CRITICAL INFRASTRUCTURE PROTECTION SPECIAL ISSUE

THE US, RUSSIA AND 'THE GREAT GAME'

For those not familiar with it the term 'The Great Game' refers to the confrontation between the British and Russian Empires played out right through the 19th Century. Britain and Russia were not the only players but also drew in other players like Turkey, France and Iran (Persia as was).

It involved diplomacy, espionage and war over a vast area of the globe, from the Bosphorus in the West to the Hindu Kush in the East. There was a war in the Crimea and two wars in Afghanistan. Now it might start to sound a bit more familiar.

For the British, the driving factor back then was the defence of India, the jewel of the Empire. For the Russians it was the expansion of their Empire and influence south into the Caucasus, the Near East and Central and Southern Asia, and the need to secure a warm water port.

Jump forward 100+ years and whilst the geographical focus of the game has shifted West to the Middle East and Central Asia, the game continues but with some important changes to the line-up of players.

Whilst post-Soviet Russia is still a central antagonist, the USA has taken over the lead role for the Western powers with UK, France, Turkey and Iran still in the game, but with new players like Israel having taken the field.

So, as President Putin declares "mission accomplished" in Syria and starts to bring his troops home, who is winning the 'The Great Game' Circa 2017.

Well, given the preponderance of forces that the US has over Russia (even without its European allies) it would seem a forgone conclusion that the US would be way out in the lead, if not already back in the changing room drinking champagne.

But not so.

Even though Russia is facing huge economic difficulties at home and its forces are a shadow of their former Soviet self, it could be argued that Russia under Putin has been rather successful in regaining some of the ground lost after the collapse of the USSR, and that the USA has failed to capitalise on what looked like an unassailable lead after that collapse.

So how and why is Putin doing so well?

Well, despite the US's overwhelming advantage in conventional forces, which in the 19th century would have meant that the US could have pressed home its advantage, either by threatening or taking military action, is no longer possible. Because nuclear weapons are a new factor in the game and Russia has lots of them (a lesson not lost on Kim Jong-un and many others decides).

It is this fact, along with control of oil and gas pipelines amongst other things, that has allowed Putin to punch above his weight (to use another sporting metaphor) on the international scene.

What has Putin achieved given his resources has been remarkable. In 2014 he seized the Crimea from the Ukraine with hardly a shot fired and few effective negative consequences. In the same year he backed pro-Russian separatists in Eastern Ukraine, again with few consequences and by doing so has probably stopped the Ukraine joining NATO, a key aim. And now in Syria, Putin has sent in the troops, with the supposed aim of defeating terrorism but with a real aim of keeping his Assad in place, all without getting embroiled in a long-term conflict as many predicted.

He comes away looking like the successful, decisive, independent, strong man of his self-promoted image, and who can argue. Many in the region including countries like Turkey and Egypt may agree. And maybe it will be enough to stop Russians worrying about the state of the economy, democracy and freedom of the press and vote him in for another term, which is probably what it is all about in the first place.

And what about the US? All depends how far back you want to go but the US policy failure in the Middle East is all too apparent. From the early withdrawal of forces from Iraq giving rise to ISIS, the US and European failure to seize the opportunity offered by the Arab spring, the failure of its avowed intention to oust Assad and failure to find peace between Israel and the Palestinians.

Which brings us to President Trumps decision to recognise Jerusalem as capital of Israel. He says that he is simply "recognising a historic and present reality" a phrase much repeated by Benjamin Netanyahu. But in the context of 'The Great Game' does that make it a good decision, I think not. Firstly, he seems to have abandoned diplomacy and negotiation and made the decision unilaterally, without any concessions from Israel, such as a halt to settlement building, a pre-requisite for peace. At the same time, he has upset key allies in the region, strengthened enemies like Hamas and al-Qaeda and is undermining US influence, whilst Putin's star is on the rise.

Ultimately, like Putin, Trump's decision may be more about voters at home than it is about geopolitics, but there are those who will be wondering whether the next decision that recognises an historic and present reality will be for a one state solution, not two!

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/WSRJan18

Managing Resilience in Critical Grid Situations - Success & Challenges

The ENTSO-E Report of the January 2017 Cold Spell provides factual information as to the events which occurred during cold spell of winter 2016/2017 in countries which experienced exceptional challenges during that period. Based on these facts, lessons learned and related areas of focus for the future are presented in the report.

An exceptional situation in January 2017 in Continental Europe resulted in system adequacy and network security issues due to cold spell in several countries. This report confirms that the measures applied during the cold spell period were effective in preventing supply interruption during all times and even more, helped to avoid use of extraordinary measures such as manual load shedding in most critical times. The cold spell, combined with the effects of the other factors which took place, in its severity was unexpected and while indeed the Seasonal Outlook did not foresee this type of event, potential adequacy issues were foreseen for France.

The extended nature of the cold spell affecting multiple countries

simultaneously coupled with the challenges faced in terms of generation adequacy issues (low reservoir levels, outages of key nuclear units, coal and gas supplies disrupted, etc.) by each country over this period was also unprecedented over many past decades.

At the same time and despite such a rare and serious event, the measures developed and the steps undertaken by TSOs, ensured uninterrupted supply and secure system and market operation

during the whole duration of cold spell; it is evident that the coordinated approach of European TSOs prevented further crisis escalation.

Furthermore, cooperation of TSOs and RSCs was demonstrated throughout the whole period. The cold spell was managed effectively at both: the regional and the local level, showing the efficiency and complementarity of the existing inter-TSO coordination and the efficiency of RSCs support to TSOs in the regions where RSCs are active, both in their regular and extraordinary conditions. The new RSC service "short-medium term adequacy", although still under development, already demonstrated in the Continental Western Europe (CWE) region,

» In January 2017 day-ahead baseload wholesale electricity prices rose to the highest level since February 2012, reaching 64 €/MWh in the EU on average. This sharp increase was mainly due to the cold spell that impacted most of the European continent in this month, resulting in increasing heating-related electricity demand that also affected wholesale electricity prices.

» In most of Central, Eastern and South-Eastern Europe there were several days in January 2017 when average daily temperatures were 10 degree Celsius below the long-term daily averages.

» Curtailments in cross-border electricity flows or explicit export bans were imposed in a few EU Member States during the January cold spell.

» Low nuclear availability and dwindling renewable generation resulted in increasing use of fossil fuels in the European energy mix at the beginning of 2017.

its added-value to better manage the adequacy issues at regional level. Regional coordination in South East Europe, if it had been implemented such as in CWE, would have supported the TSOs in this region in addressing the adequacy shortages.

Updating forecast in shorter time periods has been shown as very relevant, whereas midterm forecasts (week-ahead) showed they allow to trigger and set-up exceptional organisation sufficiently in advance to deliver adapted answers closer to real time. For example, there were big differences between Week-1 forecasts and real time, e.g. 94GW actual consumption in France compared with 101GW forecasted in Week-1, making it difficult to anticipate the effective adequacy scenarios and actions to be taken. In case the forecasts would have been realised the situation would have been much more complicated.

ENTSO-E Key Focus Areas are to show that improved processes at TSO and regional level would be beneficial ensuring both, security of operation and security of electricity supply in Europe. The steps foreseen through the application of the proposed regulation on risk preparedness plans in the Clean Energy Package seem promising to develop and implement enhanced principles and processes at regional level in order to face very rare

and tight situations affecting more than one country.

Key Focus Areas

In accordance with its roles to implement and further enhance regional co-ordination, the following recommendations were proposed for implementation primarily at pan-European level.

Seasonal Outlook

» "Stress tests" should be conducted by all TSOs supported by ENTSO-E for pan-European result and by RSCs for (short-term) regional adequacy forecast, not only regarding temperature but also regarding also other relevant conditions based on historical experience and exceptions (e. g. exceptionally dry years, multiple outages, etc.).

» Extremely low temperatures can lead to unplanned outages (incidents) like e. g. frozen river impact on hydro generation, power plant cooling, and coal /gas supply interruptions. ENTSO-E should investigate within the seasonal outlook, how to address multiple outage situations, including the risk level of probabilistic outages of generators by country.

» Hydro modelling is to be investigated including possible synergies with the Short/Medium Term Adequacy forecasting tool. Hydro modelling improvements would further require the implementation of a new tool for the Seasonal Outlooks.

Regional Coordination and Analysis

» Improve the efficiency of inter-TSO cooperation and the involvement of RSCs from week-ahead to intraday especially in SEE where regional cooperation is now being established.

» Mutual exchange of information for safeguarding measures applied among the TSOs needs to be continuously reviewed and information updated between TSOs where the situation may change year on year.

» The Short & Medium Term Adequacy service has proved its importance today as well as in the future as one of the 5 standard services provided by RSCs. Future evolution both, in the direction of short time (D-2, D-1) as well as for longer periods beyond a week is being delivered through pilot projects being implemented within ENTSO-E.

» The implementation of CACM Guideline and more specifically the setup of D-2 to intraday coordinated capacity calculation processes on all borders is a necessary precondition for ensuring secure operation of the interconnected system.

Energy Market

» For South East Europe, further evolution and effectiveness of regional electricity market would need to be of top priority.

Critical Grid Situations and Communication

» Coal storage in the thermal coal based is in general based on market expectations. TSOs to investigate the need of appropriate procedures to monitor and to take measures in the management of coal storages depending on individual risk levels of coal shortages and in line with the national regulation framework

» Due to the link between gas and electricity supply, the TSOs for gas and electricity need to ensure the close cooperation and forward planning of risk scenarios ensuring measures can be taken to guarantee security of supply in both gas and electricity.

2017/2018 WINTER OUTLOOK

The assessment at the pan-European level of electricity security of supply points out some risks for the upcoming winter in case of cold spells and low availability of the generation fleet.

There is no risk to Europe's security of supply to be expected under normal conditions. Under severe conditions, margins are expected to be tight in Great Britain, France, Belgium, Poland and Italy, but the risk of not having enough generation capacity to cover demand is contained in probability.

In case of over-generation (high variable renewable generation and low demand), there may be some curtailment needed in Ireland and in some bidding zones in the southern part of Italy.

Stress tests

Lessons have been learnt from last year's winter; 'stress tests' have been carried out as part of the present Winter Outlook.

Instead of considering situations that only happen in 1 year out of 10, the Winter Outlook 2017/2018 looks at worst-case situations that could occur in 1 year out of 20. Furthermore, ENTSO-E has analysed the risks associated with these extreme situations taking place simultaneously in all of Europe.

Added to these stress tests, the Winter Outlook 2017/2018 contains a qualitative analysis on the risk assumptions made by each transmission system operator (TSO), on risks associated with multiple outages and on risks linked to hydro reservoir levels.

Focus on hydro reservoirs

The hydro reservoir levels in Europe are generally back to historical average, except in Italy and Spain, where the levels are close to the historical minimum values. In France and Switzerland, after dropping to historical low values at the beginning of the year due to the cold spell, the hydro reservoir levels have recovered near to average values. In Austria, the October 2017 level is higher than the historical average after reaching the lowest situation last winter.

The Winter Outlook also analyses the trend in evolution of the generation sources in Europe. In 2017, there has been a continuous decommissioning of thermal power plants, which has been partly compensated by new commissioned renewable generation.

For the full report download at https://www.entsoe.eu/Documents/Publications/SDC/Winter_Outlook_2017-18.pdf

Security, Infrastructure, Rising Taxes and Charges, Smarter Regulation Top Agenda for MENA

The International Air Transport Association (IATA) highlighted five priorities which must be addressed in order for aviation to deliver maximum economic and social benefits in the Middle East and North Africa (MENA) region.

Muhammad Ali Albakri, IATA's Regional Vice President for the Middle East & Africa noted that aviation currently supports 2.4 million jobs in the MENA region and contributes $157.2 billion in GDP. "Aviation has the power to generate significant prosperity. A safe, secure, efficient and sustainable air transport industry pays huge social and economic dividends. But despite the vast benefits enabled by aviation connectivity, the operating environment for airlines in MENA remains challenging," Albakri said.

Speaking at the IATA Middle East and Africa Aviation Day in Jordan, Albakri noted that passenger demand is set to expand by 5.7% each year on average over the next 20 years, to become a market of 380 million passengers in 2035, He urged the region's governments to address five key challenges, so that aviation is able to support this growth and one of those was security:

Keeping aviation secure is integral to a state's responsibility for national security, as highlighted in a UN Security Council Resolution. "Governments have the ultimate responsibility to keep flying safe and secure. But we are in this together. Consultation on security issues among Governments and between Governments and industry needs to happen as a matter of course not as an afterthought," said Al Bakri.

"The lack of consultation prior to the recent ban on large PEDs caused airlines and passengers major inconvenience and left many unanswered questions. While we welcome that the ban was replaced by alternative measures, airlines have had to bear the brunt of the cost burden of implementing these new measures. However, the principle that was confirmed by UN Security Council resolution 2309 puts the responsibility for security clearly on the states." said Al Bakri.

There is an opportunity through the publication of ICAO's Global Aviation Security Plan—also known as GASeP—to provide a comprehensive framework for governments around the world to improve security measures in line with global standards. But GASeP will only be effective if governments cooperate – on capacity building, information sharing, identifying conflict zones and so forth.

Smarter Regulation IATA urges governments in MENA to adopt IATA's Smarter Regulation framework to avoid unintended consequences when designing or implementing aviation policies. "Recently there has been a proliferation of regulations across MENA such as the new consumer protection regulations in Saudi Arabia and that have placed an undue burden on aviation's ability to act as a catalyst for economic and social development. Smarter Regulation is the solution to achieve positive policies that support the growth of aviation and ultimately boost social and economic development," said Al Bakri.

Threats to Critical Infrastructures: An Overview for Telecom and Energy Sector

Doomsday scenarios seems to be more "realistic" when we consider the hyper interconnected nature of critical infrastructures and our desperate dependency to their continuous activities. In fact, today, any small disruption of our electricity systems or the contamination of our water systems could seriously affect and even paralyzed our daily life; additionally their cost would be huge for states' and non-state actors' budgets. For instance the cost of the long and nation-wide black out in Turkey dated March 31, 2015 was calculated around 100 million Dollars. Likewise, according to ENISA's (European Network and Information Security Agency) estimations attacks on critical infrastructure can cost organizations up to €15 million.

A Global Priority

In that respect, "securing critical infrastructures" became one of the priorities of global community's, policy makers' and private sector's current agenda. In addition, even though, every state or actor makes its own definition or prioritization about the response of the question: "What is critical", these systems are generally identified as "assets or systems which is essential for the maintenance of vital societal functions like communications, emergency services, energy, dams, finance, food, industry, health etc."

With respect to their vital role, the nature of threats are evolving and becoming a huge concern in worldwide. According to the Worldwide Threat Assessment of the US Intelligence Community's assessment, cyber threats, emerging and disruptive technologies, terrorism, weapons of mass destruction and proliferation, space and counterspace, counterintelligence, transnational organized crime, economics and natural resources and human security were listed as the top threats of 2017.

Focus is "Cyber Attacks"

As ITU (International Telecommunication Union) wrote in their 2017 Global Cyber Security Index Report, "global interconnectivity could expose anything and everything to cyber risks and everything from national infrastructure to our basic human rights can be compromised." In that respect, when a quick overview of 2017 took place in terms identifying the threats targeted critical infrastructures, it is possible to claim that in addition to the conventional "physical attacks", most of the emerging literature and media blogs start to focus on the cyber incidents and their severe impacts on critical infrastructures during the last years. Thus, during this brief blog, a quick overview of cyberattacks targeted communication and energy infrastructures will be handled.

Telecom Companies Are Under Threat

The telecom industry has been growing from Alexander Graham Bell's days and by taking their vital importance for the modern society, these infrastructures have been an important target for malicious groups since they are building, controlling and operating the systems are related to "sensitive data". Thus, it is possible to imagine that the impact of any cyberattack could be very high and high-reaching. According to PwC's Global State of Information Security, 2016, IT security incidents in the telecom sector raised 45% in 2015 compared the year before. Also according to the same company's report, only 50% of telecom companies have a security strategy for cloud computing.

How Telecommunications Organizations are Responding to Rising Cyber Risks?

Image Source: PwC

Similarly, according to a study conducted by FICO, it is argued that, in responding cyber threats companies prefer mostly, board level supporting strategies and mechanisms; ongoing monitoring, scoping and reporting and they tested data breach response level. Also, sometimes, a board member could be nominated for oversight of cyber security.

"Cyber Business Strategies" of Telecom Companies

Source: FICO

Likewise, the year of 2017 was not "calm" for telecom industry. According to the security researchers of Kaspersky, the main threats for telecommunication industry can be divided two interrelated categories: direct threats to companies and threats targeting subscribers of telecom

services. In May 2017, more than 45.000 attacks were recorded in 99 countries including Russia, UK, Ukraine, Italy and etc. In Spain, a major telecommunication company – Telefonica- was also infected. Besides the Europe, companies operated MENA Region was also under attack. For instance, it was recorded that Algerie Telecom faced a series of attacks with the aim of hack and disrupt their systems. Nevertheless, despite, the changing nature of the threat environment, it is still argued that Denial of Service Attacks was and will be the biggest issue for the companies operating in Telecom industry.

As it could be imagined, Telecom industry will continue be an attractive target for adversaries. In that regard, a critical question comes to forefront: "What should be done in securing our critical telecom industries, what could be the key recommendations to be suggested? Since the increasing threat appears in cyber space, some related suggestion might be mentioned. First of all, it seems like cyber security in telecom sector requires implementation of a discipline covering advanced technologies and processes, a skillset of counterintelligence techniques and support of top executives. Besides, the companies operating in "cyber defense" field offer a three-fold approach that covers defense, preparation and support. It is recommended that companies shall defend their system operations with the most high-tech cyber protection available, then, they shall prepare by having a cyber security action plan at the ready. Finally, they shall enlist support from relevant industry insight and top-notch threat mitigation tools.

Continuous Risk of the Big "Black Out"

Following the big black out in Ukraine which was triggered by a

well-organized cyberattack, energy sector has started work on "cyber incidents" more seriously and cyber incidents are becoming an alarming issue worldwide. Today cyber incidents are considered to be one of the top threats for industry. The cyberattack wave has been continuing in an uninterrupted nature since the Stuxnet incident. In that respect, in 2017, the industry has witnessed challenging security conditions like the years before.

For instance, in November 2017, it was noted by the British Security Chief that Russian hackers have targeted UK energy networks and telecoms. Additionally, a well-known cyber security company Symantec has reported in September 2017 that, the North American and European Energy Actors were targeted by a new wave of attack by the re-emerging Dragonfly Group. Likewise, an Israel-based cyber security company CyberInt has highlighted a new cyber-attack vector targeting energy industry that is very to identify and detect by protection layers.

In fact, generally the threats associated by energy sector is mostly about theft of information or confidential data, however, today any attack directly target operational systems, ICS (Industrial Control Systems) in energy sector could cause a serious economic damage even loss of human life. Even though there is an argument that "control systems don't connect to internet", project SHINE (SHodan INtelligence Extraction) has already identify more than 2 million control system devices directly connected to internet.

A Holistic and Coordinated Approach

It seems like the efforts in securing cyber space of energy sector is intensifying and becomes a more and more prioritized area for the policy makers and industry's

agenda. There is no doubt that every individual measure would be valuable and beneficial. However, a holistic and coordinated framework from a top-down approach is necessary. In that sense, in order to respond the question "what can be done", the latest document released by European Commission's Energy Expert Cyber Security Platform could be good starting point.

According to the experts of the platform, the first priority should be the installation of threat and risk management system, secondly establishing an effective cyber response framework is highly recommended. Thirdly, it is strongly recommending to the Commission to focus on organizational readiness and improve cyber resilience. Finally, it is suggested that building up the adequate capacity and competences in cyber security for energy sector shall be realized.

Planes, Trains and Automobiles

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

As we near the end of another year, one in which the world has continued to see acts of extreme violence carried out through terrorist activity I hope, as I am sure we all do, to see 2018 as a more peaceful year for everyone.

There is a great deal of good work being done internationally to tackle extremist activity and it is something in which we can all play a part, no matter how small. For those of us who are involved with, or have an interest in, the protection and resilience of Critical National Infrastructure we know that there are exciting new technologies and innovations continually emerging, but we also know there is a lot more to be done.

The International Association of Critical Infrastructure Protection Professionals recognises all the good work that is being done and continues to develop its activities through its strategic objectives which are:

• To develop a wider understanding of the challenges facing both industry and governments

• To facilitate the exchange of appropriate infrastructure & information related information and to maximized networking opportunities

• To promote good practice and innovation

• To facilitate access to experts within the fields of both infrastructure and information protection and resilience

• To create a centre of excellence, promoting close co-operation with key international partners

• To extend our reach globally to develop wider membership that reflects the needs of all member countries and organisations

We have had a very successful year and look towards furthering that success in 2018. We have just concluded hosting a conference in Orlando, which took place at the Kennedy Space Centre and was well supported by US Government Agencies, operators international subject matter experts and academics. This was the second conference hosted this year and we have three planned for 2018, Malaysia in July, Europe in October and the United States in December.

This year we also launched our Global Extranet, where our members can share information with each other, keep up-to-date with the latest threats, best practice, training opportunities, gain access to the World Security Report and our Linkedin Group and much more.

The Association is open critical infrastructure operators, including site managers, security officers, government agencies, government agency officials and policy makers only and now has Regional Directors in place in North America, Australasia, Southern Europe, Eastern Europe and Caspian & MENA.

If you would like any further information about the IACIPP then please contact one of the Regional Directors or to register for application online just go to www.iacipp.net

I look forward to more of you joining us and contributing to the activities we are seeking to develop in playing our part towards the protection and resilience of our Critical National Infrastructure as we move into a New Year.

In the meantime, may I wish you and your families a very Merry Christmas and a happy, peaceful and healthy New Year.

The IACIPP Poll

Give your opinion

Where do you see cybersecurity certification of Operational Technology's (ICS / Scada) components fit best?

1. Defense
2. Nuclear
3. Energy
4. Transport
5. Telecomms
6. All of them
7. None of them

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

CyberSecurity Predictions for 2018 - Threats via social media and Wireless networks will dominate next year

Researchers at Airbus' external Cyber Security business have compiled their top technology predictions for 2018, based on trends identified at its Security Operations Centres in France, UK and Germany during 2017.

Prediction 1: A lack of social media security policies will create serious risks for enterprises

As observed during 2017, social media platforms are regularly being used for the spread of fake news or the manipulation of public opinion. But social media can also be used for sophisticated social engineering and reconnaissance activities which form the basis of many attacks on the enterprise. Criminals and hackers are known to use these platforms to distribute malware, push rogue antivirus scams and phishing campaigns to lure their victims.

Markus Braendle, Head of the Airbus CyberSecurity business: "Social media provide the medium for connecting people globally, in the rapid exchange of ideas, discussions and debates in our digital world. However, from an attacker's perspective, social media have become an easy target because of the number of non-cyber security savvy users, and the fact that these platforms are easy and cost effective to use. To protect themselves against social media attacks, organisations need to implement enterprise-wide social media security policies. This includes designing training programs for employees about social media

usage, and creating incident response plans that coordinate the activities of the legal, HR, marketing and IT departments in the event of a security breach."

Prediction 2: Attacks on Wireless networks will escalate

Attacks on Wireless networks will increase as attackers seek to exploit the Key Reinstallation Attack (KRACK) vulnerability, first made public in October 2017.

The vulnerability can allow an attacker to intercept and read Wi-Fi traffic between devices and a WiFi router,

and in some cases even modify the traffic to inject malicious data into websites. It could also allow attackers to obtain sensitive information from those devices, such as credit card details, passwords, chat messages and emails.

Braendle continues: "We can expect to see an escalation of attacks over public or open WiFi connections, and in turn, an increased security provision by organisations that offer such services to their customers. Such attacks may be particularly damaging for people using old devices that are no longer supported by vendors, making them an attractive target for cyber criminals. These threats may also trigger an increased use of Virtual Private Networks (VPN) by the most security conscious users."

Prediction 3: Encryption will continue to represent challenges for law enforcement

Concerns about data privacy, the increasing use of cloud computing, an increase in data breaches and the introduction of General Data Protection Regulation (GDPR) will all contribute to the emergence of End to End Encryption (E2EE) as the most effective way for enterprises wishing to secure their data. But E2EE will also represent some challenges to law enforcement as criminals continue to use this technique for espionage and subversion.

Braendle continues: "When weighing up the cost of any security solution, it's important to consider the financial impact of suffering a security incident. After General Data Protection Regulation (GDPR) comes into effect, organisations could be fined up to 4% of their global turnover in the event of a data breach – so the cost of any solution must always be viewed in relation to the risks involved."

Navigating the Cyber Sea of Compliance

Researchers at Airbus' external Cyber Security business have compiled their top technology predictions for 2018, based on trends identified at its Security Operations Centres in France, UK and Germany during 2017.

General Data Protection Regulation (GDPR - https://www.eugdpr.org/eugdpr.org.html): Data protection law framework across the European Union (EU) focuses on protecting its citizen's data and privacy. The European Union imposes strict rules on those hosting and 'processing' this data, anywhere in the world via stringent fines.

Federal IT Acquisition Reform Act (FITARA - https://management.cio.gov/): U.S. legislation that puts federal agency CIOs in control of IT investments. Requires U.S. federal agencies to provide the Office of Management and Budget (OMB) with a comprehensive inventory of data centers and a strategy to consolidate and optimize their data. Also provides periodic "scorecards" to federal agencies on compliance across multiple assessment categories.

NIST Special Publication 800-171 - https://www.nist.gov/publications/protecting-controlled-unclassified-information-nonfederal-information-systems-and-0?pub_id=918804: Set of security requirements that may be added or referenced in federal contracts with the goal of improving the protection of Controlled Unclassified Information (CUI). Contractors and sub-contractors required to be compliant by Dec 31, 2017. Government attempt to transfer risk and bring contractors up to a common cyber security standard.

What do all of these diverse regulations have in common? They are a sampling of the growing list of cyber security requirements that the government and segments of the commercial industry must be both cognizant of and in compliance with. Many companies are only starting to become aware of the existence of these regulations and determining the impact that these requirements will have on their organizations. Beginning May 25, 2018, the EU GDPR will impose heavy fines on those companies violating the rules. These fines can be a percentage of the company's revenue. As with any new regulations, many organizations are unaware of their existence and impact; particularly smaller companies currently or planning to do business in

the European Union.

For organizations, the bottom line concern is liability. Much like personal injury law, it is not enough to simply put up a warning sign on an icy sidewalk. We all understand that if a pedestrian were to slip and fall on an owner's icy sidewalk, the owner is still liable. Owners must take active steps to achieve compliance, mitigate risks inherent to their products and infrastructure, and institute a viable cyber security program that is sustainable for the long haul. This means they must put in place a program that brings together a team of skilled people, utilizes a proven process and includes the right tools to extract decisive information. The ROI to be measured is the organization's preparedness and protection from fines and liability.

Fortunately, most of the regulatory requirements can be met by basic compliance with existing standards such as those provided by NIST. Almost all new guidance has some common denominators in existing controls and guidelines. Integrating a proactive cyber security program that both complies with regulations affecting your organization and also provides protection from legal issues is becoming imperative to any organization. Such a program isn't a "nice to have", but a must have. While the Cyber Sea is no doubt treacherous with volatile waters, our lighthouse with bright cyber experts are certified to help you navigate the path to get your organization safely to shore.

To learn more about "Defending Critical Infrastructure" download our eBook here: https://get.criticalinfrastructuredefense.com/iiot_ebook/

Author: Kevin Koppenhaver, Director of Cyber Security Solutions

Navigating The Cyber Sea of Compliance

Belcan

critical infrastructure
PROTECTION & RESILIENCE ASIA
Including Critical Information Infrastructure Protection

17th-19th July 2018
Sarawak, Malaysia
leading the debate on securing ASEAN's critical infrastructure

critical infrastructure
PROTECTION & RESILIENCE ASIA

Co-Hosted By:

CyberSecurity
MALAYSIA
An agency under MOSTI

17th-19th July 2018
Sarawak, Malaysia
www.cip-asia.com

Developing resilient infrastructure for a secure future

Call for Papers

Are you interested at speaking at the Critical Infrastructure Protection and Resilience Asia conference?

The Critical Infrastructure Protection and Resilience Asia Advisory Committee are inviting abstracts for consideration for inclusion in the conference.

If you are interested, you are invited to submit your abstract for consideration by the conference committee by submitting an abstract of approx 200 words. Your presentation should not be overtly commercial in nature.

For further details, guidelines and to submit your abstract online visit www.cip-asia.com.com

The 3rd Critical Infrastructure Protection and Resilience Asia brings together leading stakeholders from industry, operators, agencies and governments to debate and collaborate on securing South East Asia's critical infrastructure.

Gain access to leading decision makers from corporate and government establishments tasked with Critical Infrastructure Protection and Resilience.

Owned & Organised by:

TORCH

Media Partners:

World Security-index.com

WORLD SECURITY REPORT

Supporting Organisations:

NS&RC

ASSOCIATION OF RISK AND CRISIS COMMUNICATION

How to Exhibit

Gain access to a key and influential audience with your participation in the limited exhibiting and sponsorship opportunities available at the conference exhibition.

To discuss exhibiting and sponsorship opportunities and your involvement with Critical Infrastructure Protection & Resilience Asia please contact:

Suthi Chatterjee
Exhibit Sales Manager (Asia)
PRMC Thailand
Tel: +66 2 247-6533; Fax: +66 2 247-7868
Mobile: +66 (0) 87-060-5960
E: suthi@prmcthailand.com

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

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

Marc Soeteman
(Benelux & Germany)
E: marcs@torchmarketing.co.uk
T: +31 (0) 6 1609 2153

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

Protecting critical utility infrastructure

With an interconnected grid of over 450,000 miles of high voltage transmission lines, 55,000 transmission substations (>100 kV), and over 7,000 generating plants, the targets of opportunity are endless for the North American electric grid. In addition, this infrastructure is widely dispersed across North America, and in most instances, is in unpopulated and isolated locations, making it cost prohibitive and logistically difficult to physically protect all assets.

Given the limited physical protections provided to some generation, transmission, and distribution assets, it will come as no surprise that these assets are soft targets for would-be criminals or terrorists. With new attentiveness due to high profile events such as the Metcalf substation and Ukraine cyber-attack, utilities are working feverishly to implement added protections and maintain a proper Critical Infrastructure Protection (CIP) compliance program. After all, Americans have a low tolerance for grid failure and a high expectation that system operators will provide an uninterrupted supply of energy for vital services.

Critical infrastructure protection is a cyclical process of prevention, detection, mitigation, response and recovery. For system operators, the key to this protection is the identification of credible threats and the assessment of risks and potential vulnerabilities (weaknesses) at their facilities. Once a threat has been thoroughly analyzed, preventative measures to deter, detect, and delay an attack can be implemented. Of course, critical infrastructure protection planning must also include mitigation, response and recovery actions in the event an attacker is successful.

Within North America, the National Strategy for Critical Infrastructure (Canada) and the National Infrastructure Protection Plan (United States) have established a collaborative approach that is used to strengthen critical

infrastructure resiliency. These strategies recognize that each level of government, as well as infrastructure owners and operators, has a major role and responsibility in strengthening the resilience of critical infrastructure according to its respective jurisdiction. While the security of the grid is a shared responsibility between the government and the private sector, the primary responsibility rests with utility owners and operators. Utility security staff must ensure they are able to receive and act upon criminal intelligence and be prepared to identify risks and vulnerabilities associated with security threats.

Significant progress has been made in the electricity industry surrounding the issue of security. However, many do not realize the resources such as reports, guidelines, standards, and assessments that have been developed to support and enhance security programs across the country. The North American Electric Reliability Corporation (NERC) continues to enforce mandatory reliability standards while also providing educational opportunities for industry participants. A major part of this education is focused on grid resilience with an emphasis on security.

NERC and the industry have gone through multiple iterations of mandatory CIP Standards that focus on security protections. These reliability standards are the only mandatory cyber standards enforced on critical

infrastructure owners and operators. Given the political pressure to regulate critical systems, it is important for NERC and the industry to showcase these standards and demonstrate how the system is more secure because the CIP Standards, while not perfect, may be a shining example for other sectors to replicate.

In addition to expanding awareness around CIP standards and NERC resources, it is also important to discuss the distinction between compliance and security, which is an often misunderstood cybersecurity issue that surfaces again and again in critical infrastructure settings, regardless of which regulatory program we discuss. Compliance is a regulatory minimum that one must achieve, it could even be seen as a tool, but it is not a cybersecurity strategy. Boards of Directors should recognize that compliance is the minimum and that the minimum may not keep a company and its resources secure. Risk mitigation through security controls and countermeasures should be implemented on top of compliance measures to drive risk down to acceptable levels. To tackle increasing data threats, companies need to put cybersecurity at the very heart of the business. In the modern age, information security should be woven into the fiduciary, oversight and risk management purview of the board.

Since December of 2015, electric utilities in the United States and Canada have been wrestling with the postmortem reports and data findings from two significant grid hacking events in Ukraine. The subject of these attacks have been addressed by those on Capitol Hill, trade associations, regulators, and the E-ISAC. The hackers who struck utilities in Ukraine, which is the first confirmed hack to degrade a power grid, were not opportunists who stumbled across the networks and launched an attack to test their abilities. The attackers were highly skilled and planned their assault over many months by first doing reconnaissance to study

the networks and steal operator credentials, and then launching a synchronized attack against operating systems. While the U.S. has never experienced a massive cyber-attack related power outage, there have been direct cyber events in recent years against energy infrastructure, including intrusions into energy management systems, targeted malware and advanced persistent threats (APTs) left behind on computers by phishing attacks. The perception that cyber risks are low because only a few limited attacks have occurred on industrial control systems is not just ignorant, but highly dangerous.

It is important to note that electricity is only one of the 16 critical sectors identified by the Department of Homeland Security, and the interdependencies between these sectors play a significant role in responding to a major coordinated attack. For example, the electric and gas industries are becoming more "co-dependent" because the electric industry is increasingly reliant on gas-fired generation and its associated infrastructure, and most gas infrastructure is dependent on electricity to operate. As a result, failure in either sector now has potential reliability impacts or cascading effects on the other. As more gas-fired generation is added to the grid, the electric industry faces increased risk associated with common mode failure, which

occurs when multiple failures are caused by a single fault. To the extent that multiple gas-fired generators are dependent upon a single gas pipeline, several generating facilities may go down if that pipeline fails or has insufficient capacity. These interdependencies can also be found between the energy and water sectors, as well as the energy and communication sectors because communication equipment is often coupled with electric equipment across the grid.

Given these sector interdependencies and growing concern around cyber threats and attacks around the world, we must assume that at some point in the future a North American utility will suffer from a planned and coordinated attack against electrical infrastructure. As an industry, we will be judged and hard questions will be asked about how seriously we considered these threats and what we did to mitigate future attacks. Success will be determined by how quickly we are able to respond and the swiftness of system recovery. There is no doubt that security requires an "all hands" approach by everyone involved.

Brian Harrell, CPP is the Vice President of Security at AlertEnterprise, a technology and advisory firm that provides critical infrastructure owners with consultation on physical and cybersecurity protections.

S&T's Dam Simulation Program Saves Lives and Saves Taxpayers Nearly $50M

Have you ever wondered what happens when a dam fails? How fast and how far would all the water, which was being held back, reach? How long would it take to stop and just how deep would the flooding be? And, most importantly, how much damage would it cause to properties, infrastructures and the environment downstream from the dam? Not to mention the toll on human life.

With more than 96,000 dams across the United States, those are the kind of questions dam safety engineers in state and government agencies and emergency managers must answer in order to prevent loss of life and to protect properties and critical infrastructures in case of a dam failure. Almost 10 years ago, the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) waded into the discussion; developing a modelling and simulation tool to help provide better answers to those questions. To date, that tool – the Simulation-Based Decision Support System for Water Infrastructural Safety or - DSS-WISETM has modelled more than 1,800 dams so far, saving the American taxpayer nearly $50,000,000.

DSS-WISETM was developed to support the DHS Office of Infrastructure Protection, Dams Sector Section and the Federal Emergency Management Agency (FEMA). S&T funded the free flood simulation software, which quickly calculates the spread of flood water in case of dam or levee breaches.

S&T has recently released a newer version called DSS-WISETM Lite that allows for more complicated simulations. S&T funded the National Center for Computational Hydroscience and Engineering (NCCHE) at the University of Mississippi to develop the DSS-WISE™, which combined a state-of-the-art numerical model for two-dimensional flood simulation with decision support tools to map the flood and evaluate its consequences.

In 2011, NCCHE began to develop DSS-WISE™ Lite – a web-based version of this software with automated input data preparation. This web-based, automated dam-break flood modelling and mapping capability became available in 2012. In 2015, DHS Office of Infrastructure Protection, Dams Sector Section, and the Federal Emergency Management Agency (FEMA) decided to support NCCHE to create a standalone, improved version of DSS-WISE™ Lite.

"This is a dam-break flood modelling project S&T funded with a total investment of $1.6 million and a return on investment (so far) of $50 million, as well as countless lives and personal property saved," said Mike Matthews, program manager for the S&T Research Development Partnerships' Office

of National Laboratories. "This number means that states, counties and local municipalities did not have to pay for this tool or service."

While dam failure is normally a rare event, the extreme rainfall and exceptional floods driven by hurricanes led to a large number of dam failures over the last two years. In 2015, Hurricane Joaquin caused the failure of 51 regulated dams in South Carolina. In 2016, Hurricane Matthew caused 25 dam failures in South Carolina and 17 dam failures in North Carolina.

Around 16,000 dams in the U.S. are classified as high hazard dams whose failure could result in loss of life, significant property damage, lifeline disruption and environmental damage. These dams are required to have Emergency Action Plans, which is a formal document that identifies potential emergency conditions at a dam and specifies preplanned actions to be followed to minimize loss of life and property damage. An engineering study of a dam takes days to complete and could cost $32,500. DSS-WISE™ takes minutes and is free.

"In order to have an emergency action plan for a dam, you have to be able to model it," explained Matthews. "You have to be able to know if there is a breach in a dam, what happens downstream, what communities, businesses and infrastructures are impacted."

This is where the DSS-WISE™ Lite software comes into play. "The users can set up and launch a two-dimensional dam-break simulation in about five minutes," said Dr. Mustafa Altinakar, director and research professor at NCCHE. "The input data for the model is prepared automatically, and in 73 percent of the cases, the simulation results' GIS-compatible format are returned to the user within half an hour. It is the fastest model

available," he added.

The exceptional computational speed of DSS-WISE™ Lite makes it an ideal tool for operational modelling during dam safety emergencies. Dam safety engineers and emergency managers from state dam safety offices, FEMA and other agencies have used DSS-WISE™ Lite during numerous emergencies to run operational simulations that were used to prepare emergency response plans in a very short time. While it was still being beta tested in October 2016, the system was used for emergency dam-break simulations in South Carolina. More recently, in February 2017, dam safety engineers in California performed 60 simulations to test different spillway release scenarios during the Oroville Dam incident.

Already, 35 states and various federal agencies are using the DSS-WISE™ Lite capability free of charge. Since its release in November 8, 2016 through the end of November, 2017, the system handled 3,115 dam-break flood simulations for 876 dams. On average, around 22 simulations are added daily.

User groups have been set up for FEMA headquarters, 10 FEMA regions and the states under

their coverage, national Weather service and Argonne National Laboratory. Each group is assigned their geographic area for their simulations. The groups are self-managed by a group manager. Local dams safety or emergency officers who want to use the system must register online apply to their corresponding geographical group.

A few weeks ago, Altinakar's team took down the DSS-WISE™ Lite system for five days to implement major upgrades and improvements. "I was flooded with messages asking 'When is this going to be back again because our program heavily relies of DSS-WISE Lite!' People were impatient to use the capability," said Altinakar.

"The big success story here is the number of years DSS-WISE™ has been going on, and it is not just the money that have been saved, but it is also the lives that have been potentially saved and the improved planning for emergency managers in these communities," said Matthews. "The good part for me as a program manager is to know that technology we developed 10 years ago continues to be used and is paying large dividends, which means that the project was sorely needed."

New powers for police to address illegal and unsafe use of drones

Police are set to be given powers to prevent the unsafe or criminal use of drones as part of a new package of legislation.

The measures are intended to allow drone users to continue flying safely and legally, helping to place the UK at the forefront of the fast-growing drone industry. This will also pave the way for the devices to be harnessed for a range of uses by businesses and public services.

The draft Drone Bill, which will be published next spring, will give officers the right to order operators to ground drones where necessary. Officers will also be able to seize drone parts to prove it has been used to commit an offence.

New measures will also make it mandatory for drone owners to register to improve accountability. And drone operators will be required to use apps – so they can access the information needed to make sure any planned flight can be made safely and legally.

Banning all drones from flying above 400 feet or near airports could also form part of the new regulations.

The news comes as funding for a pioneering new drones programme is announced to help cities shape the way this new technology operates and the benefits it brings.

Aviation Minister Baroness Sugg said:

Drones have great potential and we want to do everything possible to harness the benefits of this technology as it develops.

But if we are to realise the full potential of this incredibly exciting technology, we have to take steps to stop illegal use of these devices and address safety and privacy concerns.

These new laws strike a balance, to allow the vast majority of drone users to continue flying safely and responsibly, while also paving the way for drone technology to revolutionise businesses and public services.

The government will publish the draft Drone Bill for consultation and introduce secondary legislation amendments in spring 2018. Changes to the Air Navigation Order will mean that that mean: drone users will have to sit safety awareness tests users of drones weighing 250 grams and over will in future have to be registered

The government is also working closely with drone manufacturers to use geo-fencing to prevent drones from entering restricted zones.

The Flying High Challenge, funded by the government and run by Nesta in partnership with Innovate UK, launched on 27 November when cities will be invited to register their interest.

Up to 5 cities will be supported in the research and development of drone technology which could transform critical services in – for example, emergency health services and organ transport, essential infrastructure assessment and repair, and parcel delivery and logistics.

National Police Chiefs' Council Lead for Criminal Misuse of Drones, Assistant Chief Constable Serena Kennedy said:

Police forces are aware of the ever increasing use of drones by members of the public and we are working with all relevant partners to understand the threats that this new technology can pose when used irresponsibly or illegally. Do not take this lightly – if you use a drone to invade people's privacy or engage in disruptive behaviour, you could face serious criminal charges.

Police officers will use all available powers to investigate reports of criminal misuse of drones and seek the appropriate penalty. Make sure you know the rules for using a drone because it is always your responsibility to ensure that you are acting within the law and in line with the Civil Aviation Authority's Drone Code.

Tim Johnson, Policy Director at the CAA said:

The Civil Aviation Authority (CAA) supports the safe development of drones in the UK. Drones can bring economic and workplace safety benefits but to achieve those we need everyone flying a drone now to do so safely. We welcome plans to increase drone operator training, safety awareness and the creation of no-fly zones.

We have been working with Government and the aviation and drone industries to educate drone operators by successfully promoting the Dronecode , which provides an easy to follow guide to UK drone rules.

Andromeda BotNet Dismantled in International Cyber Operation

The Federal Bureau of Investigation (FBI), in close cooperation with the Luneburg Central Criminal Investigation Inspectorate in Germany, Europol's European Cybercrime Centre (EC3), the Joint Cybercrime Action Task Force (J-CAT), Eurojust and private-sector partners, dismantled one of the longest running malware families in existence called Andromeda (also known as Gamarue).

This widely distributed malware created a network of infected computers called the Andromeda botnet[1]. According to Microsoft, Andromeda's main goal was to distribute other malware families. Andromeda was associated with 80 malware families and, in the last six months, it was detected on or blocked an average of over 1 million machines every month. Andromeda was also used in the infamous Avalanche network, which was dismantled in a huge international cyber operation in 2016.

Steven Wilson, the Head of Europol's European Cybercrime Centre: "This is another example of

international law enforcement working together with industry partners to tackle the most significant cyber criminals and the dedicated infrastructure they use to distribute malware on a global scale. The clear message is that public-private partnerships can impact these criminals and make the internet safer for all of us."

One year ago, on 30 November 2016, after more than four years of investigation, the Public Prosecutor's Office Verden and the Luneburg Police in Germany, the United States Attorney's Office for the Western District of Pennsylvania, the Department of Justice, the FBI, Europol, Eurojust and global partners, had dismantled the international criminal infrastructure Avalanche. This was used as a delivery platform to launch and manage mass global malware attacks such as Andromeda, and money mule recruitment campaigns.

Insights gained during the

Avalanche case by the investigating German law enforcement entities were shared, via Europol, with the FBI and supported this year's investigations to dismantle the Andromeda malware last week.

Jointly, the international partners took action against servers and domains, which were used to spread the Andromeda malware. Overall, 1500 domains of the malicious software were subject to sinkholing[2]. According to Microsoft, during 48 hours of sinkholing, approximately 2 million unique Andromeda victim IP addresses from 223 countries were captured. The involved law enforcement authorities also executed the search and arrest of a suspect in Belarus.

Simultaneously, the German sinkhole measures of the Avalanche case have been extended by another year. An extension of this measure was necessary, as globally 55 per cent of the computer systems originally infected in

Avalanche are still infected today.

The measures to combat the malicious Andromeda software as well as the extension of the Avalanche measures involved the following EU Member States: Austria, Belgium, Finland, France, Italy, the Netherlands, Poland, Spain, the United Kingdom, and the following non-EU Member States: Australia, Belarus, Canada, Montenegro, Singapore and Taiwan.

The operation was supported by the following private and institutional partners: Shadowserver Foundation, Microsoft, Registrar of Last Resort, Internet Corporation for Assigned Names and Numbers (ICANN) and associated domain registries, Fraunhofer Institute for Communication, Information Processing and Ergonomics (FKIE), and the German Federal Office for Information Security (BSI).

The operation was coordinated from the command post hosted at Europol's HQ.

Five Arrested for Spreading Ransomware Throughout Europe and US

During the last week, Romanian authorities have arrested three individuals who are suspected of infecting computer systems by spreading the CTB-Locker (Curve-Tor-Bitcoin Locker) malware - a form of file-encrypting ransomware. Two other suspects from the same criminal group were arrested in Bucharest

in a parallel ransomware investigation linked to the US.

During this law enforcement operation called "Bakovia", six houses were searched in Romania as a result of a joint investigation carried out by the Romanian Police (Service for Combating Cybercrime), the Romanian and Dutch public prosecutor's office,

the Dutch National Police (NHTCU), the UK's National Crime Agency, the US FBI with the support of Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT).

As a result of the searches in Romania, investigators seized a significant amount of hard drives, laptops,

external storage devices, cryptocurrency mining devices and numerous documents. The criminal group is being prosecuted for unauthorised computer access, serious hindering of a computer system, misuse of devices with the intent of committing cybercrimes and blackmail.

OSCE organizes seminar on relief mechanisms for natural disasters and emergencies in Turkmenistan

Effective mechanisms for responding to natural disasters and emergencies were the focus of a seminar organized by the OSCE for members of the State Commission for Emergency Situations of Turkmenistan and representatives of other relevant bodies held in Ashgabat in December 2017.

The two-day event focused on preventative and preparatory measures within disaster response procedures and aimed to facilitate the exchange of best practices in ensuring community safety in the event of an emergency situation.

"The 2014 Basel OSCE Ministerial Council Decision on Disaster Risk Reduction acknowledged the linkages between disasters and security and emphasized that co-operation on disaster risk reduction can contribute to confidence building and good neighborly relations," said Natalya Drozd, Head of the OSCE Centre in Ashgabat. "The OSCE initiated numerous projects aimed at promoting community-based disaster risk reduction and strengthening national and regional capacities to manage natural disasters and emergencies. Today's event marks the successful continuation of the activities of the OSCE Centre in Ashgabat in this area."

During the event, an international expert elaborated on disaster relief mechanisms for natural disasters and emergencies and crisis management procedures. Special attention was paid to different ways of receiving international crisis support and the importance of conducting regular crisis training.

Building a security framework for major events focus of global experts

Shaping a whole-of-society approach to enhance safety and security at major events has been the focus of international experts at a meeting in Doha.

With such events facing criminal activities ranging from disorder and violence to cyberattacks and terrorism, more than 350 participants representing law enforcement, academia, the private sector and international organizations sought to build on a global network of sports safety and security expertise established under Project Stadia.

Launched by INTERPOL in 2012 and funded by Qatar, the 10-year project aims to create a Centre of Excellence to help INTERPOL's 192 member countries undertake policing and security preparations for major sporting events. It will contribute to policing and security arrangements for the 2022 FIFA World Cup in Qatar.

Project Stadia and Qatar's Supreme Committee for Delivery and Legacy co-hosted the 1st Major Event Safety and Security Conference (7 and 8 November), in collaboration with Qatar's Ministry of Interior.

The meeting notably saw the launch of a state-of-the-art knowledge management system by Qatar's Prime Minister and Interior Minister, Abdullah bin Nasser bin Khalifa Al Thani.

It will help support capacity development activities and major event policing operations by providing countries hosting major events with unique knowledge content, and facilitate secure information exchange in real time on emerging incidents and emergencies.

The knowledge management system consolidates the learning accumulated since Project Stadia was established in 2012 through legislation, physical security and cybersecurity expert meetings, as well as training courses held with partners which include NCS4 (University of Southern Mississippi's National Center for Spectator Sports Safety and Security).

At the meeting INTERPOL Secretary General Jürgen Stock said Project Stadia underlines the role of INTERPOL in fostering collaboration across all sectors, acting as an 'early global warning system' and providing stakeholders worldwide with 'a ready network of specialists for securing major events' in the face of growing transnational threats.

Sikorsky has delivered two S-70i™ Black Hawk helicopters to the County of Los Angeles at a ceremony in Coatesville, Pennsylvania

The S-70i Black Hawk helicopters will be customized to a Firehawk™ configuration to meet L.A. County Fire Department's specifications and further protect lives and property 24/7.

A Firehawk helicopter performs aerial firefighting and additionally, can plan missions and direct other firefighting aircraft, and provide emergency medical service transport, search and rescue, and logistic support. Once modified by a specialist outfitter in 2018 with a 1,000-gallon (3,785-liter) water tank, extended landing

gear, single pilot cockpit layout and a medically-equipped interior, the new aircraft will increase to five the L.A. County Fire Department's

fleet of Firehawk multi-role helicopters.

Compared to LA County's three existing S-70A

model Firehawk aircraft, the S-70i variant includes wide chord rotor blades for increased payload and maneuverability, enhanced engine power, a stronger airframe, a digital cockpit with flight management system for enhanced situation awareness, and an Integrated Vehicle Health Management System to monitor the aircraft's operational health. Among improved safety features, the S-70i aircraft includes a terrain and obstacle avoidance system that alerts aircrew to the proximity of potential hazards on the ground.

FLIR Systems Introduces FB-Series ID Thermal Fixed Bullet Camera with Built-In Human and Vehicle Recognition Analytics

FLIR Systems has introduced the FB-Series ID, the latest fixed bullet thermal security camera in the FB-Series family. Combining best-in-class thermal image detail and high-performance onboard analytics, the FB-Series ID is ideal for narrow to wide area perimeter detection and sterile-zone monitoring.

The FB-Series ID features accurate video analytics that are capable of classifying human or vehicular intrusions. Combined with FLIR's custom Automatic Gain Control (AGC) and Digital Detail Enhancement (DDE), the FB-Series ID provides unmatched image contrast and sharpness, which improves analytic performance, resulting in

fewer false alarms.

The FB-Series ID is certified for integration with major third-party video management systems (VMS), as well as FLIR's United VMS. Outfitted to act as a standalone security system, the FB-

Series-ID can also handoff classified intrusions to FLIR pan-tilt-zoom cameras for autonomous tracking of intruders. Featuring FLIR's superior 320x240 resolution thermal imaging sensor, the FB-Series ID can detect potential intruders in total darkness, and through sun

glare, smoke, dust, and light fog. Five lens options – 93, 49, 24, 12 and 9-degree field of views – offer wide to narrow coverage and reduce the number of cameras needed to monitor fence lines, perimeters, and open areas.

"As the first FB-Series camera with built-in analytics, the FB-Series ID provides an all-in-one intrusion detection system that classifies human or vehicular intrusions with low false alarm rates," said John Distelzweig, Vice President and General Manager of FLIR's Security segment. "The FB-Series ID solidifies FLIRs initiative to expand artificial intelligence and bring thermal imaging to more customers."

Counter Surveillance Equipment helping to prevent fraud at Exam Testing Sites

The newly-launched ANDRE Advanced Near-field Detection Receiver from Research Electronics International (REI) is helping prevent fraud at exam testing sites.

Commonly used for counter surveillance operations and intelligence protection, the ANDRE is now also helping educators prevent cheating during examinations by detecting covert electronic transmissions.

According to Brazilian news reports, eleven individuals were arrested last year for using electronic devices during the high-profile National High School Examination- Exame Nacional do Ensino Médio (Enem). This year,(2017) the Ministry of Education has a new security feature; the ANDRE Advanced Near-field Detection Receiver can detect the emission of radiofrequency signals from WiFi, Bluetooth, cell phones and illegal broadcasts. ANDRE detects radio frequency transmissions,

regardless of whether they are unknown, illegal, disruptive or interference, to locate and identify participants who attempt to use electronic devices during the exam and may have circumvented inspection by metal detectors. The adoption of this new technology reinforces the security strategy of Enem, which already uses metal detectors for the surveillance and identification of electronic devices.

The Brazilian Minister of Education is quoted as

saying "Our goal is to combat the electronic points that, unfortunately, are still used in high-profile exams such as ENEM." According to the Brazilian Federal Police, more investing is being done to repress fraud, stating that "there are now almost imperceptible electronic points. As organized crime increases, we will also introduce new security solutions."

The ANDRE is a hand-held broadband receiver that detects and assists in locating nearby RF and other types of

transmitters, including mobile phones. Antenna probes included with the ANDRE can be used to search for known, unknown, illegal, disruptive, or interfering electronic transmitters. Hidden electronic devices are easily concealed in a variety of objects and access to eavesdropping and electronic bugging devices is becoming easier and more affordable. The ANDRE provides mobile RF search capability to help locate these hidden transmitters quickly and discretely.

Mr Gerry Hall, Managing Director of International Procurement Services, distributors of ANDRE said, "As organised crime increases and technology advances at an alarming rate, we find that we are facing new challenges on an almost daily basis. Exam fraud is a growing problem the world over, and as International Distributors of REI we are always ready to offer advice, support and training to counteract these increases in exam fraud."

OGSystems' Awarded MOJAVE Security Support Services Contract

OGSystems (OGS) has been awarded the MOJAVE Functional Area 2 (FA2): Security Support Services contract by the National Geospatial-Intelligence Agency (NGA).

"We have invested heavily in data analytics, visualization, and system integration across the personnel, counterintelligence and

insider threat missions," said Garrett Pagon, OGSystems President and co-founder. "This award reflects both our ongoing customer impact and our ability to innovate in security services, and we are excited to be working with NGA in this capacity."

OGS was one of five prime contractors to receive this Indefinite Delivery/

Indefinite Quantity (ID/IQ) contract with a five-year base ordering period and an estimated ceiling of $400 million. The MOJAVE FA2 contract provides a variety of security operations support including polygraph support, security specialist support, clinical psychology, counterintelligence

support and insider threat analysis to assist NGA in executing its mission to the fullest

OGS develops and implements innovative value-added security services solutions to help NGA adapt to rapid changes in the threat and technology environments.

Navigating the Cyber Sea of Compliance

FLIR Introduces Quasar™ 4x2K Panoramic Security Camera with Four High-Definition Sensors

FLIR Systems has introduced the Quasar 4x2K panoramic camera featuring four, full-high-definition visible sensors. The latest security camera in the FLIR Quasar family, the 4x2K produces 4K resolution for highly detailed scenes. The mini-dome camera offers wide area surveillance to monitor cities, critical infrastructure, and other high-profile security areas.

Offering interchangeable field-of-view options of 180- and 360-degrees, the

Quasar 4x2K can replace multiple individual cameras, allowing security operators to reduce the number of security cameras required for monitoring wide areas. With automatic stitching that combines the four sensors into a 180-degree view, the camera generates a highly detailed, seamless image that eliminates blind spots and scene duplication. Built-in infrared illumination automatically adjusts to the 180- or 360-degree viewing mode and monitors without the need to illuminate the scene.

The Quasar 4x2K integrates with FLIR's video management systems (VMS) and major third-party VMS. Using a one-step configuration process that guarantees quick and efficient mounting, the Quasar 4x2K easily adjusts to either 180- or 360-degree viewing mode in the field. With an IP67 environmentally-rated dome enclosure to withstand mist, rain, and accidental submersion, the Quasar 4x2K provides 24/7 video surveillance either in- or outdoors.

MARSS to Install Long-Range Security and Climber Detection Systems to Protect Merchant Vessels

MARSS has secured a refit contract for the installation of their automated security systems NiDAR and CLIMBERguard onboard merchant vessels.

This project will integrate security radar and daylight/infrared cameras, as well as climber detection capability to deliver layered 360° surveillance for the monitoring, detection and tracking of surface objects in the vicinity of a vessel.

The NiDAR system developed by MARSS is providing all-round air, surface and underwater perimeter security to protect high value maritime assets.

Operating autonomously and discreetly 24/7, NiDAR tracks both known and unknown objects around a vessel, while smart software algorithms automatically analyse and rank threats, triggering alerts to notify users as required.

Climber detection is achieved with the self-contained CLIMBERguard units that combine micro-radars, imaging sensors and processing to automatically detect, classify and track approaches close to and scaling the vessel sides.

Multi-touch command and control interfaces present a clear situational awareness picture to crew as a fixed installation onboard or remotely via smart mobile devices aiding decision-making and rapid response.

"We are delighted to have been awarded this contract that demonstrates the flexibility of MARSS systems to meet client requirements and deliver increased long-range security capability to vessels." Johannes Pinl, CEO & Founder.

Fortinet Protects Operational Technology Deployed in the Harshest Environments

Fortinet has announced the availability of its Operational Technology (OT) Security solution for critical infrastructure and industrial organizations. The new solution integrates ruggedized firewall, switching, and wireless access point appliances with FortiGuard industrial threat intelligence to provide integrated cybersecurity protections for industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems deployed in the field and non-environmentally controlled facilities across an organization's OT infrastructure.

Critical infrastructure is being increasingly targeted by cyber criminals, with a reported 51% of organizations experiencing a SCADA/ICS security breach within the past 12 months. The consequences of a successful attack can lead to the disruption, and even destruction of physical assets and essential services like water, electricity, and fuel.

As the utility, oil and gas, transportation, and manufacturing sectors increasingly adopt connected control systems and Industrial IoT devices, the attack surface is rapidly growing. The connected nature of these devices and systems poses serious challenges as they begin to utilize traditionally IT owned network infrastructure, wireless access points, and mobile networks. The specialized nature of OT infrastructure technologies means that most security and threat intelligence solutions don't have visibility into, let alone the ability to defend against attacks on critical infrastructures.

According to a 2014 Forrester report, "There are fundamental differences between traditional information technology (IT) and operational technology (OT)…S&R (security and risk) pros from IT and OT must respect and accept each other's differences and learn to work together."

Fortinet's Operational Technology Security solution solves the unique security challenges specific to critical infrastructure and industrial organizations, while unifying the management and administration of both OT and traditional IT infrastructures through the Fortinet Security Fabric.

Fortinet's rugged and outdoor products are industrially-hardened appliances that deliver enterprise-class connectivity and security for critical control systems facing malicious attacks, as well as extreme weather and other demanding physical environments. They are:

FortiGate Rugged Series are all-in-one firewalls that deliver specialized threat protection for securing critical industrial and control networks against malicious attacks.

FortiSwitch Rugged Series deliver all the performance and security of Fortinet's trusted FortiSwitch line, but with added reinforcement that makes them ideal for deployments in harsh outdoor environments. Management by the FortiGate simplifies operation and extends security policies down to the switch ports.

FortiAP Outdoor Series delivers secure, identity-driven WiFi access points with management provided by the integrated wireless controller functionality within the FortiGate. Combined with FortiSwitch, this provides for a truly unified access layer with common security policies.

Fortinet's rugged and outdoor series devices are offered in various form factors with features like superior mean time between failure, electromagnetic interference protection, vibration tolerance, ingress protection waterproofing, wide thermal operating ranges, fanless cooling and power over ethernet.

These devices are controlled by Fortinet's FortiOS security operating system and are backed by FortiGuard Industrial Security Service to protect the most widely-used ICS and SCADA devices and applications. FortiGuard Industrial Security Service delivers OT-specific, real-time threat intelligence for vulnerability protection, deep visibility and granular control over proprietary ICS and SCADA protocols.

The Fortinet Fabric-Ready Partner Program also enables organizations to seamlessly integrate complementary, third-party OT security solutions with the Fortinet Security Fabric. These deep technical integrations are pre-validated to ensure consistent interoperability, ease of deployment, reduced complexity, and increased automation.

Are Cell Phones the Greatest Threat to Prison Security

According to the US NIJ (National Institute of Justice*) "A widespread technology that allows people to connect with anyone, anywhere, has created concerns for corrections officials. The use of inexpensive, disposable cell phones has changed the age-old cat-and-mouse game of controlling whom inmates communicate with in the outside world and is creating serious problems for public safety officials."

"In the 1990s, cellular phones were larger and heavier and had audio capabilities only. Today they are lightweight, can be thinner than a matchbook, and can send both audio and data, including written messages and streaming video. Although these advances are welcome in society in general, they have had a negative impact on the law enforcement community, as criminals have taken advantage of cellular technology to conduct illegal activities."

In recent years, the use of contraband wireless devices by inmates in correctional facilities has grown rapidly.

Inmates use these devices to commit additional criminal acts from behind bars, such as ordering hits, running drug operations, and operating phone scams. Use of contraband wireless devices is a serious threat to the safety and welfare of correctional facility employees, other inmates, and innocent members of the public.

Statistics released by Ministry of Justice in the UK show that in 2016 alone over 20,000 mobile phones and sim cards were recovered from prisons in the UK - helping to thwart the attempts of criminals to continue committing crime behind bars.

UK Prisons Minister Sam Gyimah said: "I have been clear that the current levels of violence, drugs and mobile phones in our prisons is unacceptable. We have put in place a number of measures to help disrupt this illegal activity as it is an issue I am absolutely determined to resolve."

The Federal Bureau of Prisons in the US confiscated

5,116 cell phones from its facilities in 2016. Based on data available for the first six months of this year, the agency projects that the number of confiscations will jump by 28 percent in 2017.

The problem "is significantly worse in state and local correctional facilities," Assistant Attorney General Beth A. Williams wrote on Aug. 28 in a letter to FCC Secretary Marlene Dortch.

A multi approach is needed to control contraband communications within the prison environment.

Recently in the UK a £2 million investment has seen every prison across the estate fitted out with NLJD Non-Linear Junction Detectors ie hand-held mobile phone
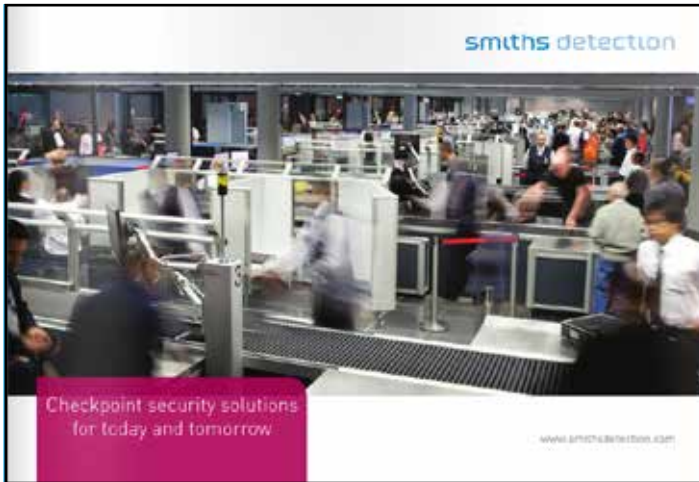
detectors and portable detection poles to step up the detection of illegal phones on the landings. Whilst in the US, Jamming devices, managed access, specially formulated paints and coatings that block radio frequency signals and even dogs are being utilised.

However, these solutions are labour intensive.

A piece of equipment that is already being used successfully at many prisons, that can be operated by Prison Officers requiring no Specialist training, is the SOTER RS. A low dosage full body scanner combining ultra-low radiation with maximum visibility. It is extremely easy to use and fast, and as it uses a minuscule dose of radiation and is therefore harmless, the dose absorbed is lower than 2 µS..

The person to be scanned stands on a platform that is transported from left to right. This process takes about 10 seconds and during that period an x-ray image is generated, showing the entire body and all contraband is revealed in it. The SOTER RS makes it impossible to smuggle contraband in the human body, including contraband wireless devices.

World Security Report

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

Border Security Report

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

January 2018
21-23
Intersec 2018
Dubai, UAE
www.intersecexpo.com

29-31
Cybertech
Tel Aviv, Israel
www.cybertechisrael.com

30-31
Asia Defence Expo & Conference Series (ADECS)
Singapore
www.asia-decs.com

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

February 2018
20-22
European Defence Procurement
Brussels, Belgium
www.eudefenceprocurement.com

20-22
World Border Security Congress
Madrid, Spain
www.world-border-congress.com

March 2018
5-6
Defence Logistics Eastern Europe
Prague, Czech Republic
www.defence-logistics.eu

6-7
Security & Policing
London, UK
www.securityandpolicing.co.uk

6-7
Security & Counter Terror Expo
London, UK
www.counterterrorexpo.com

14-15
Behavioural Analysis
Cardiff, Wales, UK
www.behaviouralanalysis.com

July 2018
17-19
Critical Infrastructure Protection & Resilience Asia
Sarawak, Malaysia
www.cip-asia.com

September 2018
25-27
Critical Infrastructure Protection & Resilience Europe
The Hague, Netherlands
www.cipre-expo.com

December 2018
4-6
Critical Infrastructure Protection & Resilience North America
Florida, USA
www.ciprna-expo.com

BORDER SECURITY
REPORT

COVER STORY

THE BODY CAVITY BOMBER
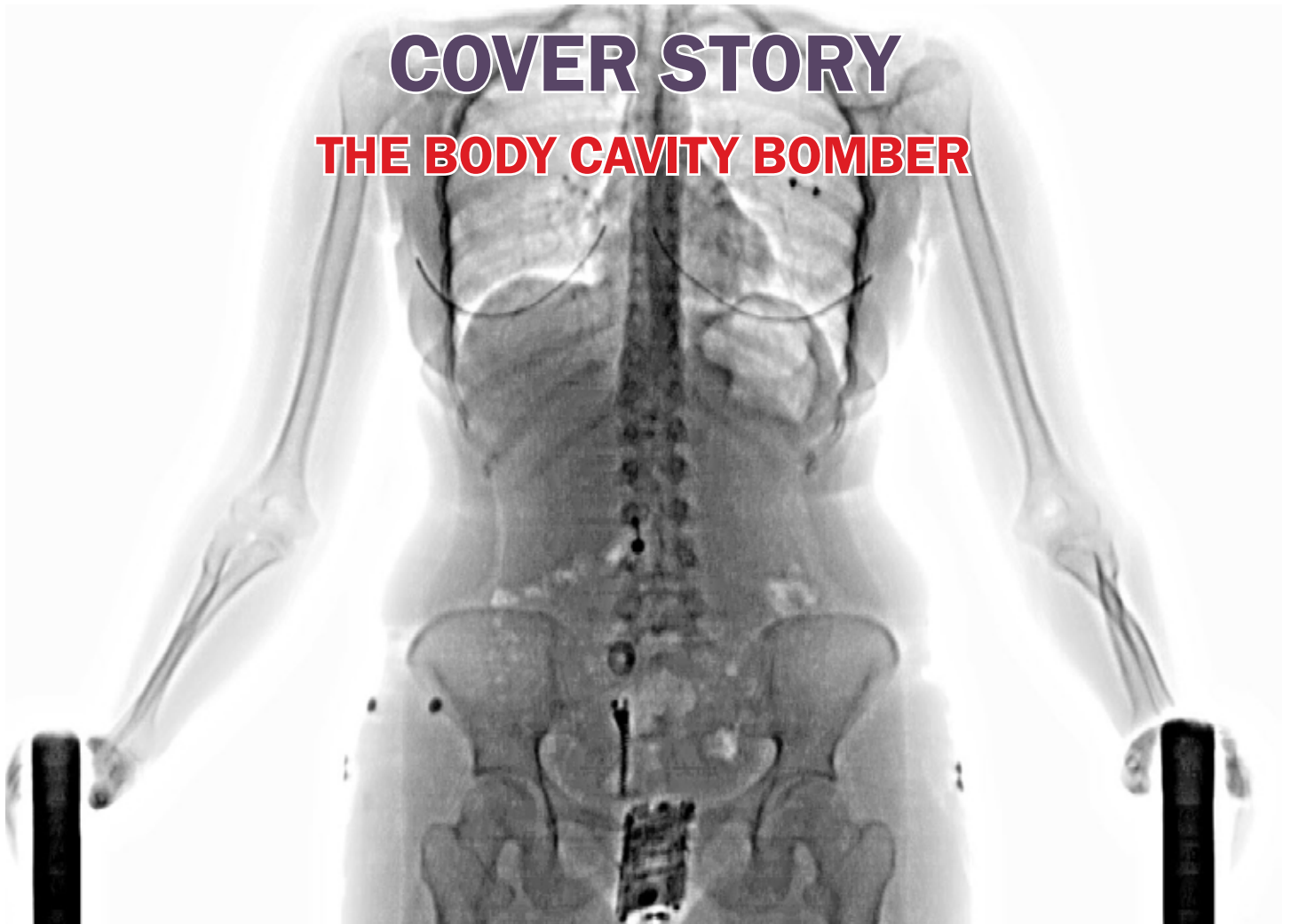
SPECIAL REPORT

Artificial Intelligence p.16

AGENCY NEWS

A global review of the latest news and challenges from border agencies and agencies at the border. p.10

SHORT REPORT

The World's Deadliest Border p.4

INDUSTRY NEWS

Latest news, views and innovations from the industry. p.18

Brexit and the Irish Border

As the United Kingdom and European Union finally reached what looks like a fudged agreement to move on to the next phase of the Brexit talks, Britain seems to have agreed that there will be no hard border between the Republic of Ireland and (EU) and Northern Ireland (UK). The UK is proposing a technological solution to the issue, which, in essence means some sort of digital self-declaration of goods passing between Ireland and Northern Ireland.

Experts say that this will be very difficult to achieve without harmonization of customs controls and regulation i.e. N. Ireland (NI) stays in the Customs Union. But this is an anathema to Unionists in NI believing as they do that this will be a major step towards unification. As the Unionists hold the balance of power that keeps Theresa May in Downing Street, that is something that is simply not going to happen.

So, will the digital option work?

Well of course it could in some regards but not in others. Allowing companies to do some sort of digital self-declaration and pre-pay duties is entirely doable. But it's not the bigger firms with accounts and IT departments that are the real problem. It is the small firms constantly coming and going across the border with bread for a local corner shop or a spare part for a car or vacuum cleaner. Are they really going to go online and declare ten sticky buns and muffin or a head gasket for Yaris, no, of course not? But like their income tax return for small businesses an annual self-declaration is more feasible. Most people are honest and if asked to declare how many sticky buns they have exported over the course of the year will declare something plausible at least

Keeping regulation and safety standards as harmonised as possible, particularly around agricultural produce and foodstuffs will also go a long way to making it workable.

This approach of course breaks down when it comes to those criminals that will exploit the border for their nefarious activities. For this we will have to rely on CCTV, NPR, face recognition, big data and good old-fashioned intelligence to spot the patterns and arrest the bad guys. And of course passport control for everyone travelling to the UK mainland, yet another contentious issue to be overcome.

It will be difficult, expensive and will require a good deal of flexibility but overall, I'm optimistic that it can be made to work. Who knows, if they get it right, it may become the blueprint for border management.

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

» p.5

» p.10

» p.13

» p.26

New Study Concludes Europe's Mediterranean Border Remains 'World's Deadliest'

IOM, the UN Migration Agency's Global Migration Data Analysis Centre (GMDAC), has released a new report reviewing the evidence of Four Decades of Cross-Mediterranean Undocumented Migration to Europe and concludes that Europe's Mediterranean border is "by far the world's deadliest."

Relying on analysis of IOM estimates from the Missing Migrants Project, the report states that at least 33,761 migrants were reported to have died or gone missing in the Mediterranean between 2000 and 2017 (as of 30 June). Professor Philippe Fargues of the European University Institute, the report's author, notes that this number likely under-reports the actual scale of the human tragedy, even as the record number of migrant deaths may have begun to subside in 2017 due in part to cooperation between the EU and Turkey, and now Libya, to stem migrant flows.

"Stopping migration and eradicating deaths at sea may [be] conflicting objectives. Shutting the shorter and less dangerous routes can open longer and more dangerous routes, thus increasing the likelihood of dying at sea," Prof. Fargues states in the report.

The report analyzes irregular migration across the Mediterranean since the 1970s. It highlights that irregular arrivals to Europe have increased in response to more restrictive migration policies by some European countries.

Prime examples from the report are the irregular migration from North Africa and Turkey to Europe in the 1970s, after visa requirements were introduced for temporary labour migrants from these regions. These

policies encouraged those who were already in Europe to stay, increased irregular migration of family members to join their relatives in Europe and gave way to the smuggling business.

Absence of legal pathways for asylum-seekers and refugees to travel to Europe and seek asylum also increased arrivals by sea along the Eastern, Central and Western Mediterranean routes since 2009.

The study also highlights differences between the modern pattern of migration from Africa to Italy, mostly via Libya, and that from the Middle East to Greece via Turkey. For example, Professor Fargues concludes that since 2009, "arrivals to Greece from Turkey are primarily of nationals from origin states affected by conflict and political instability (Iraq, Afghanistan, and Syria), who would be likely to receive refugee status in the EU." These asylum-seekers had no options for humanitarian visas or regular migration in their countries of origin, the report states.

Arrivals to Italy from North Africa largely originate across sub-Saharan Africa in response to deep migratory pressures – population growth coupled with limited livelihood opportunities, high unemployment and poor governance and political and economic instability.

People from major refugee-source countries were a minority of migrants arriving in Italy, except for a short period in 2013–14. However, the number of first residence permits issued in Europe in 2009–2016 to African nationals – an indicator of regular migration – was higher than that of African migrants arriving irregularly by sea. The report also notes that most migrants in Libya come from countries that are not among the top countries of origin of migrants smuggled to Italy.

The report concludes by acknowledging the limitations of available data on irregular migration and identifying further research and data needs.

Download full report at:

https://publications.iom.int/books/four-decades-cross-mediterranean-undocumented-migration-europe-review-evidence

THE BODY CAVITY BOMBER

The threat posed by the cavity bomber is nothing new. In fact, I have been writing on the subject regularly since 2009. But just because it is an old problem, it doesn't mean that in all that time we have done anything meaningful to mitigate that threat.

So, what's the background?

Back in August 2009 the attempted assassination Prince Mohammed bin Nayef, the Saudi Interior Minister, was the first time that this method of attack was reported. On this occasion, with the element of surprise on their side, the terrorist was able to pass through two airport security screenings and the Prince's own security before detonating a device that used a mobile phone card and a half kilo of explosives that had been inserted in his rectum.

Abdullah Hassan Tali al-Asiri

Fortunately, the Prince was unhurt but the perpetrator, a Saudi citizen, Abdullah Hassan Tali al-Asiri, was blown in two.

There has been a lot of talk about why the attempt failed, many commentators saying that the body absorbed the blast and therefore it would not work on an aircraft. Not so, my sources tell me that the blast, though directed downwards, blew a 6" hole in the concrete floor, which is enough to be devastating virtually anywhere in the pressurized cabin of a soft skinned aircraft but especially if the perpetrator position themselves on a door.

In 2012 we had the attempted assassination of Afghanistan's intelligence chief, Asadullah Khalid, again perpetrated using an IED carried concealed inside the suicide bombers body cavity.

Asadullah Khalid, Afghanistan's intelligence chief

Following a previous assignation attempt by a terrorist with a bomb hidden in his turban, this individual was asked to strip in an armoured room and observed by CCTV.

The bomb was obviously not picked up using this method, and so the unnamed assailant was allowed to see Mr Khalid, where the bomb was detonated.

Mr Khalid was not killed but suffered serious injuries that required ongoing treatment in here the US.

This is not a threat that will go away. It will have been noted by terrorist organisations around the world that twice, VIP security screening has been penetrated and they have successfully detonated a device.

With no shortage of young men and women willing to die for their cause and the small amounts of explosive needed for these high-profile attacks, it will no doubt be used again.

Now, there is probably a limit to the size of a device that can be carried in the rectum, limiting the explosive power,

but there are some well known and well known and well used ways of increasing the amount that can be carried in the body.

Every week at airports around the world, drugs mules are caught carrying swallowed illegal drugs inside their stomach. They have been known to carry over two kilos, in up to 150 capsules (usually condoms).

In prisons, a wide variety of objects are routinely smuggled into prison hidden inside prisoners or visitors body cavities. Typically, these will be high value prison contraband such as mobile phones, drugs, cigarettes etc.

According to an msnbc report in 2012, a working 0.38 calibre revolver with a six-inch barrel was smuggled into a jail cell by a criminal suspect, Michael Leon Ward. The suspect had been strip searched and asked to perform what's called a "squat and cough" but the weapon was not discovered. It was only discovered when officers were alerted by other inmates.

In September of this year, Illinois police arrested 20-year-old Amika Witt. During a cavity search of her vagina, they found a Kimber.380-calibre handgun, fully loaded and with a bullet in the chamber.

Kimber.380-calibre handgun

These may seem like extreme cases and it's true that a standard pistol is almost certainly going to be picked up by metal detector, even carried internally, but it illustrates what a determined individual can do.

The routine use of these methods of smuggling materials through some of the world's most secure correctional facilities makes for worrying reading.

Other methods such as surgically inserting drugs into

mules in breast implants have also been widely reported and terrorists have also experimented with surgically inserting IED's in animals.

Now if a terrorist were to combine these methods of carrying explosives, conceivably they could conceal significantly more explosives inside the body. More than enough to down an aircraft, attempt assasinations or cause considerable damage to other critical national infrastructure targets such as power stations, chemical plants of nuclear facilities.

Nor does the use of body cavities as means of smuggling, mean that the explosive has to be detonated in the body. The components can be recovered, assembled and used in more conventional sabotage methods.

The nightmare for security officers is that most of the usual methods of detection currently used in security screening will not pick up explosives carried internally.

So what technology do we have and what are their limitations?

Metal detectors, even on the highest sensitivity setting are not likely to pick up the very small amounts of metal required for a modern IED using sim cards and detonators. And on higher sensitivity settings are likely to give off too many false alarms, making them unreliable.

Millimetre wave scanners are now widely used in airport screening and are very effective in detecting objects beneath clothes but cannot see objects carried internally.

Another technology tried in the US by the Transport Security Agency (TSA) is the Explosive Trace Portals (ETPs), commonly known as as puffer machines. These use a mass spectrometer to detect trace compounds in air circulated around a person in a booth. Some of these machines were deployed in airports but were later withdrawn because of reliability issues. It is also not clear whether these machines would detect explosives carried internally in any case.

Trace detection technology such as Ion Mobility Spectrometry is a commonly used method for individuals or belongings to detect either vapours or particles, which

No 10 defends closer EU co-operation on cross-border crime

Downing Street has defended a decision to work more closely with the EU on cross-border crime as it prepares for Brexit.

The UK is joining forces with the remaining member states to strengthen action against the criminal movement of money across national boundaries.

Prime Minister Theresa May's spokesman said: "The PM has been clear that when it comes to security and criminality we want to co-operate closely with the European Union.

"This is a decision based on the fact that we are still an active member and the decision was taken in that light.

"As to what we do going forward that's all a matter to be discussed."

Financial Secretary to the Treasury Mel Stride said the move would "enhance border security without imposing disproportionate burdens on business".

He added: "The proposed new regulation will reinforce the existing controls of cash moving across EU borders, bringing these controls in line with international norms and best practices for addressing evolving forms of

criminality.

"Until the UK leaves the EU it remains a full and participating member. We will continue to work with the EU institutions, with the aim of ensuring that UK objectives are preserved as the negotiations progress on any compromise text."

is then analyzed by the machine. It is quick and reliable but it relies on the carrier having handled the explosives at some stage during preparation for the operation. But given the fact that its use well known and the intended location of the hidden device, the perpetrator may well rely on a close friend or colleague to help with the insertion!

However, there is a technology that is already in daily use that will detect any object carried internally, and that is the low dosage X-Ray body scanner.
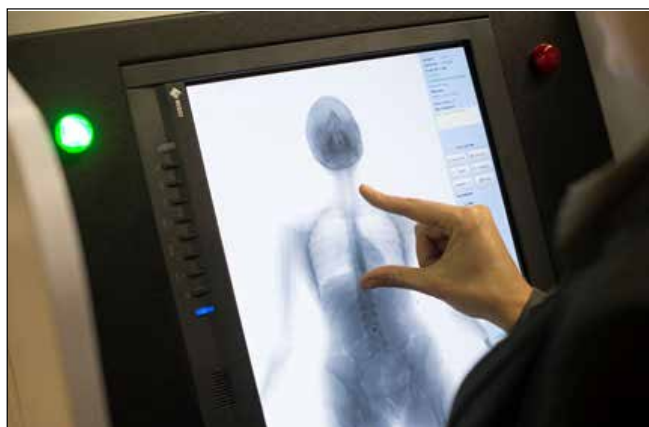
They are in use in correctional facilities around the world especially here in the US. These machines are also already widely in use by custom officials at airports around the world for detecting drugs and contraband smugglers.

But in arrivals, not departures.

So why not use the X-Ray body scanners to scan everyone getting on an aircraft?

Speed is one thing; an X-Ray scan takes too long for mass screening.

Then there are also the ethical and privacy concerns still to be addressed by the authorities and although the X-Rays scans are in very low safe doses, there will inevitably be some reservations to be addressed on behalf of the travelling public.

But, as the manufacturers themselves will tell you, X-Ray body scanners are best used for targeted individuals, identified by other means.

As yet, the only machines of this type that I know of, being used for screening boarding passengers are in Nigeria and maybe one other country. The machines in Nigeria and were paid for by the US government, but are being used exclusively for drug interdiction and only and for passengers flying directly to the USA. All the other machines in airports around the world are being used in arrivals for catching drugs mules.

Another technology that could be of real value is behavioural-analysis software. This software is designed to work in conjunction with CCTV systems to screen travellers for unusual behaviour patterns and the involuntary physical and physiological reactions that people exhibit in response to a fear of being discovered. However, these systems are currently a work in progress, but as CCTV systems and control rooms are already in place, could be another

relatively easily deployable, non-intrusive layer to airport security.

The essential fact remains though, that right now the global airport security community has no mass screening detection technology currently deployed to counter the threat of the IED carried internally. Nor is there any likelihood of developing one in the short to medium term.

So, what's to be done?

Advanced Passenger Information is a key component but will only be truly effective when it is applied universally and we have found a way of sharing intelligence and watch lists, through trusted third parties like Interpol. But that only really works for the people we know.

For the individuals that we don't know, we need properly trained security staff applying effective questioning and risk assessment techniques (I constantly told not to use the term 'profiling').

Some stop gap measures would be more use of explosive dogs to check the passenger queues. Dogs are still the most effective explosive detection but also provide some deterrent and reassurance for the public. Dogs will also add to the general discomfort of would-be suicide bombers, making them easier to spot.

We should make sure that effective technologies, already available elsewhere in the system, such as through body-scanners, are made available to officers for pre-flight screening.

Finally, we should keep a random and unpredictable element to our security screening and use of technology. The terrorist will watch for patterns and seek out the inevitable flaws in the system.

Maybe they will use an insider or send a woman with a baby. Maybe the terrorist will be home-grown like Richard Reid.

The terrorist has the luxury of time and surprise, target switch is part of their stock-in-trade as we struggle to plug one gap, our enemies are already looking for the next one!

Tony Kingham, Editor

Senators Say They're Closing In on a DACA and Border Deal

Senate Majority Leader Mitch McConnell vowed to bring a vote on immigration legislation if a bipartisan group of lawmakers can come up with a deal next month that includes border security as well as protections for undocumented immigrants brought to the U.S. as children.

There is support from lawmakers in both parties for the deportation shield in the Senate, but it likely would hit opposition from a group of conservative Republicans in the House that has stymied action on the issue in the past.

"I encourage those working on such legislation to develop a compromise that can be widely supported by both political parties and actually become law," McConnell said in a statement.

McConnell said that would include improving border

security and immigration enforcement in the U.S. and dealing with the Deferred Action for Childhood Arrivals, or DACA, program established through executive action by former President Barack Obama.

The Republican and Democratic senators working on an immigration agreement were meeting Wednesday afternoon. They said earlier in the day that they are closing in on a deal, though a final resolution isn't likely to come until January.

Democrats dropped their insistence on including the deportation protections for the group known as "dreamers" in the stopgap government funding that Congress must pass by Friday to avert a government shutdown.

Spanish Guardia Civil Supported By EUROPOL Breaks Up Illegal Tobacco Factory

On 5 December 2017 the Spanish Guardia Civil, with support from the State Border Guard Service of Ukraine, the European Union Border Assistance Mission to Moldova, the Bulgarian Police of the Ministry of Interior, the Romanian Guard Police, the Greek Police, and Europol, arrested 18 members of a criminal organisation for manufacturing more than two million cigarettes per day.

The organised crime group had invested almost EUR 3 million to start up their illegal tobacco factory in Granada and had even created their own cigarette brand. The workers, mainly from Ukraine and Bulgaria, were living in safe houses and forced to work more than 12 hours each day in a very unhealthy working environment.

As a result of the investigation, the factory in Granada has been dismantled and eight searches were carried out in Granada and Malaga. During the searches, 10 tonnes of tobacco leaves, 4 tonnes of fine-cut tobacco, 4.5 million cigarettes, machinery, filters, paper and glue, were seized. Seven Ukrainian workers were arrested in the factory, while they were illegally producing cigarettes.

Operation DRAGON Delivers Major Blow To Organised Crime

Law enforcement authorities from more than 60 countries, coordinated and supported by Europol and Frontex, have joined forces to target organised crime groups and their infrastructures across the EU in a series of actions in hundreds of locations, with the cooperation of Eurojust, INTERPOL, AMERIPOL, CLACIP, NCFTA, CCWP, UNODC and IATA.

Operation Dragon has been the fourth cooperative international law enforcement operation under the EU Policy Cycle targeting serious and organised crime in the EU and globally, and involved actions in hundreds of locations between 5 June and 20 October 2017.

EU Member States and their international partners came together to disrupt the activities of criminal groups involved in the following crime areas: payment card fraud, facilitation of illegal immigration, cybercrime, synthetic drugs/cocaine/heroin trafficking, firearms trafficking, euro counterfeiting, organised property crime, excise fraud and trafficking in human beings.

As part of Operation Dragon, law enforcement authorities assigned thousands of police, border and coast guard as well as customs officers to actions that focused on key hot spots in the EU, with the aim of having a lasting and significant impact on serious and organised crime, disrupting criminal groups and their activities for months or even years to come.

Electronics Payments Organised Criminals Disrupted

Four key members of an international criminal network responsible for compromising payment card data and illegal transactions against European citizens were arrested during a joint law enforcement operation called "Neptune".

The operation run by the Italian Carabinieri, in cooperation with the Bulgarian General Directorate of Combating Organised Crime, and the National Police of Czech Republic, supported by Europol's European Cybercrime Centre (EC3) culminated today with the arrest of four Bulgarian citizens. The leaders of the transnational criminal group actively supervised all stages of criminal activities, including placing technical equipment on ATMs in the central areas of European cities, producing counterfeit credit cards and subsequently cashing out money from ATMs in non-European countries, for example Belize, Indonesia and Jamaica.

Enhancing border security by detecting illicit travel documents

Developing the knowledge and skills of specialized officials to identify fraudulent documents was the focus of an INTERPOL workshop in Nassau.

Involving 16 border control officers and law enforcement

officials from four countries – Bahamas, Colombia, Jamaica and Mexico – the three-day security document examination training sought to enhance border security by developing the capacity of participants to detect fake and counterfeit travel documents often used by criminals and terrorists.

"It has become very easy for people and goods to cross international borders. Hence, international cooperation must be strengthened to guard against the increase of fraudulent documents which threatens national security," said the Head of the INTERPOL National Central Bureau in Nassau, Telinda Missick.

During the training course, the second to be jointly delivered by INTERPOL's Counterfeit and Security Documents Branch (CSDB) and international digital security company Gemalto, participants also took part in practical exercises which examined printing methods, document security features, document verification technologies and examination techniques.

Biometric data plays key role in fighting crime and terrorism

Responding to the threats posed by foreign terrorist fighters (FTFs), INTERPOL is working to increase the use of its biometrics databases and capabilities to better track their movements globally.

Launched earlier this year, Project First is among INTERPOL's initiatives to assist law enforcement in member countries in enhancing their border security through the use of biometric data – such as fingerprints and facial recognition

– on FTFs and other individuals linked to terrorist activities.

Underscoring the growing recognition of biometrics as a critical tool against transnational crime, speakers at the 1st INTERPOL Fingerprint and Face Symposium, organized by INTERPOL's Fingerprints unit, included the UN Counter-Terrorism Committee Executive Directorate, the UK ACRO Criminal Records Office and the Biometrics Institute.

Safeguarding victims of human trafficking and smuggling priority for international experts

International experts in human trafficking and migrant smuggling are calling for expanded cross-sector involvement in order to protect the world's most vulnerable from the exploitation of organized crime groups.

With such groups constantly innovating in their pursuit for low-risk, high profit margins, discussions during the 5th edition of the INTERPOL Global Trafficking in Human Beings and Smuggling of Migrants Conference will focus on the essential role both the public and private sector

play in preventing, detecting, reporting, disrupting and ultimately prosecuting those responsible for crimes which have no borders, and no limits.

Participants will explore emerging trends such as trafficking for forced criminality including drug cultivation or pickpocketing. They will also focus on how the private sector is developing tools to help law enforcement in the disruption of trafficking and smuggling activities.

OSCE Programme Office in Dushanbe holds training course on raising awareness of human trafficking

A three-day training course organized by the OSCE Programme Office in Dushanbe on raising awareness of human trafficking and identifying and assisting victims concluded on 13 December 2017 in Dushanbe.

During the course 20 representatives from civil society and NGOs that work with trafficking victims discussed the most common types of human trafficking and ways to assist the victims.

"Using an interactive approach, we focused on gender roles in a patriarchal society and how they, in combination with poverty, create a favorable environment for trafficking in human beings. We worked on case studies in order to better understand and identify potential and presumed victims, including children, and practiced interviewing skills with victims through role plays," said Vesna Ivanovikj-Castarede, Gender and Anti-Trafficking Officer at the OSCE Programme Office.

Raising awareness among the general public and working with professionals and civil society is part of the comprehensive approach of the OSCE Programme Office in combatting trafficking in human beings. Co-operation with all relevant actors will continue to prevent trafficking in human beings and to support state institutions in their efforts to provide assistance to identified victims.

OSCE and UNODC train Kyrgyz officials to disrupt terrorist financing and to use sanctions pursuant to relevant UNSC Resolutions

A six-day training course aimed at strengthening the capacity of government officials from the Kyrgyz Republic to disrupt the financing of terrorist networks, including practical sessions on how to use sanctions pursuant to UN Security Council Resolutions (UNSCR) 1267,1988,1989,2253,2255, 2368 was held in Bishkek.

The training course was organized by the OSCE's Transnational Threats Department and the UN Office on Drugs and Crime (UNODC)'s Global Programme against Money Laundering, with the support of the OSCE Programme Office in Bishkek and with the participation of the Analytical Support and Sanctions Monitoring Team established pursuant to UNSCR Resolutions 1526 (2004) and 2253 (2015) concerning ISIL (Da'esh), Al-Qaida and the Taliban and associated individuals and entities. Attended by 16 government officials, the course was led by OSCE and UN experts, supported by four national experts.

This course was part of a series of progressively advanced training courses on countering the financing of terrorism for Kyrgyz officials from the Financial Intelligence Unit, the Ministry of Interior, the intelligence services and the Prosecutor's Office. From June to October, the OSCE and UNODC organized two training sessions and two train-the-trainer courses for Kyrgyz officials focused on analysis and investigation. A three-day train-the-trainer course in November provided national experts with the chance to familiarize themselves with more complex analytical and operational planning methods, including preparing UN sanctions listing cases. The training process focuses on localized scenarios based on real-life cases.

The training programme helped the participants to understand how inter-agency co-operation can contribute to disrupting terrorist financial networks and to strengthen their skills.

UN Migration Agency Launch First Global Migration Data Portal

Germany's Federal Foreign Office and IOM, the UN Migration Agency's Global Migration Data Analysis Centre (GMDAC) will launch today (15/12) the Migration Data Portal in Berlin. The Migration Data Portal brings together the key facts and figures about global migration trends in one place for the first time.

"Especially in critical times, such as those we are facing today, it is our task to ensure that responses to migration are based on sound facts and accurate analysis," said IOM Director General William Lacy Swing.

The idea to develop such a portal was first discussed and agreed upon on 12 July 2016, at the 2nd Berlin Roundtable on Refugees and Migration, where the former German Foreign Minister met with heads of international organizations working on migration, including IOM, UNHCR, the IFRC, the EC and the World Bank. The Portal was developed by IOM and with the support of the Economist Intelligence Unit (EIU).

The Migration Data Portal was developed with financial support from the US Department of State and Germany's Federal Foreign Office.

The portal communicates global data on migration through visualizations, infographics and videos. It simplifies the navigation through complex international migration data for policy makers, journalists, statisticians and anyone interested in migration.

The portal also covers a wide range of topics including

data on immigration and emigration trends; the linkages between migration and development; data on irregular migration; students and children; and data on migration policies as defined by the United Nations development goals and background on a global compact on migration expected to be adopted by the UN in 2018.

At its initial stage, the portal features 70 indicators from 15 international data providers (UNDESA, UNHCR and World Bank among others) and aggregates data at the national, regional and global levels. This range offers ample opportunities to explore and compare data while, understanding the context behind it.

"At a time when migration is high on the global agenda, it is essential that everyone has access to the key facts and figures about migration, and that we better understand the strengths and weaknesses of data on migration," said Frank Laczko, Director of IOM´s Global Migration Data Analysis Centre.

German foreign policy employs a coherent strategy to manage migratory movements more efficiently and to address the root causes of forced migration. For fact-based policies and responses, reliable data are vital to ensure efficient, needs-based humanitarian aid, to counter harmful assumptions and to fight populism.

The development of the Migration Data Portal is a big step forward towards making the multitude of data on migration better and more available to policy makers.

The Migration Data Portal will scale up in coming months, making more data available at the regional and national levels. Visit the Migration Data Portal at: www.migrationdataportal.org.

Mediterranean Migrant Arrivals Reach 167,724 in 2017; Deaths Reach 3,095

IOM, the UN Migration Agency, reports that 167,724 migrants and refugees entered Europe by sea in 2017 through 13 December, with just over 70 per cent arriving in Italy and the remainder divided between Greece, Cyprus and Spain. This compares with 358,018 arrivals across the region through the same period last year.

IOM Rome reported Thursday (14 December) that according to Ministry of Interior figures, 118,010 men, women and children have arrived in Italy this year. With just over two weeks remaining in 2017, these totals indicate total arrivals this year are expected to be well short of the 181,436 who arrived in 2016, by an estimated 35 per cent, given current December arrival rates. This month new arrivals are averaging fewer than 80 migrants per day; that compares with 260 per day in December 2016 and 310 per day in December 2015.

IOM Spain reported that total arrivals at sea in 2017 are now at 20,473 men, women and children being rescued in Western Mediterranean waters. IOM's Missing Migrants Project (MMP) reported this week confirmation of four more deaths in the Western Mediterranean: the Spanish Coastguard reported two missing and one dead in the Alboran Sea on 13 December, plus MMP added one case from 27 November, of a migrant who died in a ferry bound for mainland Spain in Port of Melilla.

There were no new reports of deaths in the Central Mediterranean Sea route.

On Thursday (14 December) IOM Athens' Kelly Namia reported at least five incidents off the island of Lesvos, Samos and Leros that required search and rescue operations. The Hellenic Coast Guard managed to rescue some 200 migrants and transferred them to the respective islands.

Since 1 August, Namia reports 16,769 men, women and children have entered Greece by sea via the Eastern Mediterranean or almost 50 per cent more migrants than entered (11,405) during all of 2017's first seven months. Namia further reported that 576 migrants or refugees entered Greece by sea during the dates 11-13 December, or nearly 200 per day.

Through 13 December, the total number of sea arrivals to Greek territory is 27,598. If that average holds through the month's 18 remaining days, 2017 is likely to see the lowest total of sea migrants arriving irregularly to Greece in the last four years.

IOM's Missing Migrants Project (MMP) reported worldwide deaths have reached 5,323 men, women and children during migration in 2017.

In the Western Mediterranean, MMP reported the Spanish Salvamento Marítimo has recorded testimonies of 32 migrants rescued from a sinking boat on 13 December, reporting that two people went missing in the Alboran Sea between Spain and Morocco during their voyage. In another rescue operation on the same day (13 December), the body of a migrant was found in a boat, five nautical miles west of Alboran Island. The Spanish Coastguard rescued 68 survivors from this boat.

Additionally, reports emerged of the death of a young man inside a container in a ship bound for mainland Spain in Port of Melilla on 27 November. Since 1 January 2017, IOM has recorded the deaths of 210 people in the Western Mediterranean route to Spain – a number that surpasses the total number of deaths recorded in the Western Mediterranean for all of 2016, which totalled 128.

In the Middle East, three migrants died in a vehicle accident on 4 December 15 km from Murchehkhort, in Isfahan (Iran). Additionally, the MMP team recorded cumulative data of deaths confirmed between 1 January and 4 December 2017 on the Iran-Afghanistan border: 97 Afghan migrants reportedly died in vehicle accidents at various locations this year.

On the US/Mexico border, 14 migrants died of hypothermia due to extremely low temperatures in the past two weeks. On 7 December, a Mexican man was found dead in a ranch near Eagle Pass, Texas, while remains of another man of unknown nationality were discovered on a ranch near Norias, in Kenedy County (Texas).

On 8 December, a Guatemalan national suffering from hypothermia passed away in the Big Bend area, near Marfa, Texas. On 9 December, the remains of one migrant were found on the Mexican side of the border, in Nogales, Sonora (Mexico).

The Webb County Medical Examiner reported that an additional 10 migrants have died from hypothermia in various locations in Texas between 1 and 13 December. During this period, Missing Migrants Project also recorded the death of a migrant due to unknown causes in a ranch near Falfurrias, Texas, on 7 December.

MMP data are compiled by IOM staff but come from a variety of sources, some of which are unofficial.

8th ASEANAPOL Training Cooperation Meeting (APTCM) Singapore

The Executive Director of ASEANAPOL Secretariat, Police Inspector General Yohanes Agus Mulyono together with the Director for Plans and Programmes, ACP Aidah Othman and ASP for Plans and Programmes attended the 8th APTCM hosted by the Singapore Police Force.

The two days meeting were attended by all 10

ASEANAPOL Member Countries, 4 Dialogue Partners, 3 Observers and the Secretariat itself. This year's meeting also witnesses the representative from the International Law Enforcement Academy (ILEA) Bangkok giving a presentation. At the meeting, delegates presented their annual training progress, challenges encountered and future plans to enhance training cooperation. The Dialogue Partners and Observers also reiterate their commitment and willingness to cooperate with Member Countries in the field of training and capacity building.

Next, all delegates were brought to visit the Home Team Academy and the Home Team Tactical Centre for briefing and demonstration by the Home Team members.

The two days fruitful meeting were conducted in a friendly and mutual atmosphere amongst all Member Countries, Dialogue Partners and Observers.

ICAO traveller identification event highlights key aviation role in combatting terrorism and cross-border crime

The fight against international terrorist and criminal movements took another step forward recently, as experts and senior officials gathered for ICAO's 13th Traveller Identification Programme (TRIP) Strategy Symposium.

"The ICAO TRIP strategy reinforces the global line of defence against international terrorist movements, cross border crime, and the many other threats to the safety and security of civil society and international aviation," stressed ICAO Secretary General Dr. Fang Liu in her opening address to the event.

"The main part of our work in this area is conducted under Annex 9 to the Chicago Convention, on Facilitation. Facilitation activities are strongly supportive of the UN Sustainable Development Goals (SDGs), and the ICAO TRIP Strategy also significantly contributes to UN Security Council Resolutions 2178 and 2309."

The world's foremost travel document and identity management event, this latest edition of the TRIP Symposium is seen as an important step in maintaining

the global momentum on anti-terrorism priorities recently achieved through the United Nations Security Council (UNSC).

Dr. Liu presented an aviation security brief to the UN Security Council this September, having also been invited to its Counter-Terrorism Committee (CTC) meeting in July of 2017. Along with enhanced screening and security checks, the CTC has highlighted the important role of airlines in tracking the global movement of higher risk passengers.

ARTIFICIAL INTELLIGENCE

Editor of Border Security Report, Tony Kingham, interviews the Co-founder of iOmniscient, Dr Rustom Kanga, on his latest thought around the advent and use of Artificial Intelligence.

Q: You have been in the artificial intelligence business for a long time. I believe you implemented your first commercial AI system back in 1982

Dr Kanga: That is right. Relative to what we do now that was rather primitive though I would say it is very similar to much of what is sold today by a number of companies under the label of Artificial Intelligence.

Q: So your video analytics today is very different to what you get from others?

Dr Kanga: Of course. We set ourselves the goal of maintaining a 5 to 10 year lead on our competitors. We have managed to maintain that in virtually all areas. Of course for those of our technologies that are patented we maintain a 20-year lead.

Q: Everyone is talking about Deep Learning Systems. Is this something you use?

Dr Kanga: Systems that can improve themselves through continuous learning have been around for a very long time. As computing power becomes less expensive it is possible to implement more sophisticated learning systems. Deep learning essentially involves studying many more characteristics of an object or of an environment and hence developing a more accurate understanding of it.

From the beginning all our systems have had a self-learning component. For instance, our systems will understand the environment and self-adjust when the light begins to fade as day changes to night.

While we use Deep Learning when we need to, our philosophy is to do more with less. So if we can use cleverer algorithms that require less computing power then we favour that

approach. For instance, if one wanted to recognize a dog, you could study every characteristic that different dogs have – they have 4 legs, they have their tongue sticking out when they pant, some have fur, some don't and so on. This involves deep learning. On the other hand we could see a dog's wagging tail and know it is a dog from that single characteristic. This requires much less computing power – there is no need for expensive GPUs and we can achieve an accuracy that is within 1% of the results you might get using deep learning. It does not mean we don't use deep learning. But we use it selectively where we see it gives most benefit.

Q: So why do others suggest Deep Learning is the future of Artificial Intelligence.

Dr Kanga: When you say "others" you are presumably referring to purveyors of GPUs who actively promote it because they sell more GPUs. Our goal is to provide our customers with the most cost effective technology that can do the job for them. This is not necessarily the most computer intensive.

Q: So you do not use GPUs at all? What about GPUs for Face Recognition

Dr Kanga: Today we don't see the need to use GPUs. Over time there may be a reason for us to do so.

For Face Recognition we have developed algorithms that can recognize faces with 22 pixels between the eyes with high accuracy and we can recognize down to 12 pixels with a slightly reduced accuracy. Compare that with the 60 to 300 pixels that other suppliers require. On a standard 2-megapixel camera we could

recognize a person 30 meters away while others may do it at a couple of meters' distance. More importantly we can use a standard PC even in a dense crowd while they require GPUs because they need to process more pixels and hence do more computing.

In fact, several GPU manufacturers provide open source Face Recognition algorithms and hence many people can now offer Face Recognition systems based on the same open source algorithms. They are all very similar and they all require heavy computing and hence a GPU.

Q: What other types of Artificial Intelligence are there

Dr Kanga: I would categorize Artificial Intelligence systems into two main types – heuristic systems and neural network systems. Deep Learning is a more sophisticated and more computing intensive form of neural networks.

Heuristic systems are rule based

systems. They have the advantage that they can be implemented very quickly and adapted to new requirements within minutes unlike neural networks which require a long learning period sometimes extending to weeks or months.

Humans use many types of reasoning simultaneously and we do the same in our systems. We use a hybrid approach using all the different types of artificial intelligence in combination taking advantage of the strengths of each one while mitigating their weaknesses.

Q: Computers are supposed to be good for deductive reasoning. What about intuition.

Dr Kanga: Computers are indeed very good at deductive reasoning. However, we also use a form of fuzzy logic which enables the system to use the limited information it receives to intuitively make judgements. Ultimately artificial intelligence is about emulating human intelligence and we use the various

technologies available to us to do this effectively.

Q: There are some very large companies in this field such as Oracle, Microsoft, CISCO and Huawei. How do you compete against them?

Dr Kanga: We don't compete against them. Such companies tend to be our partners. They use our technologies for many of the solutions they sell.

Q: In the field of video intelligence most people are focussed on one of three areas – Behaviour Analysis, Face Recognition and Licence Plate recognition. You do all of them.

Dr Kanga: Yes – we are not selling these technologies just as technologies. We help our customers to solve their problems. This often requires different technologies working together in different combinations. So what we have put together is a platform with a number of building blocks which can be put together in infinite permutations to actually address each particular problem.

We are therefore able to put together solutions to meet the specific requirements of about 30 different industries and we can achieve this without expensive customization.

Q: I understand you go beyond video in your analytics

Dr Kanga: Humans don't just use their eyes. They use their nose and ears as well to understand their environment. We do the same – so in addition to video analysis we do sound analytics and smell analytics. So for instance if we see a person falling down we can send someone to help him as it may be a simple accident. But if we

hear a gunshot at the same time we may recommend caution as someone obviously had been shot.

Q: Video Analytics requires cameras. How do you do Smell Analytics?

Dr Kanga: A camera is a sensor for light. A microphone is a sensor for sound. For Smell we have sensors that that can determine the chemical composition of air that passes over it and we can then analyse the mix. When people talk of IOT – the internet of things, most IOT devices are simple analogue devices with limited outputs – often it's a device which is either on or off or it provides information on a known scale such as a thermometer. Video, sound and smell analytics is IOT at the most sophisticated end of the spectrum as it involves understanding the very complex output of these devices.

Q: Different companies are good at different things. You do many things. Which ones are you good at.

Dr Kanga: We have a philosophy of being Best in Class in everything we do. If we are not good at it then we leave it to someone else. So for instance we have stayed out of the field of Autonomous Vehicles. We felt we did not have a sufficient differentiator or the necessary resources to become leaders in that field so we have exited that. However, in everything we do offer, you would be hard pressed to find anyone who could do it better.

Q: If your systems are so good they must also be more expensive.

Dr Kanga: One of our value propositions is that we can implement an intelligent system at a lower cost than a recording system. This is

because one of our design principles is that our technologies must reduce the infrastructure costs. So our systems require fewer cameras, less computing power, less storage and less network bandwidth than any other system on the market.

Q: Has everything been discovered or is there a lot of improvement possible in the technology.

Dr Kanga: 10 years after the Wright brothers managed to get the first powered plane off the ground, airplanes were already being used during the first world war. These were primitive planes but they flew and were useful. Today we can land a man on the moon.

Artificial Intelligence is a young technology. I would say it is at the same stage in its evolution as the planes in world war 1. In fifty years the technology will be considerably more advanced. But today the technology works and is already useful and it is certainly better than implementing systems with no intelligence.

Q: So what is next in AI. You already have many Firsts. How do you come up with the next big thing.

Dr Kanga: My partner Ivy or I might see a great idea in a movie like Star Wars or in a show like CSI. We ask our Engineering team to build that. The normal reaction is "that is impossible. The idea was developed in a Hollywood studio". Nevertheless, after much hair tearing and table thumping six months later we might have a prototype built. This is how many of our new products get created.

Thanks for your time and all the best.

AGENCY NEWS AND UPDATES

ITBP unveils mechanised column for deployment on China border

The ITBP today showcased its maiden mechanised column of power vehicles and machines, along with its agile PARA commandos, aimed at speedy mobilisation of troops along the Sino-India border.

The mountain warfare-trained force unveiled a fleet of its newly-acquired military trucks, sports utility vehicles (SUVs), all-terrain vehicles (ATVs), snow scooters, bikes, mobile communication wing, excavators and a few other medium- lift four-wheeled vehicles during its 56th Raising Day celebrations at its base here.

A contingent of special PARA commandos, sporting maroon berets, also marched down the track for the first time.

Iraq 'takes over' Turkey border crossing from Kurds

Iraqi government forces took control of the key border crossing with Turkey in the Iraqi Kurdistan region on Tuesday after weeks of tensions between Baghdad and Erbil.

The border crossing "has been handed over to the central government" of Iraq, Turkish Prime Minister Binali Yildirim told his ruling party at a televised meeting in Ankara.

He said all controls at the border will now be carried out by Iraqi and Turkish officials on their respective sides.

Greek police block migrants' march to border with Macedonia

Police blocked some 200 migrants and asylum-seekers Wednesday from leaving a city in northern Greece for the Macedonian border in hopes of traveling on to other European Union countries.

Dozens of officers in riot gear used shields to push back the migrants near the center of Thessaloniki and blocked the road with police buses. The marchers, who included families with young children, refused to leave and sat down in the street. No one was hurt in the brief confrontation.

The migrants, most of them from Syria, Iraq and Somalia, had gathered throughout the day in Thessaloniki. Many said they were responding to a campaign on social media for a march to the Greece-Macedonia border to

protest their inability to relocate to other European countries.

Police seize counterfeits worth millions

Hundreds of thousands of counterfeit goods valued at PLN 52 million (EUR 12 million) have been seized and 11 foreigners suspected of smuggling have been detained by police in Poland.

In a joint operation by the tax office, border guards and police targeting illegal migration and illegal trade, more than 200 buses filled with counterfeit goods were found near Warsaw.

Among the goods were fake brand-name clothes, shoes, accessories and cosmetics.

Police say the goods were to be sold to wholesalers and retailers and distributed throughout Poland and in other Central and Eastern European countries.

Ukraine Border guards stop international channel of trafficking in human beings

Representatives of the operative-search Unit of the Eastern Regional

Directorate of the State Border Guard Service of Ukraine found a criminal group.

5 people during 2016-2017 recruited and transported to the Russian Federation residents of the Dniprovska and Zaporizhzhia regions who were in a difficult financial situation in order to exploit in the sphere of intimate services.

Recently, at the "Goptovka" international checkpoint, border guards during passport control detained two women from Dniprovskyi region, who tried to smuggle Ukrainian women for sexual slavery to Russia Federation.

By operational means, law enforcement officers found another 9 Ukrainian women who could become potential victims of the criminal group. Offenders found all these women of job search announcements via the Internet, and promised them employment in the field of providing household services, such as waiters, dishwashers, etc.

During the investigation, law enforcement officers established the involvement of one of the offenders in the illicit trafficking of weapons. In the personal car of the offender, border guards found an arsenal of weapons, that consisted of grenades F-1, smoke checkers, signal missiles and almost 300 ammunition to the Kalashnikov rifle.

Police to step up patrol at Malaysia-Thai border

The Royal Malaysia Police (PDRM) has stepped up patrol in areas bordering Thailand to prevent the illegal entry of the Uighur people who had escaped from an Immigration detention centre in southern Thailand into Malaysia.

Inspector-General of Police Tan Sri Mohamad Fuzi Harun said security measures were also taken by the army in the border areas of Kedah, Kelantan and Perak.

"We do no rule out the possibility of them (Uighur people) trying to sneak into the country and we have taken action by stepping up border patrol , especially along the Thai border," he said when contacted by Bernama here today.

Mohamad Fuzi said PDRM would extend its full cooperation to the Thai authorities in sending back the Uighurs.

Singapore, Malaysia bust Internet love scam syndicate in cross-border ops

A total of 14 suspects were arrested in Malaysia and Singapore in a cross-border operation against an Internet love scam syndicate, the police said.

Ten Africans were among 11 people picked up in Kuala Lumpur by the Commercial Crime Investigation Department (CCID) of the Royal Malaysia Police in an operation recently held.

Simultaneously, Singapore Police's Commercial Affairs Department (CAD) arrested three Singaporean men for assisting to transfer the syndicate's

benefits from the criminal conduct.

According to the statement, the suspects are believed to be responsible for at least 7 cases reported in Singapore and 25 cases reported in Malaysia. Victims lost approximately S$245,000 in these cases.

Indonesia tightens border security following Marawi liberation declaration

Indonesian authorities have tightened security in some areas bordering the Philippines and at the Philippine mission in Jakarta following Manila's declaration that its southern city of Marawi has been liberated from pro-Islamic State militants.

Philippine President Rodrigo Duterte made the declaration Tuesday after two commanders of the rebel alliance were killed. Marawi had been partly held by fighters linked to Islamic State since an attack in May.

Indonesia's National Police Chief Gen. Tito Karnavian told a press conference Thursday that the deaths of Isnilon Hapilon and Omarkhayam Maute, as well as the liberation of Syria's northern city of Raqqa from Islamic State militants by U.S.-backed Syrian forces have taken a toll on the IS terrorist network.

He warned, however, that the militants

who have not been killed may still try to escape, with as many as 100 militants still at large in the southern Philippines. He added that some Indonesians are among the jihadists in Syria and Marawi.

Illegal work organisers targeted in WA and QLD operations

The Australian Border Force (ABF) has executed a series of Taskforce Cadena-related warrants on properties in Queensland and Western Australia, targeting labour hire intermediaries (LHI) providing illegal farm workers.

Taskforce Cadena is a joint agency initiative between the Department of Immigration and Border Protection (DIBP), led by its operational arm the ABF, and the Fair Work Ombudsman (FWO).

An additional 13 people of interest were also located at the property, comprising a mix of non-citizens from PNG and the Solomon Islands, most suspected of working in breach of their visa conditions and likely to have their visas cancelled, and one residing and working illegally in Australia who has been detained ahead of his removal.

Canberra man arrested following 356kg ecstasy importation

A joint Australian Federal Police (AFP), ACT Policing and Australian Border Force (ABF) operation yesterday (5 December 2017) resulted in the arrest of a 23-year-old Canberra man, following the detection of 356kg of MDMA at a Sydney air cargo facility.

The investigation began in May 2017 when ABF officers intercepted an airfreight consignment from Germany, destined for an address in Fyshwick, Canberra. The consignment contained 144 buckets labelled as chlorine, concealing bags of a white crystalline substance. A presumptive test indicated a positive reaction to methylenedioxy-methamphetamine (MDMA).

AFP officers seized the consignment and forensic testing confirmed the total weight of MDMA concealed in the consignment was 356kg. This has the potential to produce over 1.2 million tablets with an estimated street value up to $40.5 million dollars.

Spain migrant crisis: Calls for Ceuta border fence to be reinforced

Spanish police have called for a border fence to be reinforced as they coming under huge pressure to protect an enclave in North Africa.

The Civil Guard Command in Ceuta say they have been overwhelmed by the rising numbers of migrants trying to jump the border fence into the region.

And some officers have even been attacked as they try to prevent illegal border crossings.

Data reveals there has been a huge increase in new arrivals in Ceuta - with agents intercepting 2,661 migrants since October 2016, a rise of 71 per cent over the previous 12 months.

THE MOST ENGAGING DISCUSSIONS IN BORDER MANAGEMENT

■ EVENT UPDATE

**20th-22nd March 2018
Madrid, Spain**
www.world-border-congress.com

World Border Security Congress Congress Programme recently announced the preliminary congress programme for the 2018 event.

The international border security community gathers in Madrid, Spain on 20th-22nd March 2018 to discuss the latest issues, challenges and solutions facing the industry.

The past few years has seen unprecedented crisis on a global scale, from the Middle East warring factions creating mass refugee movements across Europe, illegal economic migrants from Africa and Asia have created increasing challenges for the international border management and security community.

As the global migration crisis continues, the challenges faced by the global border management community show little sign of abating. As the war against IS in Iraq, Syria and Libya approaches

its conclusion, returning IS fighters will continue to exploit the crisis to infiltrate fighters into Europe, the USA and elsewhere. Borders in the Middle East and Africa remain porous and will continue to provide challenges.

Human traffickers especially use the crisis and the opportunities it affords to maximise their trade in human misery.

International organised criminal gangs continue to thrive with both drug and human traffickers utilising the dark web and new technology to assist their activities.

It must be the aim of every border management agency to continuously improve and evolve to meet the challenges of future by fully embracing technology and taking every opportunity to meet, share and co-operate!

We need to continue the discussion, collaboration and intelligence sharing.

Supported by the Organisation for Security & Cooperation in Europe (OSCE), the European Association of Airport and Seaport Police (EAASP), National Security & Resilience Consortium, International Security Industry Organisation and International Association of CIP Professionals, the World Border Security Congress is the premier multi-jurisdictional global platform where the border protection policy-makers, management and practitioners together with security industry professionals, convene to discuss the international challenges faced in protecting borders.

The Congress programme will deliver high level discussions and a series of Closed Agency Only Workshops for promoting greater collaboration on the international challenges.

On behalf of the Organising Committee, you are cordially invited to **Madrid, Spain on 20th-22nd March 2018** for World Border Security Congress, the premier annual gathering of border and migration management professionals.

ENHANCING BORDER SECURITY THROUGH CONSTRUCTIVE DIALOGUE

Topics of discussion at the 2018 World Border Security Congress will cover:

Identifying and understanding the latest and evolving threats and challenges for border agencies

What are the latest developing threats and challenge of keeping people and trade moving whilst enhancing security in the terrorist age -Safety-Security and Speed

Foreign fighters and counter-terrorism strategies at the border

As more and more foreign fighters return from the conflict zones of the Middle East, what are the current and future strategies to identify and impede the flow of foreign terrorists, such as the adoption of API and PNR. What are the profiling and behavioural indicators for identifying foreign terrorist fighters and how do we stay ahead of the game?

Implementation of Advance Passenger Information

Advancing the use of API and PNR, bridging the gaps that prevent full exploitation of the significant advantages these systems offer for improved border management.

2017/18 Border Security Challenges:
– Migration Crisis Tests European Consensus and Governance
– Migrants and refugees streaming into Europe from Africa, the Middle East, and South Asia
– Big Business of Smuggling Enables Mass Movement of People for Enormous Profits
– Climate Change and Natural Disasters Displace Millions, Affect Migration Flows
– Rohingya refugee crisis grows in Asia
– Tackling Southeast Asia's Migration Challenge
– ISIS threat grows in Asia, threatening to send 500,000 migrants to Europe
– Border Skirmishes Resonate in National Domestic Politics
– Women's Labour Migration from Asia and the Pacific

Coordinating Coastal and Maritime Border Surveillance

Proper and efficient co-ordination of maritime, coastal, port and land border surveillance systems is essential in securing national borders. How is this best achieved across multiple agencies and what systems are needed to do the job?

Big Data and how to use it at the border

With massive amounts of data from legacy systems, sharing info from others. How do you get info out of silos and used in collaboration. How can social media be best used to identify and detect threats.

Counter-Strategies for Human and Drug Trafficking

What are the most effective strategies and what other strategies and technologies need to be employed for disrupting the global trade in drugs and human beings that flow towards the developed world

Surveillance Systems and Technologies on the Border

How far are we from the development and implementation of future technologies for really smart border control? What are the technology gaps and how do we close them?

Future trends in International Border Management

The border community are facing extraordinary set of challenges in the increasingly globalised world of the early 21st century. What are the changes and trends in border management that will equip us to meet the challenges of today and the challenges of the future?

Further details on the full programme and registration to attend the Congress in Madrid in March 2018 can be found at **www.world-border-congress.com**.

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

We need to continue the discussion, collaboration and intelligence sharing.

The World Border Security Congress is the premier multi-jurisdictional transnational platform where the border protection, management and security industry policy-makers and practitioners convene to discuss the international challenges faced in protecting borders.

The Full Preliminary Congress Programme guide (pdf version) can be downloaded direct from the World Border Security Congress website **www.world-border-congress.com/PSG**

Silver Sponsor:

S2 GLOBAL
An OSI Systems Company

CLOSED AGENCY ONLY WORKSHOPS

FOR BORDER AGENCIES AND AGENCIES AT THE BORDER ONLY – If you are interested in participating in the Closed Agency Only Workshops, in order to obtain clearance to attend the Closed Workshops, please register via the Online Agency Registration complete the Agency Registration Form to begin the approval process.

If you have any queries please contact Neil Walker, Event Director, World Border Security Congress at neilw@world-border-congress. com.

The World Border Security Congress aims to promote collaboration, inter-agency cooperation and information/intelligence sharing amongst border agencies and agencies at the border to better engage and tackle the increasing threats and cross border security challenges that pertain to today's global environment.

Border agencies and agencies at the border can benefit from the 'Closed Agency Only Workshops', hosted by the Organization for Security & Co-operation in Europe (OSCE) and the International Organization for Migration (IOM), with a series of behind closed door discussion and working group opportunities.

This years Closed Agency Only Workshop topics are:

Challenges in the Mediterranean
"How are the multiple challenges faced by authorities in the Mediterranean being tackled? As high levels of economic migration, THB and trafficking in cultural property continue or grow, can the enhanced use of 'risk analysis capacities' help us meet the challenges?"
Chair: OSCE

Ensuring international funding/support reaches the hotspots
Poor border management in one country has immediate impact on its neighbours especially in parts of Africa and Central Asia. Helping poorer countries struggling with border management issues is therefore an act of enlightened self-interest. Ensuring the funds available reach the border hotspots is essential.
Chair: IOM

Information Exchange - the way forward
Everyone agrees that the sharing information, such as national/ international databases, and intelligence is essential for secure borders. How do we implement the systems and build the trust to make this a viable?

Madrid Marriott Auditorium Hotel & Conference Center

Avenida de Aragon No 400
Madrid 28022, Spain
www.marriott.com

Accommodation online booking:
www.world-border-congress. com/hotelonline

Part of the Principe Felipe Conference Centre, the 4-star Madrid Marriott Auditorium Hotel & Conference Center is within 10 minutes of the Madrid-Barajas Airport and lies 10 km from downtown and 4 km from the shopping malls.

All the rooms are equipped with mini bar, safe, telephone, air conditioning, satellite TV and internet access.

The Madrid Marriott Auditorium Hotel & Conference Center is an ideal venue for the World Border Security Congress with excellent conference facilities, as well as additional services and functions rooms.

Special Accommodation Rates for Attendees to the World Border Security Congress

The World Border Security Congress has negotiated special discounted rates for delegates to stay at the hotel.

eGates from secunet for faster border control at Vienna International Airport

The airport in Vienna is one of the key hubs to Eastern Europe, and it now relies on automated border control systems (eGates) from secunet. A total of 25 eGates were installed in December and have now been put into operation, ensuring convenient and efficient border control.

The implementation of biometrics-based eGates means that passengers can now expect shorter transfer times as well as faster arrivals and departures at Vienna airport. This is because passengers pass through the control gates autonomously, so checks can be performed in parallel. The entire process takes just a few seconds - from placing the electronic passport on the ID reader for an optical and electronic check of security features, to exiting the gate.

While the experience of crossing the border is more pleasant and quicker for passengers, border control officers are comprehensively supported in their sovereign responsibilities by means of intuitive monitoring. Integrated, sophisticated document verification, high-performance biometric procedures, and smart sensors ensure the same high level of security which is achieved with stationary border control. The secunet easygate is based on open standards, meaning that it can be flexibly adapted to future changes and expansions.

The overall system for border control initially consists of 25 control gates, of which 16 are available for departures and nine for arrivals. In addition to training, support, and maintenance, the company is also delivering software for monitoring, evaluation and administration workstations, and a centralised server system for connecting peripheral systems and controlling the eGates.

Vision-Box implement paperless biometric self-boarding solution to expedite passenger flow and improve traveler experience

Los Angeles Airport is trialing an advanced biometric self-boarding solution by Vision-Box to clear travelers flying out of the USA in a contactless, quick and secure way.

The new passenger flow solution allows travelers to board their aircraft in just a few seconds simply by looking into a high-resolution face capture system at the traveler-friendly flow-control gateway. No need to present their travel document or boarding pass anymore. The system deployed by Vision-Box captures a live, high quality image of the traveler's unique biometric facial traits, for US Customs and Border Protection to match it against the passenger's file containing the digital facial token captured at the initial immigration process. This process permits as well to virtualize the process of sending the boarding-pass details to the Airline Departure Control System, using face as a token to reconcile the passenger and his flight. After assuring the identity and eligibility of the passenger on that specific flight, the gateway then opens and the traveler can swiftly board the aircraft.

WCC Joins the Secure Identity Alliance as an Advisory Observer

The Secure Identity Alliance, the global identity and secure eServices advisory body, today announces that WCC, a world leading developer of advanced search and match technology and solutions, has joined the Association as an Advisory Observer.

With over two decades of experience in the industry, Sanjay Dharwadker is an expert voice on identity, biographic data and digital identity topics at a variety of global bodies and organizations, including the International Organization for Standardization (ISO), the European Committee for Standardization (CEN) and the International Civil Aviation Organization (ICAO).

He is also involved in enabling new generation identity solutions that address the United Nations' (UN) ambitious Sustainable Development Goals (SDGs), which include a target of zero statelessness for all global citizens by 2024 and legal identity for all by 2030.

"Identity is a complex matter that involves multiple stakeholders and requires adherence to national and international laws – especially privacy laws," comments Sanjay Dharwadker. "Our goal is to provide insights that will help enable the Secure Identity Alliance and its members address the challenges of enabling civil registration and legal ID for citizens around the globe. By transforming diverse ideas into concrete solutions, the ID industry will then be able to help ensure that people everywhere in the world can benefit from the empowerment and prosperity that comes with having a legal and verifiable civil identity."

ADVERTISING SALES

World Border Security Congress

20th-22nd March 2018
Madrid, Spain

www.world-border-congress.com

The World's most engaging event and discussion...

Enhancing Border Security Through Constructive Dialogue

The world is experiencing the largest migration movement in history, with challenges for the border management and security community, as little sign of peace and security in the Middle East is apparent and porous borders in Africa and Asia continue to provide challenges.

International organised criminal gangs and human and drug trafficking groups exploit opportunities and increasingly use the internet and technology to enhance their activities.

Controlling and managing international borders in the 21st Century continues to challenge the border control and immigration agencies around the world. It is generally agreed that in a globalised world borders should be as open as possible, but threats continue to remain in ever evolving circumstances and situations.

Advancements in technology are assisting in the battle to maintain safe and secure international travel. 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.
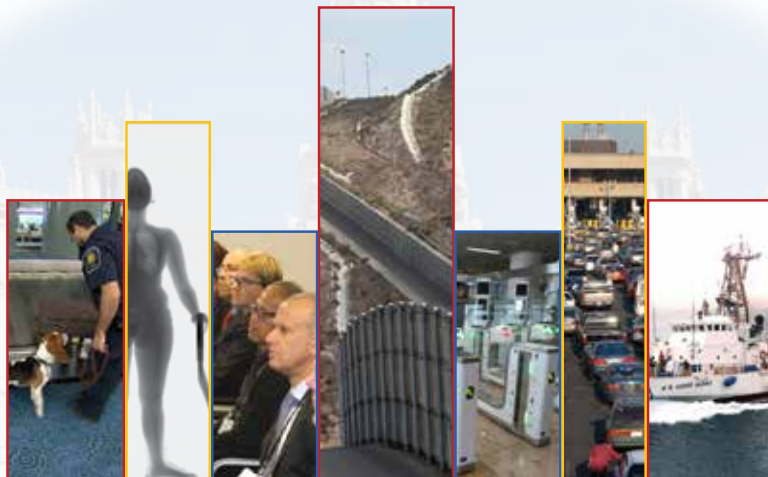
ONLINE REGISTRATION OPEN

For further details and to register online: www.world-border-congress.com/registration

Join us in Madrid, Spain on 20th-22nd March 2018 for the next gathering of border and migration management professionals.

www.world-border-congress.com

Speakers include:
- Dr Enrique Belda, Deputy Director General of Information Systems and Communications for Security Secretary of State for Security, Ministry of Interior, Spain
- Rasa Ostrauskaite, Director, Transnational Threats Department, OSCE
- James Douglass, President, European Association of Airport & Seaport Police
- Alvaro Rodríguez Gaya, Head of Strategy of Europol's European Migrant Smuggling Centre (EMSC), EUROPOL
- Paul Broadbent, Chief Executive, UK Gangmasters and Labour Abuse Authority
- Thomas Wuchte, Executive Secretary, International Institute for Justice and the Rule of Law

...for the international border management and security industry

Supported by:

OSCE Organization for Security and Co-operation in Europe | European Association of Airport and Seaport Police | ISIO - International Security Industry Organisation | International Association of CIP Professionals | NS&RC

Media Partners:

BORDER SECURITY REPORT | WORLD SECURITY REPORT | World Security-index.com