) with a mobile office and UFED (Universal Forensic Extraction Device).

The organised crime group, made up of individuals of Sub-Saharan origin, arranged for migrants to be smuggled from French-speaking African countries (Guinea, Cote d'Ivoire, Mali and Senegal) to Spain by boat, usually providing them with fake documents. Upon their arrival at the Spanish coast, the migrants were contacted by members of the criminal organisation who would arrange for their transfer to safe houses in Northern Spain, and from there on to France.

Criminal Network Smuggling Cigarettes and Alcohol Thwarted in Poland



The Gdańsk Bureau of the Polish Central Bureau of Investigation (Centralne Biuro Śledcze, CBŚP), together with

the Regional Prosecutor's Office in Gdańsk and with the support of Europol arrested five suspects and seized over 39 million cigarettes.

Police officers from the CBŚP conducted since 2015 an investigation supervised by the Regional Prosecutor's Office in Gdańsk. The case concerns an international criminal group dealing with the illegal trade in cigarettes. The arrestees were charged for being members of an organised criminal group by the Regional Prosecutor's Office in Gdańsk.

Drug Dealer Gang Modified Vehicles to Smuggle Narcotics Across Europe

During the summer of 2017, the suspects trafficked to Wuppertal significant amounts of cocaine and amphetamine from several locations in the Netherlands (Rotterdam and Venlo, among others). Once in Germany, they stored the substances in apartments waiting to deliver it to other European countries, such as Denmark, Sweden, Switzerland, Austria, and Italy, hidden into professionally modified compartments of rental cars.

This operation resulted in the arrest of two individuals in Denmark last May and identification of two additional suspects, alongside two in Sweden in the beginning of June and has culminated with the execution of six arrest warrants. More recently, three individuals were arrested

in Wuppertal on 21 June on the occasion of which of a large contingent of 200 police officers from the German and Dutch authorities carried out 18 house searches. Six high-value cars, a motorcycle, EUR 110 000 in cash and two watches worth EUR 500 000 each were seized.

A marijuana plantation, with hundreds of plants, was also dismantled, and three shipments of drugs, containing 50 kg, 41 kg and 14 kg of amphetamine respectively, heading to Denmark and Sweden were confiscated.



INTERPOL border security training supports female ASEAN officers



In response to the growing security threats posed by transnational crimes such as human trafficking and migrant smuggling in Southeast Asia, INTERPOL conducted a

training course to enhance border security in the region.

The 10-day integrated border management course brought together 20 female police and immigration officers from nine Association of Southeast Asian Nations (ASEAN) countries to review best border management practices, including counterfeit document analysis, identifying human trafficking victims and the use of INTERPOL's policing capabilities.

With more and more people travelling across international borders every day, police and immigration officers face the growing challenge of identifying criminals attempting to conceal themselves among legitimate cross-border travellers.

Enhancing the fight against the illicit traffic of cultural property



In cooperation with the Italian Carabinieri's Headquarters for the Protection of Cultural Heritage, INTERPOL has launched an enhanced version of its Stolen Works of Art database, called P.SY.C.HE. (Protection System for Cultural Heritage).

By radically transforming the process of recording information, the new version of the database allows for

faster dissemination of information on stolen works of art worldwide.

Specialized officers will now be able to directly insert, modify and delete data related to cases in their respective countries. Previously, this was carried out by INTERPOL officials at its General Secretariat headquarters, based on information sent by member countries. This simplified process will invariably lead to a richer pool of information in INTERPOL's database, which will assist specialists and investigators worldwide.

Both INTERPOL National Central Bureaus and officers from the INTERPOL Works of Art Unit will continue to ensure that photos and descriptions of stolen items meet INTERPOL's quality control standards.

P.SY.C.HE now allows users to enhance their key word searches with image comparison features by simply uploading a photo of the work of art.

INTERPOL-led Mediterranean operation closes ranks on foreign terrorist fighters

INTERPOL has deployed officers to eight Mediterranean seaports to assist local authorities screen travelers and detect potential terrorists during the summer tourist season.

Codenamed Operation Neptune, the counter-terrorism sea border operation addresses the threats posed by the travel of foreign terrorist fighters using Mediterranean

maritime routes between North Africa and Southern Europe, as well as by people, drugs, or firearms traffickers.

In the first week of Operation Neptune, more than 350,000 searches of INTERPOL databases resulted in the detection of four suspected foreign terrorist fighters and the localization of a missing person.

Trade and customs officials discuss trade facilitation in Central Asia at OSCE-supported workshop in Tajikistan



Senior trade and customs officials from five Central Asian countries, Afghanistan, and their main trading partners – Russia and Turkey, received practical guidance on trade facilitation at a three-day annual training workshop in Dushanbe. The event was jointly organized by the OSCE Programme Office in Dushanbe and the United Nations

Economic Commission for Europe. The OSCE Border Management Staff College in Dushanbe hosted the workshop.

This interactive and practice-oriented workshop aimed at equipping participants with knowledge on various tools and approaches for trade facilitation implementation in the region and engaging them in discussions on policy instruments for enhancing efforts to achieve trade facilitation in Central Asia.

The workshop was attended by 26 participants from Afghanistan, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, Turkmenistan, Turkey, and Uzbekistan. It covered current activities in the implementation of the World Trade Organization's Trade Facilitation Agreement and the practical steps towards facilitating procedures on borders with Uzbekistan.

OSCE celebrates World Day against Trafficking in Persons in Kyrgyzstan

A scientific conference titled Current challenges of human trafficking, attended by representatives of scientific and education organizations of Kyrgyzstan, was held in Bishkek on 30 July 2018, on the occasion of World Day against Trafficking in Person.



The conference was organized by the Kyrgyz Ministry of Education and Science, the OSCE Programme Office in Bishkek, the International Labour Organization and the association El Agartuu.

Various research findings on human trafficking in Kyrgyzstan showing that the country serves as the origin, transit or destination for victims were presented at the conference.

"Labour and sexual exploitation of people is an invisible but serious issue across the world, including in Kyrgyzstan,"

said Head of the OSCE Programme Office in Bishkek Pierre von Arx. "As a counteraction, OSCE supported the development of the National Action Plan on anti-trafficking, which addresses four main areas of combating human trafficking: prevention, prosecution, victims protection, and partnership between state bodies, civil society and international organizations."

Nurzhan Tulegabylova, the head of El Agartuu, said that international reports suggest that over 80 per cent of victims of transnational trafficking are women and children, 70 per cent of which are sold to another country for the purpose of sexual exploitation. "However, precise statistics of trafficked victims in Kyrgyzstan are not yet available, because trafficking is still unfortunately treated as a latent problem."



Mediterranean Migrant Arrivals Reach 59,271 in 2018; Deaths Reach 1,504



IOM reports that 59,271 migrants and refugees entered Europe by sea through 5 August 2018. That total compares to 117,102 at this time last year, and over 263,436 at this time in 2016.

Arrivals to Spain (see chart below) lead all countries with 23,741, or just over 40 per cent of all Mediterranean irregular migrants, who this year have surpassed those coming on competing routes. Their migration volume has

USD 45 Million Needed for 2018-2020 Migrant Response in Horn of Africa, Yemen



IOM and its partners launched a Regional Migrant Response Plan (RMRP) for the Horn of Africa and Yemen through which they are appealing to the international community for USD 45 million. The plan details support to migrants on the move in the Horn of Africa and Yemen from 2018 to 2020.

The response plan, developed in coordination with regional and country level non-governmental and intergovernmental partners, is a migrant-focused humanitarian and development strategy for vulnerable migrants from the Horn of Africa, specifically those from Somalia, Djibouti and Ethiopia, moving to and from Yemen. The plan targets some 81,000 people.

Irregular migration from the Horn of Africa to the Gulf

nearly tripled the number of those registered at this time last year, when some 8,677 had arrived through 31 July.

Arrivals to Italy trail Spain by almost 5,000. Two weeks ago, the gap between those two destination points was just under 200 individuals – an indicator of how quickly the Spanish route has surged. Italy now reports receiving less than a third of all irregular sea arrivals (around 32 per

cent), while Greece continues to receive about 28 per cent, an amount that has remained steady throughout the year.

Significantly, Greece’s arrivals thus far in 2018 are running nearly 5,000 ahead of last year’s totals on this date, an increase of almost 50 per cent. Arrivals to Italy, on the other hand, are down over 80 per cent compared to 2017 data.

countries has been steadily increasing over the past few years, with approximately 100,000 people entering Yemen, a major transit point on this route, in 2017. Often, migrants and refugees cross the Gulf of Aden from Djibouti or Somalia, arriving in Yemen with the support of smugglers.

The countries on this route are beset with humanitarian challenges. In Yemen, partners estimate that more than 20 million people need humanitarian assistance, while Somalia and Ethiopia are also in the grip of complex emergencies because of conflict and recurrent disasters.

The plan estimates that, like in 2017, up to 100,000 new arrivals from the Horn of Africa will reach Yemen in 2018, while 200,000 migrants and refugees will return from the Kingdom of Saudi Arabia and Yemen to the Horn of Africa countries in the same period. Of these, 150,000 and 50,000 will return to Ethiopia and Somalia, respectively.



GLOBAL REVIEW OF MIGRANT SMUGGLING DATA AND RESEARCH

At the 2018 International Migration, Integration and Social Cohesion (IMISCOE) Conference in Barcelona last month the IOM launched its newest publication *Migrant Smuggling Data and Research: A Global Review of the Emerging Evidence Base – Volume 2*.

The UN Migration Agency notes that this report picks up where the first volume left off, building on a review of current migrant smuggling data and research by covering additional geographic areas that could not be included in the first volume. Volume 2 also delves into migrant smuggling in specific countries seriously affected by this transnational phenomenon, such

as Ecuador and Mexico.

Marie McAuliffe, IOM's Head of Migration Policy Research, organized and co-edited the report.

Volume 2 highlights several aspects that are common to migrant smuggling in various locations, namely its clandestine and hidden character; the agility and dynamism of



smugglers, facilitators, networks and migrants; and the variable impacts on people, most apparent when things go wrong and people are harmed or die en route.

The report is part of a broader project to counter migrant smuggling, of which research is one key pillar. In her speech to launch the publication, McAuliffe noted that “Just as responding to migrant smuggling is challenging for all these reasons, researching migrant smuggling is also challenging. It can be demanding and at times dangerous, but it is also important.”

She went on to stress that research and critical enquiry can help us learn from migrants by documenting their experiences, recognizing their circumstances and better understanding their decisions so as to help amplify the voices of those use or are exploited by smugglers.

Florian G. Forster, who leads IOM’s Immigration and Border Management (IBM) Division, said the report was financially supported by the Republic of Turkey.

Forster, who is coordinating IOM’s efforts in the field of counter migrant smuggling, underlined the importance of partnerships and close cooperation among the relevant agencies within the United Nations system: “IOM notably cooperates very closely with UNODC, the recently launched initiative by the two UN bodies for a Joint Platform on Counter Migrant Smuggling being another important element of this coordinated UN system-wide effort.”

Three research-specific recommendations for countering smuggling were issued based on the two volumes of the report: partnerships between policymakers and researchers on aspects of migrant smuggling should be strengthened; research capacity and institutions within regions should be built up in regions and countries where smuggling is prevalent; and emerging and priority topics for research and data collection should be points of focus in the development of global, regional, and national policies that are better able to respond to migrant smuggling effectively.

In his forward the Director General, William Lacy Swing said:

The smuggling of migrants across international borders on routes crossing land, sea and air continues to pose a challenge to migration governance and impedes safe and orderly migration. Migrant smugglers

are increasingly becoming a central part of the irregular migration journey, resulting in enormous profits for criminal smuggling networks while reducing the ability of States to manage their borders. Given that it is often a clandestine undertaking, migrant smuggling may only become visible when tragedies occur or emergency humanitarian responses are required, such as we have seen intensify in recent months in Libya. In 2017, for example, the International Organization for Migration (IOM) arranged for the return home of more than 19,000 migrants who had become stranded or detained in Libya, many at the hands of smugglers and traffickers.

Events involving people drowning or perishing inside trucks or caught up in modern-day slavery networks regularly capture the media’s attention, but the headline-grabbing stories are likely to be just the tip of the iceberg. The recorded number of migrant deaths or missing in four years (between 2014, when IOM started the Missing Migrants Project, and 2017) is more than 25,000 – 2016 being the deadliest year with 8,067.

Reliance on smugglers makes migrants particularly vulnerable to abuse and exploitation and heightens the possibility that they could become trafficked. Migrants who have experienced abuse by smugglers have little effective recourse to justice. In this ever more pressing situation, States are being severely tested in the fulfilment of their responsibilities to protect migrants’ rights and manage their borders.

Against this backdrop and building on



the contribution of the initial volume published in late 2016, it is timely that we complete a review of current data and research on migrant smuggling. The report builds on the first volume by covering geographic areas that could not be included in volume 1, while also delving into migrant smuggling in specific countries seriously affected by this transnational phenomenon.

Volume 2 is again the result of a collaboration between IOM and researchers from a range of backgrounds and academic disciplines and was supported by the Government of Turkey. As a host country of some 3.5 million

Syrian refugees and a transit country of significance, Turkey – along with many other countries – experiences first-hand the considerable challenges in combating migrant smuggling while at the same time supporting

refugees in need.

This report is part of a broader project to counter migrant smuggling, of which research is one key pillar. As we respond to Member States and Organizational priorities, including in the context of the current negotiations on the draft global compact for migration, we hope that readers will find this second volume as useful as volume 1. Both reports are aimed at policymakers, researchers, analysts, students and practitioners working on the complex topic of migrant smuggling. The work undertaken and presented here provides a solid base to build upon and reassess in the years ahead in order to gauge progress on the increasingly important collection, analysis and reporting of data and research on migrant smuggling globally.

The full report is available at

http://publications.iom.int/system/files/pdf/migrant_smuggling_data_vol2_0.pdf.

Cross-border e-Commerce Police action leads to 95 arrests

Police forces across Europe have arrested 95 professional fraudsters and members of internet-based criminal networks in a successful cross-border e-Commerce Action (eComm 2018).

The joint law enforcement operation, coordinated by the European Cybercrime Centre (EC3) from Europol's headquarters in The Hague, was supported by 28 countries and ran from 4 to 15 June 2018. It received the direct assistance from merchants, logistic companies, and banks and payment card schemes. Europol also supported national authorities on-the-spot by providing analytical services in their investigations.

The main goal was to target online fraud through a coordinated law enforcement action within the European Union (EU) and beyond, followed by an awareness-raising

campaign. This action also marks the start of several investigations with more arrests expected in the next few months. The activity was inspired by a similar UK pilot conducted in collaboration with Visa.

The suspects arrested during the operation were responsible for more than 20 000 fraudulent transactions with compromised credit cards, with an estimated value exceeding EUR 8 million.

The e-commerce action focused on combating card-not-present (CNP) fraud, to help create a safer online environment for customers worldwide by sharing information and developing best practices between law enforcement and the private sector. It promotes the hashtag #BuySafePaySafe: tips to avoid becoming a fraud victim.

Experts from Sudan, Libya, Niger, Chad discuss border security

Experts from Sudan, Libya, Niger and Chad held meetings in Sudan's capital Khartoum to discuss border security and combating cross-border crimes and human trafficking.

The meetings seek to reach consensus agenda for the third ministerial meeting of the four countries, which will begin in Khartoum Thursday on joint borders with the participation of foreign, defense and interior ministers as well as chiefs of security.

Sudanese State Minister for Foreign Affairs Mohamed Abdalla Idris praised the efforts of the four countries to

reach common understandings and cooperation to face the threats against their joint borders, a statement said.

He also praised the framework agreement they reached last June in the Chadian capital Ndjamen, reiterating Sudan's support and readiness to implement the agreement and establish the mechanism agreed upon.

The deal stipulated steering joint patrols on the borders, exchanging information, establishing a center for joint operations, and implementing development projects along the joint borders.

Pakistan Will Add 60,000 Troops to Patrol Afghan Border

Pakistan will add as many as 60,000 troops to boost its patrols along its disputed border with Afghanistan in an effort to curb the flow of insurgents passing between the two nations.

The move will consolidate Pakistan's border operations, which have been beefed-up in recent years after widespread insecurity wracked the country following the U.S. invasion of Afghanistan. Domestic terror-related violence is now at its lowest in more than a decade. The

army, which has 661,000 regular and paramilitary troops, have previously been more focused on the country's eastern border with arch-rival neighbor India, with which it's fought three wars against since British India's partition in 1947.

Pakistan has come under increasing pressure to act against the Afghan Taliban and the affiliated Haqqani network.

Efforts to combat trafficking, including of children, must focus on both effects and roots of this crime, OSCE officials say on world anti-trafficking day



Effective policies to combat trafficking in human beings, including the trafficking of children, must focus on both the effects and the roots of this terrible crime, OSCE senior officials said today, on the occasion of the World Day against Trafficking in Persons.

Such policies need to include a focus on a survivor-centred approach, tailored to the needs of both adults and children, as well as on measures to eliminate the ability of traffickers to profit from their crime, the officials said.

“A survivor-centred approach that is gender and culturally sensitive can be achieved by strengthening national referral mechanisms to include survivors’ voices and a focus on their needs in all aspects of policy development and implementation. This is important to guarantee that rehabilitation of, and assistance to human trafficking survivors is rooted in international human rights standards,” said Ingibjörg Sólrún Gísladóttir, Director of the OSCE Office for Democratic Institutions and Human Rights (ODIHR). “At the same time, disruption strategies should be in place to ensure that this crime becomes unprofitable, by curbing demand, inhibiting financial flows to organized criminal networks and empowering survivors to prevent re-trafficking and re-victimization.”

According to the 2016 UNODC Global Report on Trafficking in Persons, 27 per cent of reported global trafficking cases

occur within the OSCE region. More than half of those trafficked worldwide are women, and one in five is a child.

OSCE Secretary General Thomas Greminger noted that UNODC had chosen responding to the trafficking of children and young people as the focus for this year’s World Day and stressed that in recent years, there has been an increased focus within the OSCE on combatting the trafficking of children in particular.

“With the adoption of a comprehensive Ministerial Council decision against child trafficking as well as other forms of sexual exploitation, the OSCE unequivocally reiterated that there is no place in our region for the abuse of children,” Greminger said. “While maintaining close attention to persistent forms of child exploitation, both transnational and internal, our Organization is committed to helping countries engage partners, including civil society, the business community, the travel and tourism industry, the technology industry, and international organizations across the full spectrum of anti-trafficking efforts to prevent harm, protect victims and hold traffickers accountable.”

Valiant Richey, the OSCE Acting Co-ordinator for Combatting Trafficking in Human Beings, stressed that the Organization’s efforts to address trafficking in children directly benefit from such engagement.

“Mindful that the best interest of the child is a primary consideration, and that a trauma-informed approach should take into account the respective gender-specific concerns of girls and boys, the OSCE is aiding in the promotion of innovative, partnership-oriented and informed responses from policy to practice,” said Richey. “Through our research on technology, our ground-breaking training programmes and our workshops on migration, we are working to enhance the protection, safety and health of all children, while building more effective and efficient criminal justice systems to investigate and prosecute traffickers.”

Agreement against organized crime in Latin America



The European Union supports the signing of a police cooperation agreement between 5 countries through the AMERIPOL support project.

Authorities from five Latin American countries met in Buenos Aires to sign the Police Cooperation Agreement in the fight against transnational organized crime. An agreement sponsored by the European Union through the project EL PACCTO: Apoyo a AMERIPOL, managed by the FIIAPP.

The Minister of Security of Argentina, Patricia Bullrich, the Minister of Government of Bolivia, Carlos Romero, the Minister of Security of Brazil, Raul Jungmann, the Minister of the Interior of Ecuador, Lino Mauro Toscanini, and the Deputy Minister of Security of Panama, Jonattan del Rosario have attended this signature under the AMERIPOL Summit: "Road to institucionalización".

This Agreement constitutes a fundamental advance in the fight against organized crime at the regional level, integrating operational information for joint

investigations and contributing to a safer world.

The ambassador of the European Union, Aude Maio-Coliche, has highlighted its importance for the establishment of a coordinated police cooperation between the Latin American region and EUROPOL, and has shown the commitment that the EU has with the region through its Action Outside in the fight against organized crime. For its part, the Minister of Security of Argentina has put in value the importance of this agreement, because it is the first of these characteristics signed in the region.

The leader of the AMERIPOL support project, Marcos Alvar, has reviewed the background of this agreement, such as the support provided by the European Union and the Spanish National Police in the first phases of the project. Through this work, the SIPA I (AMERIPOL police information system) has been developed, which already manages more than 30,000 drug trafficking records.

Regarding its future, the system is expected to evolve towards SIPA II and expand to crimes related to transnational organized crime beyond drug trafficking: trafficking in human beings, cybercrime, illegal immigration, gender violence and others.

These data can be stored and exchanged in a secure manner between the parties to combat organized transnational crime in a practical, effective and proactive manner. And the implication of these five countries responds to the need to equip themselves with an instrument that allows this controlled exchange of information. As of its signature, the Agreement is open to the adhesion of other countries belonging to AMERIPOL.

AMERIPOL presents its activities and goals

In spite of its socio-economic progress, the region continues to face significant challenges in the area of public safety. The project Support for AMERIPOL, financed by the European Union and managed by FIIAPP, organised an event at its headquarters in Bogotá, at which the audience was presented with the work done in the previous phase of the project and the activities planned for the three years of the second phase.

In addition, a special emphasis was laid on the importance of completing the signing of the Quito Agreement, and developing an AMERIPOL Police Information System, which is to include both strategic and operational information in order to contribute to fighting organized crime. The event was attended by the military and interior attachés to Colombia.

AGENCY NEWS AND UPDATES

Camels join police in new border patrol unit



A new police unit has been unveiled to patrol remote sections of the Kenya-Somali border in efforts to combat banditry.

The pioneer camel patrol unit under the Border Patrol Unit of the Administration Police Service will be based in Isiolo County and will involve 50 camels that are currently being trained.

The creation of the unit was informed by rising cases of terror attacks targeting security personnel on patrol in far-flung areas.

Police statistics show up to 70 police officers have been killed in the last two years in separate attacks by terrorists using Improvised Explosive Devices (IEDs). The officers are usually targeted while driving through harsh terrain that

makes their vehicles vulnerable to attacks by bandits and terrorists.

The camels will be used to patrol parts of North Eastern region as well as areas prone to cattle rustling.

Smart fence to guard border in Punjab soon

In a major move to prevent cross-border smuggling and infiltration, the central government is going to replace the existing border fence with a smart one all along the international border with Pakistan in Punjab. Inspector general of the BSF Punjab Frontier, Mukul Goel said this was likely to be done in near future.

While denying to elaborate further on the subject, he said a pilot project was going on outside Punjab and once it achieves success, the existing border fence would be replaced with the smart fence. In past, Union minister of state for home affairs Kiren Rijju had announced that the smart fence would be installed by end of 2018 or early 2019 but the government has not even started the work. The smart fence will be erected all along the nearly 553km

stretch of the Indo-Pak international border in Punjab.

Comprehensive border security measures to be completed in 100 days

The Turkish government has not let up on its fight against terrorism and illegal crossings across its borders. In the next 100 days, as per Ankara's action plan announced by President Recep Tayyip Erdoğan, the construction of border walls and the establishment of state-of-the-art security systems will be completed.

In order to combat terrorism, smuggling and irregular migration, the Interior Ministry has been working non-stop to increase the security of the country's southern, eastern and western borders. The speeding up of the work on the border walls was announced Saturday in a written statement by the Interior Ministry.

The 100-day action plan states that the lighting of the 18-kilometer-long Iranian border with eastern Ağrı and Iğdır provinces will be

completed in the next 100 days.

ICA trials eye scans to boost border security



Eye scans for Singaporeans and permanent residents are being trialled at Woodlands and Tuas checkpoints, and Tanah Merah Ferry Terminal, as part of plans by Singapore's border agency to better secure the borders.

The trial, conducted at selected counters at the three checkpoints, involves officers scanning travellers' iris images in addition to fingerprint verification, an Immigration and Checkpoints Authority (ICA) spokesman said.

Intensive traffic at the Bulgarian-Romanian border

The traffic of the entrance and exit for passenger cars at Kalotina border checkpoint, Kulata border checkpoint and Makaza border checkpoint is intense. At Kapitan Andreevo Border Crossing, traffic is intense for outbound trucks. At the Bulgarian-Romanian border traffic is intense at all border checkpoints for passenger cars at the entrance. This was reported by the Border Police press center. Traffic information on border crossings is at 16.00. At the Bulgarian-Macedonian border traffic is normal at all border checkpoints.

Operation Stonegarden Supports Border Security in Rio Grande Valley



The U.S. Border Patrol's Rio Grande Valley Sector continues to coordinate border security efforts with state and local law enforcement agencies through Operation Stonegarden. Operation Stonegarden provides funding to state and local law enforcement agencies to enhance border security and keep communities safe.

In July, under Operation Stonegarden, state and local law enforcement agencies arrested a total of 43 illegal aliens during four significant smuggling attempts. Some illegal aliens were discovered in the trunks of vehicles and others were found in local stash houses. One of the individuals being smuggled was identified as having a prior conviction for Statutory Rape-2nd Degree and had served one year confinement for that crime.

All the individuals were turned over to the U.S. Border Patrol for appropriate processing.

American teenager arrested at border with 11,500 fentanyl pills

A teenager was arrested at the U.S.-Mexico border with what official said was 11,500 fentanyl pills.



It is the largest fentanyl pill bust at the border ever, according to the Los Angeles Times.

Cristian Araujo Aguirre, 19, was also transporting 61 pounds of meth and 14 pounds of heroin.

Police night-time swoop on boat heading for Kent beach find 'illegal migrants'



Police smashed an alleged people-smuggling ring as they waited under cover of dark to intercept a speedboat packed with illegal immigrants.

Officers swooped on the boat, carrying illegal migrants from Vietnam, as it landed on a Kent beach under the cover of darkness.

The group were caught in the early hours of the morning as their speedboat landed on the beach in Walmer.

The eight arrests were part of a joint operation involving Kent Police, the Eastern Region Special Operations Unit (ERSOU) and Border Force.

A 35-year-old man from Eyeworth, Bedfordshire, and a 34-year-old from Oxford were also arrested at the scene on suspicion of conspiring to assist unlawful immigration to the UK.

Three other men were then arrested later that day in connection with the investigation and have been taken into police custody for questioning.

MZP push for tight border security

Mizo Zirlawi Pawl (MZP), an apex student body in state had asked the government to make strict laws and tighten security along the Mizoram border to prevent the influx of illegal immigrants from Assam.

MZP has also threatened to set up infiltration gates along the Assam-Mizoram border if the government fails to take steps by August 15.

President of MZP, L. Ramdinliana Renthlei expressed apprehension that Mizoram might face an influx of foreigners from Assam after publication of the draft NRC in which about 40 lakh people have been left out.

He said many neighbouring states of Assam have sounded the alert in view of the possible entry of the foreigners from Assam.

Renthlei slammed the state government for being silent and for not taking any security measures in view of the possible entry of foreigners from the neighbouring state. He said many foreigners, who have been left out in the draft NRC might try to enter Mizoram as well.

He also said that after there were reports about the possible entry of foreigners

from Assam, the students' body had approached the state government to tighten security along the Mizoram border.

Serbia, Montenegro sign cross-border agreements



Deputy PM and Interior Minister Nebojsa Stefanovic spoke on Wednesday in Belgrade with Montenegrin Minister of the Interior Mevludin Nuhodzic.

According to the Serbian government, they discussed cooperation between the police of two countries in the fight against organized crime.

After the meeting, the ministers signed seven agreements and two protocols on cross-border transportation and border control.

The interlocutors pointed out that the police of the two countries, with even more intense cooperation, want to send a clear message to criminals - that they will fight against them even stronger and that they will stand in the way of organized criminal groups.

Border between Kosovo and Albania to be opened

Albanian Diaspora Minister Pandeli Majko is announcing the opening of "the border" between Albania and

Kosovo.

"We want to open the border between Albania and Kosovo. The prime minister told me that a decision has been made. Starting on January 1, free movement between Albania and Kosovo began," Majko said.

Bavaria Reconstitutes Its Border Police



Bavaria, Germany's second most populous state, recently re-formed its previously dissolved border police. The Bavarian Grenzpolizei (German for "Border Police") has been reconstituted in order to address crimes and immigration violations committed by the migrants currently flooding the Federal Republic of Germany.

Heathrow Airport border staff 'seize missile parts that were being sent to Iran'

A suspected attempt to fly missile warhead components to Iran via Heathrow has been thwarted by the UK Border Force.

At least two "O rings" — which can be used to form seals in rockets — were detected during an inspection of freight being flown out from the airport.

They were supposedly being sent

for use in the Iranian oil industry. But Border Force staff halted the shipment after becoming suspicious that the real intention was to use them in missiles.

An investigation is now under way which could lead to criminal action against those responsible for sending the parts.

\$150m sanctioned by US is for Pak-Afghan border security

The \$150 million in the United States (US) Department of Defence (DOD) funding authorised for the financial year 2019 is dedicated to Pakistan's border security operations, a US embassy spokesperson said.

Border Guard Service of Ukraine seeks to modernize ships, boats for maritime border guard



Head of the State Border Guard Service of Ukraine Petro Tsyhykal during his working visit to Lithuania studied experience of the Lithuanian border guard service and told about the plans of the Ukrainian authority.

The press service of the State Border Guard Service of Ukraine said that Tsyhykal met Commander of the State Border Guard Service of Lithuania Renatas Požėla and studied the

details of their state border guard system.

Tsyhykal said that the State Border Guard Service is improving the system of control over the maritime surface picture and intensively uses maritime border guard, which includes about 70 ships and boats of various projects. According to him, the State Development Program provides for the reform of maritime border guard in accordance with the standards of NATO and the European Union.

Drug seizures drop nearly 90 percent at Border Patrol checkpoint



Drug seizures at the Falfurrias checkpoint dropped nearly 90 percent from 2014 to 2017, according to the Texas Department of Public Safety.

Drug seizures at the Falfurrias checkpoint dropped 87.77 percent, according to the meeting minutes. Drug seizures at the Sarita checkpoint plummeted too, falling 78.69 percent during the four-year period.

Hidalgo County Sheriff Eddie Guerra said the numbers reflected a major shift by smugglers.

"These organizations are making more money smuggling humans than smuggling narcotics," Guerra said.

Big drug busts became less common when Colorado and other states

legalized marijuana, Guerra said. Measured by weight, marijuana made up the majority of drug seizures..

Laredo PD and Border Patrol disrupt narcotic smuggling attempt



Border Patrol Agents assisted the Laredo Police Department in disrupting a narcotics smuggling attempt.

LPD notified the Laredo Sector Border Patrol that they were in pursuit of a 2006 red Dodge Durango suspected of being loaded with narcotics.

The subject attempted to abscond on foot, but after a brief chase, the LPD officer and a Patrol Agent apprehended him.

A search of the vehicle yielded five bundles of marijuana weighing 360 lbs. with an estimated street value of \$288,000.

Voiceprint Reporting – New Authentication Method for Border Control

Biometric voiceprint technology will be applied in border security in Canada. In an effort to keep fewer people in immigration detention while upholding public safety and national security, the Canada Border Services Agency (CBSA) is rolling out a voice reporting system that uses biometric

voiceprint technology as one of the new elements to its “Alternatives to Detention” program. Other elements to the program include in-community tailored case management services and electronic monitoring.

The voice reporting system will use the voiceprint technology to enable as many as 10,000 individuals to report to the CBSA at agreed-upon intervals, using either cellphones or landlines.

Serbian Police Seize 590 kg of Marijuana at Bulgarian Border



Serbian police seized two large shipments of marijuana at the border crossing with Bulgaria, Serbian interior ministry said.

“Members of the border police directorate of the interior ministry confiscated 590 kilograms of marijuana and arrested two people,” it confirmed.

The police operation took place at the Dimitrovgrad border crossing in southeast Serbia.

The press release added that 292 packages of the narcotic weighing around 316 kilograms were discovered in a truck with Croatian registration plates, while the 56-year-old driver is a citizen of Bosnia and Herzegovina.

Moreover, in a truck registered in

Serbia, driven by a 51-year old Serbian truck driver, police found another 253 packages of marijuana, weighing 274 kilograms in total.

Border Security Force (BSF), Assam Rifles sensitised to prevent entry of Rohingyas



Border Security Force (BSF) and Assam Rifles have been sensitized to ensure that members of the Rohingyas minority do not enter the country and states have been asked to enumerate and confine those who have immigrated illegally.

Home Minister Rajnath Singh told the Lok Sabha during Question Hour that his Ministry had issued an advisory to the states in February concerning the Rohingya.

“The BSF and Assam Rifles have been fully sensitized to ensure that Rohingyas are not able to enter,” Rajnath Singh replied to a query posed by a Shiv Sena member. He said Rohingyas have, however, entered the country in “large numbers”.

“It should not happen that the Rohingyas spread out and stay wherever they want,” he said, adding that the states have been advised to prepare their “biography” (profiles) and take biometrics. “The advisory also says that their movement should also

be monitored and the states should be fully alert,” the Minister added.

Border Police & VAT Inspectors Nab Cigarette Smugglers from the PA



Israeli Border Police officers foiled attempts to smuggle 770 boxes of cigarettes, 40,000 rolled cigarettes and tobacco from the territories into Israel in the Barta'a area.

Border Police operate in areas adjacent to Yehuda and Shomron in order to provide protection in addition to thwart and seize the smugglers of goods in order to protect the safety and security of the public.

In a joint activity of Border Police officers together with VAT inspectors of the Israel Tax Authority, a vehicle was stopped for inspection which came from the territories, which raised the suspicions of the police near Nachal Iron, which is more commonly known by the Arab name, Wadi Ara, an Israeli Arab municipality in the north.

In the vehicle, police found large amounts of cigarettes and tobacco smuggled from the PA (Palestine Authority) village of Barta'a. They found 770 boxes of cigarettes of various kinds in the vehicle in addition to an unspecified quantity of tobacco.

TECHNOLOGY AND BORDER SECURITY IN EUROPE



Border security has always been complicated when it concerns the 28 countries that comprise the European Union (EU). The conflict between vision and need is at the center of the ongoing debate.

The vision of the EU for the free movement of people, goods, services and capital between countries, is unhappily married to the need of these same countries to manage migration and maintain internal security. The European refugee and migration crisis has compounded matters "... with tens of thousands of people

arriving by land and boat to Europe fleeing conflict, poverty and disasters in the Middle East and Africa." (<https://www.independent.co.uk/news/world/europe/eu-border-control-spending-refugee-crisis-austria-coast-guard-mediterranean-a8397176.html>).

With the amount of people crossing borders in Europe expected to reach 887 million by 2025 (European Commission 2016 Report), threats such as unauthorized overstays, terrorism and organized crime will only compound border challenges. Criminals have taken notice and

regularly exploit this scenario by taking advantage of borders too bogged down with issues of processing overloads, and administrative inefficiencies to protect effectively.

The result is that transnational terrorists and members of organized crime illegally cross borders to engage in human and drug trafficking, money laundering, and the import of counterfeit or unsafe goods. Often, these crimes are facilitated by technologies such as mobile devices, the Internet, social media, and even encrypted apps.

Border control authorities have had to rethink their strategies in order to stay ahead of criminal digital tactics. "...border control has evolved from "narrow" protection of territory by the border guard to a complex high-technology process...and a wider concept of border security with large-scale data management in cyberspace." (<https://www.tandfonline.com/doi/full/10.1080/09662839.2016.1276057>)

With this new perspective comes a digital horizon that demands large-scale data management and analysis to react to the dangers of a connected criminal underworld.

On the perimeters of this wild technological arena, border agencies are tasked with needing to quickly sort out and identify criminals from the rest. To accomplish this task, especially when peak activity has a negative impact on success, digital solutions have been introduced to scale, automate and speed up border procedures.

Some European countries have



embraced innovative border security initiatives such as "Smart Borders" with automated border control (ABC) systems, biometrics for identity verification and satellite-assisted surveillance. While tools such as ABC may be useful, unfortunately until adoption improves these solutions will not have an impact on present day scenarios such as the influx of "irregular" migrants flowing in from neighboring regions of the European Union.

Lastly, but perhaps most importantly, effective emergent border security technologies tend to receive a "knee-jerk" reaction from societies. The controversy lives at the intersection of effective border security technology and the growing gaps between the technology, citizens, and politics. Border agencies leveraging cutting-edge digital security must factor-in the need to safeguard individual privacy rights while protecting the common good. In addition, these agencies

face other challenges such as strict limitations of data usage that restrict certain access to border control databases.

The conclusion many seem resigned to accept is that the EU and border security will continue to be a challenging dynamic. The diverse approach to migration in Europe from open border advocacy to illegal immigration restrictions in whatever way the law will allow has become – as it has in many countries around the globe - an unavoidable reality needing to be addressed. And as these border crimes continue to advance in the level of sophistication, technology will continue to be at the center of all discussion related to border security, for years to come.

Visit www.cellebrite.com

BORDER MANAGEMENTS ANNUAL GATHERING

EVENT PREVIEW



19th-21st March 2019
Casablanca, Morocco
www.world-border-congress.com

The annual gathering of the international border management and protection community moves to Casablanca, Morocco on 19th-21st March 2019.

Co-hosted by the Ministry of Interior and General Secretariat for Migration and Border Surveillance of Morocco (Directeur de la Migration at de la Surveillance des Frontieres), the World Border Security Congress is delighted to be welcomed to the North African country and economic hub of the region.

The 2019 World Border Security Congress will see over 230 delegates from more than 50 countries gather for the 3 day meeting for some great discussions, meetings, workshops and networking with colleagues and peers from the global border security community.

Borders in the Maghreb are increasingly dangerous. Armed with tools designed for the pre-Arab Spring environment, Morocco, Algeria and Tunisia face a complex new world of transnational actors that leverage



the African Union Economic, Social and Cultural Council (AU-ECOSOCC), National Security & Resilience Consortium, International Security Industry Organisation and International Association of CIP Professionals, demonstrating the World Border Security Congress remains the premier multi-jurisdictional global platform where new challenges and treating those challenges as opportunities to do things better in the future.

REGISTRATION OPEN

Governments around the world need to continue to invest in their border security, as a wide range of threats, such as combating terrorism, controlling the movement of goods and monitoring personnel across international borders, continue to pose challenges requiring round the clock monitoring.

Registration for the 2019 World Border Security Congress is now open and if you are interested in attending, register your place at www.world-border-congress.com/registration.

Further details and the agenda will shortly be announced and can be viewed at www.world-border-congress.com.

borders for profit and for sanctuary.

The Arab Maghreb Union (AMU) was designed to deepen cooperation among the Maghreb states, buttress the region's economy through greater interregional trade, enable the free movement of people, and lay the groundwork for future political integration. However, the promise of an integrated Maghreb has not materialized, though the union still exists.

The region is also a main thoroughfare for the West African human trafficking and migration route to Southern Europe, with access to Spanish soil and the EU border in the North African enclaves of Melilla and Ceuta, just a short journey from mainland Europe across the Mediterranean, whilst smuggling of arms and illegal goods across North Africa also adds

pressure on the governments and border security forces of the region.

Advancements in technology are assisting in the battle to maintain safe and secure international travel and detect illicit goods and smuggling. The border security professional still remains the front line against these threats.

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.

Supported by the Organisation for Security & Cooperation in Europe (OSCE), the European Association of Airport and Seaport Police (EAASP),



UK Border Force Deploys Agilent Resolve Handheld Raman Systems for Hazardous Material Detection

Agilent Technologies Inc. today announced that UK Border Force is now using Resolve, the company's handheld Raman system, to detect bulk chemicals—whether benign, hazardous, or illegal—through opaque packages and containers.



This system is the latest addition to a suite of advanced technologies deployed to detect illegal shipments. The deployment is part of

a multi-million-pound framework agreement between the UK Home Office and Agilent Technologies.

Rigaku Analytical Devices Chosen for Project Global Shield, a World Customs Organization Program

Rigaku Analytical Devices has been chosen to provide its Progeny ResQ system to be used in Project Global Shield, a World Customs Organization (WCO) Program. A minimum of 38 Progeny ResQ analyzers will be used in global customs operations to identify and analyze chemical products, including explosives, toxic industrial substances, and precursor chemicals

Lead by the WCO and in partnership with the International Criminal Police Organization (INTERPOL) and the United Nations Office on Drugs and Crime (UNODC), Project Global Shield initiated in 2010. The program commenced as a six-month joint operation to combat increasing illicit use of precursor chemicals used to manufacture improvised explosive devices (IEDs) by monitoring cross-border movements. Following initial success of the project, in March 2011 the WCO project transitioned to an expanded long-term program with customs administrations in 85 countries committed to participate in this global collaborative initiative. "We are extremely proud to participate in this important global mission," said Bree Allen, President of Rigaku Analytical Devices. "We are committed to providing the highest performing handheld Raman for explosive and



chemical detection and identification technology to support counter terror and border security operations around the world. Its rapid response time, easy operation, and ability to identify colored materials and through packaging demonstrate how the Progeny ResQ 1064nm Raman analyzer is the instrument of choice for the safety & security industry."

Veridos Wins €340 Million Contract in Bangladesh

Veridos has announced today the conclusion of a major contract. The Ministry of Home Affairs of the People's Republic of Bangladesh, acting through the Department of Immigration and Passport (DIP), has commissioned Veridos with the supply, installation, and implementation of next generation electronic

passports and border control systems in Bangladesh. The contract, with a volume of around €340 million, will run for 12 years.



Bangladesh will move from machine readable to advanced electronic travel documents that meet the highest security standards. This includes high-tech color personalization technology to ensure the ultimate color brilliance of each ePassport holder's image, improving visual verification. With more than 160 million inhabitants, Bangladesh is the world's eighth most populous country and will provide the highest output of passports with color photos worldwide. Major General Md Masud Rezwan, director

general of the DIP, said: "Our citizens will get benefits from the ICAO*-compliant ePassports with convenient and secure travel. With Veridos's unique solution portfolio for the entire value chain for passports and their ID production expertise, we have found the perfect company to implement this turnkey project. With their support, we can enhance the technology by which we can assemble the ePassport booklets in Bangladesh. This creates highly skilled jobs and know-how transfer with Germany."



Harris will supply its XL-200P advanced digital handheld radios that have an intuitive and customizable user interface. The radios are packed with features ideal for mission-critical users: built-in active noise cancellation, Bluetooth® and GPS. They also meet and exceed the stringent MIL-SPEC standards for explosive atmospheres, fluid contamination and immersion.

Additional benefits of the XL-200P to the CBP include: software defined

architecture that enables new capabilities far into the future; multiple bands that solve interoperability issues; and a more simplistic and cost-effective way to deploy and maintain its fleet. Harris' commitment to standards-based systems also means CBP is not locked into proprietary solutions.

"Harris' advanced technology will help CBP's 60,000-plus employees stay better connected as they protect our nation's borders," said Nino DiCosmo, president, Harris Public Safety and Professional Communications. "These contracts are a major step forward in bringing reliable communications to our border patrol customers, who often operate in extremely challenging coverage areas."

Harris Corporation to Upgrade US Customs and Border Protection Communications

Harris Corporation has been awarded two contracts totaling \$26 million to upgrade the U.S. Customs and Border Protection's (CBP) mission-critical communications to safeguard the nation's borders.

Sas R & D Services have introduced the world's first full High Definition Videoscope

Sas R & D Services have introduced the world's first full High Definition Videoscope -Built on the same platform as their respected Ultimate Fiberscope®, The Readyscope offers toughness and dependability with field reparability.

The Readyscope® gives the brightest, clearest,

sharpest HD image of inspections. With



Smiths Detection technology chosen for Standard 3 upgrade at Helsinki airport

Smiths Detection's local partner, Oy Machine Tool Co, has been selected by Finnish operator, Finavia, to support the transition to Standard 3 at Helsinki Airport with approved hold baggage screening systems.



interchangeable monitors, the videoscope offers 10X zoom, a sunshield, damage resistant probe tip and field repairable to save time and money, inspections are conducted without compromising operator's situational awareness. The software is capable of filtering out colors to zero off tints in gasoline or diesel fuels. The full 180 degree articulation offers the best-in-class viewing

capability. Tungsten braid or Nonconductive probes available in either the standard 2.0m/80" length or made to order for specific operational requirements..

Since its introduction the Readyscope has been purchased by US Customs (CBP) - DEA – US State Department and is being supplied to many countries in Europe, Asia and South America.

Included in the contract are eight high-speed, HI-SCAN 10080 XCT scanners, which combine high resolution X-ray technology, computed tomography (CT) and advanced detection algorithms to increase both security and operational efficiency significantly.

Security, speed and efficiency are critical to the extensive development programme underway at the airport, which will allow the airport to serve 30 million passengers annually and increase baggage handling capacity by 50%.

ADVERTISING SALES

Sam Baird
(UK, Germany, Austria, Switzerland, Israel & ROW)
E: sam@whitehillmedia.com
T: +44 7770 237 646

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

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

Annabel McQueen
(Benelux)
E: annabel.mcqueen.am@gmail.com
T: +44 20 8249 6152

