

**INCORPORATING**

**BORDER SECURITY  
REPORT**

# **WORLD SECURITY REPORT**

Official Magazine of



International Association of  
**CIP Professionals**

MARCH / APRIL 2018  
[www.worldsecurity-index.com](http://www.worldsecurity-index.com)

**FEATURE:**

**Making Our Critical  
Infrastructures More  
Resilient: Best Practices**

PAGE 9

**FEATURE:**

**Business interruption and  
cyber incidents dominate risk  
landscape for companies of  
all sizes and sectors in 2018**

PAGE 12

**FEATURE:**

**To Protect and Protect Again**

PAGE 16



**COVER STORY**

**SECURING COMMUNICATIONS AT A TIME  
OF 'EXTREME EVENTS'**



**critical infrastructure**  
PROTECTION & RESILIENCE ASIA

17<sup>th</sup>-19<sup>th</sup> July 2018

Sarawak, Malaysia

www.cip-asia.com

*Developing resilient infrastructure for a secure future*

# Register Today

The 3rd Critical Infrastructure Protection and Resilience Asia will bring together leading stakeholders from industry, operators, agencies and governments to collaborate on securing Asia.

Southeast Asia has seen a rise in insurgency-related attacks and terrorist activities, creating uncertainty and insecurity on critical national infrastructure.

Climate change has also seen more extreme weather patterns, creating additional hazardous, unseasonal and unpredictable conditions and a severe strain on infrastructure.

The conference will look at developing existing national or international legal and technical frameworks, integrating good risk management, strategic planning and implementation.

*Be part of the discussion - and solution!*

Register online at [www.cip-asia.com](http://www.cip-asia.com)

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

Owned & Organised by:



Media Partners:



Supporting Organisations:



Strategic Partner:



In Partnership With:



## Latest Confirmed Speakers include:

- Ir. Md Shah Nuri Md Zain, Chief Executive, National Cyber Security Agency (NACSA), Malaysia
- Dato Dr Chai Khin Chung, Director, State Security Unit, Sarawak, Malaysia
- Franz-Josef Schneiders, Head of Division, Federal Ministry of Transport and Digital Infrastructure, Germany
- Oliver Carlos G. Odulio, VP, Head of Asset Protection & Risk Management, PLDT Inc, Philippines
- Elli Pagourtzi, Project Manager, Security for Security Studies (KEMEA), Hellenic Ministry of Interior, Greece
- Bill Hutchison, Honorary Professor, Security Research Institute, Edith Cowan University, Australia
- Dato' Dr. Haji Amirudin Bin Abdul Wahab, Chief Executive Officer, CyberSecurity Malaysia
- Bill Bailey, Regional Director Australasia, International Association of CIP Professionals (IACIPP), Australia
- Nur Ilyia Roslan, Researcher, Cybersecurity Malaysia
- Senior Representative, Cyber Security Centre, Universiti Pertahanan Nasional Malaysia
- Senior Representative, Sarawak Energy, Malaysia
- Norhamadi bin Ja'afar, Senior Executive, CyberSecurity Malaysia

For full conference programme visit [www.cip-asia.com](http://www.cip-asia.com)

# FLORIDA: WHAT PRICE TOO HIGH?



As another US school suffers the appalling human tragedy of a mass shooting, it would be strange if I were not to mention it in this month's issue. But the reality is, much of what I would say on the subject has already been said after previous shootings and nothing's changed.

One can only wonder at the useless platitudes offered by President Trump and other politicians, who talk about "no teacher, no child should ever be in danger in an American school" and that "no child is alone, we will protect you" but then in an astonishing piece of deflection, switches the conversation and blame to the need to tackle

mental health issues in the US. As if it is mental health that killed 17 people and injured 15 others and not a 'troubled' individual armed with a legally obtained AR-15 assault rifle, one of the world's most efficient killing machines.

In a sort of 'Emperors new clothes' moment politicians and gun supporters alike indulge in a mass self-delusion, where they ignore all statistics and kid themselves that it is not the availability of guns that's the problem, but that it is a social problem.

They say that if we put the proper checks in place and monitor properly individuals that are showing signs of mental health issues, then the problem will be solved. After all, Cruz was flagged up as a risk on numerous occasions.

They ignore that fact that every society around the world has problems with mental health issues, but they do not have the same problem with mass shootings. The missing element in the equation is that the mentally ill are not usually armed with assault rifles.

It also quietly ignores that fact that next year and every year after that, tens of thousands of gun owners in the US will be affected by previously undiagnosed mental health issues that may not be immediately apparent to family, friends and colleagues. Other gun owners will be angry, stressed out, jealous, fanatical or just plum mad!

The reality is that those people in the US that like their guns, will continue to come up with arguments to support gun ownership, aided by politicians that want their votes, and the mass killings continue. Only when the price becomes too high will something change, but nobody knows yet what constitutes 'too high'?

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/WSRMAR18](http://www.torchmarketing.co.uk/WSRMAR18)

[www.worldsecurity-index.com](http://www.worldsecurity-index.com)

### Editorial:

Tony Kingham  
E: [tony.kingham@knmmedia.com](mailto:tony.kingham@knmmedia.com)

### Contributing Editorial:

Neil Walker  
E: [neilw@torchmarketing.co.uk](mailto:neilw@torchmarketing.co.uk)

### Design, Marketing & Production:

Neil Walker  
E: [neilw@torchmarketing.co.uk](mailto:neilw@torchmarketing.co.uk)

### Subscriptions:

Tony Kingham  
E: [tony.kingham@knmmedia.com](mailto:tony.kingham@knmmedia.com)

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



Copyright of KNM Media and Torch Marketing.



20<sup>th</sup>-22<sup>nd</sup> Mar 2018  
Madrid, Spain

[www.world-border-congress.com](http://www.world-border-congress.com)



17<sup>th</sup>-19<sup>th</sup> July 2018

Sarawak,  
Malaysia

[www.cip-asia.com](http://www.cip-asia.com)



2<sup>nd</sup>-4<sup>th</sup> Oct  
2018  
The Hague,  
Netherlands

[www.cipre-expo.com](http://www.cipre-expo.com)



4<sup>th</sup>-6<sup>th</sup> Dec 2018

Orlando  
Florida, USA

[www.ciprna-expo.com](http://www.ciprna-expo.com)

## Securing communications at a time of 'extreme events'



The first duty of any government is to provide for the security and safety of its citizens!

In historically, that would mean defending the population against aggressive neighbouring tribes and nations. Not much if anything would or could have been done to protect the population against natural disasters, like earthquakes, floods, famine or disease. These would be seen as acts of god, punishment for some imagined or real wrongdoings!

Today, in the technological age we have changed our view of what's possible and therefore what we expect from our governments. We now expect governments to protect us from any hazard, whether it is from this world and beyond!

Natural disasters still pose the greatest threat to life and property and sadly the world seems to have experienced plenty of those in recent years including tsunamis, floods, hurricanes galore, volcano's, volcanic ash clouds, earthquakes and pandemics.

But then of course there are what seem like more remote possibilities of 'extreme events', which could

result in major global disasters that could affect everyone on the planet. They may seem more remote, but they are in fact, inevitable!

So, what are we talking about when we talk about 'extreme events'?

Meteor strikes, such as the so-called Tunguska event in Russia in 1908 that caused an explosion that knocked over an estimated 80 million trees covering 2,150 square kilometres.

More recently, in 2013 150-foot asteroid (designated D14) hurtled past the earth coming within 17,150 miles, closer than some of our own satellites. A near miss by

space standards.

Whilst not big enough to cause an extinction event, had D14 hit the earth, weighing in at 143,000-ton, it would have done incredible damage, releasing the energy equivalent of 2.4 million tons of TNT and wiping out 750 square miles of territory (1,942 square kilometres).

Caught on camera and only a few hours apart from D14's fly-by, a meteor exploded spectacularly above Russia's Ural Mountains. The experts say it was a co-incidence. And we have no reason to doubt it but the real issue is that we were powerless to prevent either of them.

The most disturbing thing about Asteroid D14 is that the was only identified one year prior to it buzzing the planet. So, what other unexpected and unwelcome guest could already be on their way?

Another extreme event are so-called supervolcano's. Supervolcano's are those volcano's that have in their history had eruptions that measure 8 on the Volcanic Explosivity Index, (VEI). They are not typically the single volcanic cone, instead are usually characterized by a large caldera, or depression, that was formed during past explosive eruptions. Should they erupt they have the potential to throw in excess of one thousand cubic kilometers of volcanic debris up into the atmosphere causing massive destruction, not just in the immediate locality, but regionally and possibly even globally.

Yellowstone in the US is probably the most well-known example and is still extremely active as millions of tourists can tell you. Some scientists believe Yellowstone has been on a regular eruption cycle of around 600,000 years. The last eruption was 640,000 years ago.

VEI7 eruptions are not quite supervolcano's but are still massive and but more frequent. The Mount Tambora eruption took place in Indonesia in 1815, and as a result, 1816 became known as the 'Year Without a Summer'. Again, in Indonesia, Mount Rinjani erupted in 1257 possibly triggering a little ice age.

Then there's Campi Flegrei, under the Bay of Naples, which is the bookies favourite as the most likely to erupt. Whilst not as big as some of the others the entire caldera keeps swelling and deflating, and scientists are really not sure why. What this activity does indicate is that an active magmatic system exists and a recent scientists report in the journal Nature Communications said it could be ready for an eruption. No one can say with any certainty that it will erupt, but it's likely that it will.



That brings us neatly to tsunamis. Tsunami's are caused by events such as earthquakes like the one on 26 December 2014 killing between 230,000–280,000 people in 14 countries. The third-largest earthquake ever recorded. Other causes can be volcanic eruptions, landslides, glacier calving, meteorite impacts and other disturbances above or below water. Whilst some argue that tsunami's are not considered extreme events in themselves, but are in fact the consequence of other events...but that's just semantics. The death toll indicates otherwise.

Another scenario, is the solar flare and its big brother, a coronal mass ejection (CME).

On September 6th of this year the sun unleashed two monster solar storms, the second of which was the most powerful we've seen in more than a decade. The burst of radiation was so intense, it caused high-frequency radio blackouts across the daytime side of earth that lasted for about an hour. These solar storms can release as much energy as a billion hydrogen bombs.

But there is something that will have even more impact for us here on earth, which is the coronal mass ejection. These solar explosions propel bursts of particles and electromagnetic fluctuations into earth's atmosphere. Those fluctuations are something like an Electro Magnetic Pulse, causing electric fluctuations at ground level that could fuse conductive wires, down communications and blow out transformers in power grids. A CME's particles also have the potential to take out satellites and aircraft.

Then of course in addition to natural disasters, there's man kinds ability to create its own disasters.

Although the threat of conventional war in the developed world has receded (though not disappeared),

other threats have emerged. As we have witnessed recently, rogue states like North Korea now poses the ability to deliver nuclear attacks via inter-continental ballistic missiles.

Global terrorists like ISIS and al-Qaeda have potential to deliver mass destruction through the use of modern technology like dirty bombs, chemical attacks, cyber-attacks, WMD and maybe one-day nuclear weapons.

Industrial disasters such as the those at Bhopal in India and Chernobyl in Russia are also obvious examples of unexpected home-grown disasters that can strike us at any time.

Then there's the cascade effect of a natural disaster causing a man-made disaster, like the earthquake that caused the tsunami that caused the Fukushima nuclear disaster.

Whatever the threat or disaster, it is the ability of the authorities to organise and move the available resources to the point of most need that is the key to managing the disaster effectively. Whether it's for search and rescue, medical assistance, shelter, sustenance or law and order; fundamental to the principle of good organisation is good reliable and resilient communications.

Good communications are taken for granted and we are increasingly dependent on them for the necessities of life, from our livelihoods to the weekly shopping delivery.

Most of those communications are being relayed over the existing Public Switched Telephone System (PSTN) infrastructure. Quite apart from all landline telephone calls, virtually all computer information is already relayed via the PSTN and the proliferation of technologies like Voice over Internet Protocol (VoIP) as a first choice for individuals and businesses will only

increase our dependence on the existing infrastructure.

Few communications systems are completely reliable, they rely on a whole load of interconnections and interdependencies, as well as a power source. Communications tend to rely on other infrastructure, such as road, rail and bridges. So, flooding can cause a bridge collapse and that can cause local communications failures. These potential points of failure are often unidentified until it is too late.

In the event of a major disaster, although a complete national failure of the telecommunications system is unlikely, local communications failure or serious degradation of service within the disaster area is probable, due to damage to infrastructure, loss of power or simple overload. Mobile systems are particularly vulnerable to overload.



**critical infrastructure**  
PROTECTION AND RESILIENCE EUROPE

**critical infrastructure**  
PROTECTION AND RESILIENCE EUROPE

**2<sup>nd</sup>-4<sup>th</sup> October 2018**  
The Hague, Netherlands  
[www.cipre-expo.com](http://www.cipre-expo.com)

**SAVE THE DATES**  
**Working together for enhancing security**

**CALL FOR PAPERS NOW OPEN** - visit [www.cipre-expo.com](http://www.cipre-expo.com) for details

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

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

[www.cipre-expo.com](http://www.cipre-expo.com)



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

Owned & Organised by:  

Hosted by: 

Supporting Organisations:     

Media Partners:  



So here are 3 good examples of what has been done to keep the phones ringing.

Researchers then from the University of the Philippines, Electrical and Electronics Engineering Institute (UP EEEI), with support from the Department of Science and Technology (DOST), addressed this problem by developing a technology that restores basic communication services in the aftermath of disasters. The 'ROGER' System or RObust and Rapidly Deployable GSM Based Stations and Backhaul for Emergency Response System is an intervention that aims to provide emergency responders and affected communities with a reliable communication system during relief, rescue, and recovery efforts in case conventional communication channels (i.e. commercial telecommunications companies) go down. This technology is in "standby mode" in disaster-stricken area, and can be "unpacked" on site after the disaster. It is expected to provide a canopy of 2G coverage that will allow early responders with ROGER SIM cards to communicate and coordinate with one another.

The main components of the ROGER System are the IP Backhaul, the Base Station, and the Power Supply. The IP Backhaul is a point-to-point, long range wireless backhaul that links the GSM cell hoisted in the disaster-stricken area to the disaster command centre by utilizing IEEE 802.11 WiFi and TV white space (TVWS). The TVWS is an underutilized spectrum of the existing communication channel. The GSM Base Station, on hand, contains the so-called heart of the ROGER System, which is a software-defined radio (SDR) that runs on open source software and an IP-based network. It mimics the functionality of a traditional cellular/GSM base station. Simply put, the GSM Base Station provides cellular phone signal to allow calls and texts for phones with provided ROGER SIM cards. Within the ROGER network, authorized users can

use their regular mobile phones to place calls to one another or to an emergency hotline. If interconnection to the commercial phone and cellular networks are still in place, users may call other people outside the ROGER network. The entire ROGER system is designed to be solar-powered, but a generator set is also set up as backup power source in case there is not enough solar energy for approximately three consecutive days. The ROGER System will be dismantled immediately once conventional GSM communication services have been restored.

Satellite communication, already used routinely by the military, is another obvious option.

To this end the Luxembourg government launched emergency.lu a Rapid Response Kit satellite communications system. The system consists of satellite infrastructure and capacity, broadband and voice communication and satellite ground terminals as well as transportation equipment. The system has already been widely deployed effectively after natural disasters around the world including during the aftermath of Hurricane Irma earlier this year. This system has been designed primarily for use in disasters overseas, but presumably could just as easily be deployed for a local disaster, if enough kits are available? However, it is not pre-positioned, so relies on the transport infrastructure to be deployed.

The UK Government believes the most likely of extreme event is in fact the solar flare or coronal mass ejection, which has the potential to damage or degrade existing terrestrial telecommunication and commercial satellite communications.

To guard against this eventuality and ensure that the UK

Government and emergency services are able to effectively respond to the situation, the UK has developed the High Integrity Telecommunications System or HITS.

HITS was developed by the UK Government's, Civil Contingencies Secretariat (CCS) in a partnership with Astrium and the UK Ministry of Defence (MOD).

The CCS is part of the UK Government's Cabinet Office and works across Government and industry to improve the ability of the UK to respond to and recover from significant emergency events.

Astrium is the prime contractor for the Skynet 5 contract with the UK Ministry of Defence. This program provides all secure voice, data, video, internet and broadcast communications for UK armed forces operating anywhere overseas.

They own and operate military hardened satellites that are resistant to any known attack and have both onboard and ground based technology to overcome the interference threat posed by high solar flare activity.

So, what is it? HITS is a secure and resilient satellite-based communications system capable of delivering secure data and telecommunications completely independently from the main UK telephone network.

The system is designed to provide telephone and internet communications to the emergency services and related agencies in the event of a national emergency when the existing landline or mobile networks are either down or seriously degraded.

It is however completely interoperable with those parts of the regular networks that are still functioning so will facilitate the break-out of calls onto other networks such as mobile phones.

It is installed at the Central Government Crisis Management Facilities, COBR, and at each of the UK's Devolved Administrations Crisis Management Centres. It is deployed at fixed sites across the UK, mainly in Police Strategic Command Centres (SCCs) because the Police usually the lead service in times of emergency.

Every HITS installation comes with a number of phones and laptops, usually three of each, as well as at least one networked printer.

In addition to the core network sites, each Police Force Area will also have at least one pre-determined fall-back location, where HITS Transportable Terminals are deployed. These fall-back locations are designed as an extra level of communication security should any of the main HITS installations be within the disaster area and so be unavailable as a result.

These Transportable Terminals can be deployed anywhere in England and Wales and will usually be driven to the relevant location although they can be carried by whatever transport is available.

They are on call 24/7 and can be on the road within 6 hours of an emergency call out by the Cabinet Office.

Each transportable unit comes with up to 10 digital phones and laptops, so that they can effectively act as a mobile command centre wherever it's needed. They are equipped with their own generators and fuel, so are able to operate fully autonomously for up to seven days. Each of them has trained Astrium personnel on hand to support the emergency services throughout the deployment.

Whether it is satellite or GSM communication, in an 'extreme event' pre-positioning of communications equipment (and other supplies) as much as is practicable, is the key to effectiveness.

After all, if you rely on a system that depends on the transport infrastructure to get to the point of most need, haven't you already set it up to fail?

*Tony Kingham*  
Editor





# Making Our Critical Infrastructures More Resilient: Best Practices



Today, our national critical infrastructures (CI) are more vulnerable than ever before and high-impact disruptions are no more rare or and low-probability events. In that regard, CIP (Critical Infrastructure Protection) discipline has already become one of the leading topics in the policy makers' agenda and any threats against our CI systems, which could be considered as the "lifelines" of the nations, are perceived as "threats to national security". In that sense, with respect to evolving and sophisticated dynamics of natural and man-made threats, it is undeniable that almost every state has started to implement its national CIP policies.

Despite its criticality, the concept of "Critical Infrastructure Resilience" (CIR) had been mostly underestimated and only in the last five years it gained much more attention especially in the field of homeland security and civil protection practices. Especially as a response to the new emerging threats in the "age of uncertainty", it is possible to observe that many national security strategies have already adopted risk based "all hazards" approach with a special focus on the concept of "resiliency".

Nonetheless, it is possible to observe that in general infrastructure planning requirements little references to resilience was made and there is a lack of supporting guidelines which provides a holistic overview how to achieve "more resilient critical infrastructures". Besides, governments and policy makers generally facing challenges regarding

the complex bureaucratic and cross-jurisdictional processes, intensive data requirements, limited technical capacity in planning and investing to the infrastructure resiliency improvement plans.

### Two Distinct Concepts: CIR and CIP

It shall be highlighted that even though both CIP and CIR policies are parts of integrated risk management approaches and strategies, these two concepts are distinct. According to the policy paper released by Italian Association of Critical Infrastructures Experts (AIIC), since there is the tendency to confuse the concepts like security, resilience or risk management, resiliency

could be imagined as a "multifaceted problem"

Figure-1: All Influences All Perspective- A Multifaceted Problem



**Defining “Resilience”**

Resiliency shall be firstly handled as a process not a single outcome. Additionally, since there has been no consensus how to “measure the resiliency”, the concept has also various definitions and it is generally associated with “the ability to bounce or spring back into shape after being pressed or stretched.” In other words, it refers to the ability of a system to resist, absorb, recover from a negative affect and successfully adapt to changing environment. In general, when this definition and understanding is handled with CIP policies, being resilient could be considered with “the capability to cope with severe disruptions which would have negatively impact CI that the CIR framework should operate in a multidisciplinary nature and address technical (logical and physical), organizational, social and economic dimensions of the infrastructures.”

According to the experts, similar to CIP policies, CIR policies also vary according to nations. For instance, in US, PPD-21 (Presidential Policy Directive – Critical Infrastructure Security and Resilience) defines resiliency as “the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incident.” On the other hand, in UK’s Sector Resilience Plan for Critical Infrastructure 2010 document defines the resilience as: “the ability of a system or organization to withstand and recover from adversary.” Another point could be added that for example, while the national policies in US and

Resilience Elements	Infrastructure Management Strategies	Layered Defense Elements
Fault Tolerance	Asset Management	Baseline Structural Design
Adaptive Solutions	Risk and Vulnerability Assessment	Pre-Incident & Evolving Threats, Detection/Prevention/Attribution
Critical Asset Redundancy	Asset Substitution	Incident Preparedness And Response
Mitigation	Disaster Response/ Post Event Recovery	Recovery
<b>LESSONS LEARNED</b>		

Fig. 3 Resource: Volpa, Infrastructure Resiliency: A Risk-Based Framework, Access

Australia recognize CIP as an enabler of CIR by considering “resilience” alongside with the protection and put a special emphasis on the “voluntary” approach, European policies mostly focus on regulatory measures. (1)

Figure-2: Resilience Cycle for the Infrastructure Owner

**Designing the Framework**

According to the experts, since resiliency is not a static concept and derived from principals of multi-layered defense and risk mitigation, the resiliency framework should be based on an “adaptive approach” which is capable to respond today’s complex and dynamic risk environment. According to a well-known resilience specialist Stephen Flynn, resiliency consists of four outcomes: Robustness, resourcefulness, rapid recoverability and adaptability. Very similarly, Volpa’s white paper (Figure-3) about the

“Infrastructure Resiliency: A Risk-Based Framework” states that a resilient infrastructure should be/have:

- Robust and Fault-tolerant
- Adaptable, aware and resourceful
- Functional flexibility and layers of redundant safeguards
- Response and recovery capability for mitigation of event consequences

Figure-3: Infrastructure Resiliency Framework

**Best Practices and Recommendations for CIR policies**

As it was discussed previously, the most challenging part regarding the planning and investing for more resilient critical infrastructures is to identify a comprehensive and globally accepted guideline for implementing best practices. Nonetheless, it is possible to illustrate some recommendations and practical guidelines based on the current approaches.

For instance, a set of five principals were introduced by Deloitte’s report on “Building Resilient Infrastructure” for infrastructure planning as: Identifying the disaster risks, applying robust methodologies for Cost and Benefit Analysis, coordinating-centralizing and

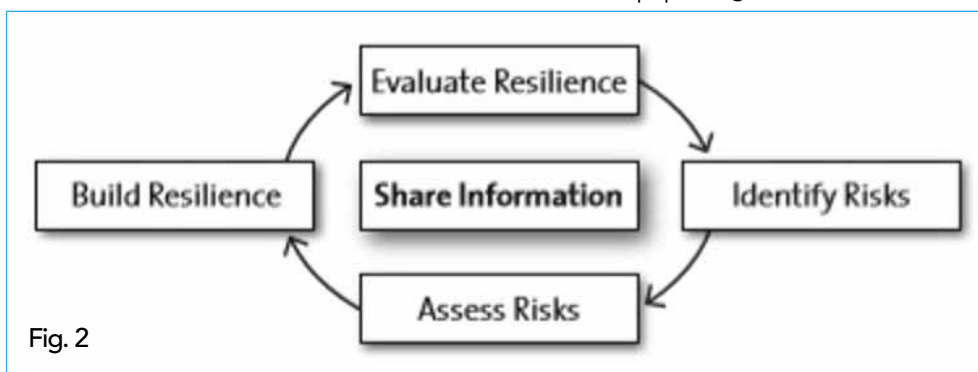


Fig. 2



making the available data for critical data and information, strengthening approval processes and embedding ongoing monitoring of resilience. (2) Besides a few other key points and actionable items in improving the CIR policies are worth to be mentioned:

- Establishing an Effective Public Private Partnership (PPP): In most of the states strengthening the resiliency of critical infrastructure is seemed to be a shared responsibility among public and private sector authorities. In that sense, the business-government partnership remains to be an effective platform especially for exchanging information. In some countries like US or in the European Union level, effective platforms for PPP's have already initiated. For example, in the European Union level, European Public Private Partnership for Resilience (EP3R) which is engaging with National PPP's in building CIR policies can be illustrated.

Figure 4- : Diagram of Infrastructure Stakeholders Involved in Resilience



- Encouraging Information Sharing: As being a useful outcome and the principal value of the PPP's, information sharing is a crucial component of CIR policies which facilitates more informed decision making on how best to protect CI.

Besides, in defending CI, by sharing useful information which shall be distributed in a proper methodology (for ex: traffic light protocols), it is possible to identify critical trends and incidents which could be transform into the actionable recommendations for all actors. Nevertheless, the opportunities and challenges of information sharing process shall be calculated and its "using guideline" should be introduced by policy makers. For instance, establishing ground rules for information exchange and identifying what information could not be shared outside of the partnership shall be determined in advance. Like PPP structure, some countries like US have already implemented information sharing platforms and methodologies. For

instance, The Trusted Information Sharing Network (TISN) for CIR policies was established by Australian Government in 2003.

Finally, in addition to all technical and technological aspects, it shall be kept in mind "cultural" aspects play a crucial role in building national CIR policies and infrastructure problems are also "social". Thus, policy makers should calculate cultural and social dynamics in building CIR policies whether for example they will be voluntary or regulatory to participate. Besides, understanding the networks and going beyond the theoretical aspect by practicing operational resilience should be considered as the cornerstones for achieving a future resilient infrastructure.

*Ms.Ayhan Gücüyener is a Researcher and Regional Director of the International Association of CIP Professionals (IACIPP)*

## Business interruption and cyber incidents dominate risk landscape for companies of all sizes and sectors in 2018



They take aim at the backbone of the connected economy and, when they strike, can jeopardize the success, or even the existence, of companies of every size and sector. Business interruption (# 1 with 42% of responses / # 1 in 2017) and Cyber incidents (# 2 with 40% of responses, up from # 3 in 2017) are this year's top business risks globally, according to the Allianz Risk Barometer 2018.

Larger losses from natural catastrophes (# 3 with 30% of responses, up from # 4 in 2017) are also a rising concern for businesses, with the record-breaking 2017 disaster year also ensuring Climate change and increasing volatility of weather (# 10) appears in the top 10 most important risks for the first time. Meanwhile, the risk impact of New technologies (# 7 2018 / # 10 2017) is one of the biggest climbers, as companies recognize innovations such as artificial intelligence or autonomous mobility could create new liabilities and larger-scale losses, as well as opportunities, in future. Conversely, businesses are less worried about Market developments (# 4 2018 / # 2 2017) than 12 months ago.

These are the key findings of the seventh Allianz Risk Barometer, which is published annually by Allianz Global Corporate & Specialty (AGCS). The 2018 report is based on the insight of a record 1,911 risk experts from 80 countries.

"For the first time, business interruption and cyber risk are neck-and-neck in the Allianz Risk Barometer and these risks are increasingly interlinked," says Chris Fischer Hirs, Chief Executive Officer, AGCS. "Whether resulting from attacks such as WannaCry, or more frequently, system failures, cyber incidents are now a major cause of business interruption for today's networked companies whose primary assets are often data, service platforms or their groups of customers and suppliers. However, last year's severe natural disasters remind us that the impact of perennial perils shouldn't be underestimated either. Risk managers face a highly complex and volatile environment of both traditional business risks and new technology challenges in future."

### New business interruption triggers emerging

Business interruption (BI) is the most important risk for the sixth year in a row, ranking top in 13 countries and the Europe, Asia Pacific, and Africa & Middle East regions. No

business is too small to be impacted. Companies face an increasing number of scenarios, ranging from traditional exposures, such as fire, natural disasters and supply chain disruption, to new triggers stemming from digitalization and interconnectedness that typically come without physical damage, but with high financial loss. Breakdown of core IT systems, terrorism or political violence events, product quality incidents or an unexpected regulatory change can bring businesses to a temporary or prolonged standstill with a devastating effect on revenues.

For the first time, cyber incidents also rank as the most feared BI trigger, according to businesses and risk experts, with BI also considered the largest loss driver after a cyber incident. Cyber risk modeler Cyence, which partners with AGCS and is now part of Guidewire Software, estimates that the average cost impact of a cloud outage lasting more than 12 hours for companies in the financial, healthcare and retail sectors could total \$850 mn in North America and \$700 mn in Europe.

BI also ranks as the second most underestimated risk in the Allianz Risk Barometer. "Businesses can be surprised about the actual cause, scope and financial impact of a disruption and underestimate the complexity of 'getting back to business'. They should continuously fine tune their emergency and business continuity plans to reflect the new BI environment and adequately consider the rising cyber BI threat," says Volker Muench, Global Property and BI expert, AGCS.

### Cyber risks continue to evolve

Cyber incidents continues its upward trend in the Allianz Risk Barometer. Five years ago it ranked # 15. In 2018 it is # 2. Multiple threats such as data breaches, network liability, hacker attacks or cyber BI, ensure it is the top business risk in 11 surveyed countries and the Americas region and # 2 in Europe and Asia Pacific. It also ranks as the most underestimated risk and the major long-term peril.

Recent events such as the WannaCry and Petya ransomware attacks brought significant financial losses to a large

number of businesses. Others, such as the Mirai botnet, the largest-ever distributed denial of service (DDoS) attack on major internet platforms and services in Europe and North America, at the end of 2016, demonstrate the interconnectedness of risks and shared reliance on common internet infrastructure and service providers. On an individual level, recently identified security flaws in computer chips in nearly every modern device reveal the cyber vulnerability of modern societies. The potential for so-called "cyber hurricane" events to occur, where hackers disrupt larger numbers of companies by targeting common infrastructure dependencies, will continue to grow in 2018.

Meanwhile, privacy risk is back in the spotlight following huge data breaches in the US. The introduction of the General Data Protection Regulation (GDPR) across Europe in May 2018 will intensify scrutiny further, bringing the prospect of more, and larger, fines for businesses who do not comply. Time is running out to be GDPR-ready. "Compared to the US where privacy laws have been strict for decades and cyber security and privacy regulation is continuously evolving, firms in Europe now also have to prepare for tougher liabilities and notification requirements. Many businesses will quickly realize that privacy issues can create hard costs once the GDPR is fully implemented," says AGCS's Global Head of Cyber, Emy Donovan. "Past experience has shown that a company's response to a cyber crisis, such as a breach, has a direct impact on the cost, as well as on a company's reputation and market value. This will become even more the case under the GDPR."

Cyber threats also vary according to company size or industry. "Small companies are likely to be crippled if hit with a ransomware



attack, while larger firms are targets of a greater range of threats, such as the DDoS attacks which can overwhelm systems," says Donovan.

Allianz Risk Barometer results show that awareness of the cyber threat is soaring among small- and medium-sized businesses, with a significant jump from # 6 to # 2 for small companies and from # 3 to # 1 for medium-sized companies. With regard to sector exposure, cyber incidents rank top in the Entertainment & Media, Financial Services, Technology and Telecommunications industries.

**Weather and technology risk on the rise**

After a record-breaking \$135 bn in insured losses from natural catastrophes alone in 2017[1] – the highest ever – driven by hurricanes Harvey, Irma and Maria in the United States and the Caribbean, Natural catastrophes returns to the top three business risks globally. "The impact of natural catastrophes goes far beyond the physical damage to structures in the affected areas. As industries become leaner and more connected, natural catastrophes can disrupt a large variety of sectors that might not seem directly affected at first glance around the world," says Ali Shahkarami, Head of Catastrophe Risk Research, AGCS.

Respondents fear 2017 could be a harbinger of increasing intensity and frequency of natural hazards. Climate change/increasing weather volatility is a new entrant in the Risk Barometer top 10 in 2018 and the loss potential for businesses is further exacerbated by rapid urbanization in coastal areas.

Meanwhile, the risk impact of New technologies is one of the big movers in the Allianz Risk Barometer, up to # 7 from # 10. It also ranks as the second top risk for the long-term future

after cyber incidents, with which it is closely interlinked. Vulnerability of automated or even autonomous or self-learning machines to failure or malicious cyber acts, such as extortion or espionage, will increase in future and could have a significant impact if critical infrastructure, such as IT networks or power supply, are involved.

"Although there may be fewer smaller losses due to automation and monitoring minimizing the human error factor, this may be replaced by the potential for large-scale losses, once an incident happens," explains Michael Bruch, Head of Emerging Trends, AGCS. "Businesses also have to prepare for new risks and liabilities as responsibilities shift from human to machine, and therefore to the manufacturer or software supplier. Assignment and coverage of liability will become much more challenging in future."



The ever changing nature of threats, whether natural through climate change, or man-made through terrorism activities, either physical or cyber attacks, means the need to continually review and update policies, practices and technologies to meet these growing demands.

## Call for Papers

**Abstract Submittal Deadline: 30th April 2018**  
**Submit your abstract online at [www.ciprna-expo.com](http://www.ciprna-expo.com)**

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

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

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

For further details visit [www.ciprna-expo.com](http://www.ciprna-expo.com)

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

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

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

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

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

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

Owned & Organised by:

Supporting Organisations:

Media Partners:





## ‘What has been’ and what the future may hold?

John Donlon  
Chairman  
International Association of CIP Professionals  
(IACIPP)

2018 is well underway and hopefully will be a year where we will all see a dramatic reduction in the use of extreme violence carried out through terrorist activity.

The start of a New Year is obviously a good time to reflect on ‘what has been’ and what the future may hold both professionally and personally and this is something that we within the IACIPP have been considering in the context of Critical Infrastructure and Information. What will be the new challenges to be faced and what might we see in terms of new innovations, from both a public and private perspective?

The CIPRNA conference held in December at the Kennedy Space Center in Orlando hosted a broad range of presenters from Government Agencies, Academia and the Private Sector all providing an insight into the complexities of future challenges whether they be from developing physical security, natural disasters or cyber activity.

The threat of physical attacks is unlikely to subside but as may have been expected, the topic generating the most significant debates were those around cyber and its use as a disruptive and destructive tool against our infrastructure and information.

Cyber is already becoming increasingly attractive as such attacks know no borders, physical or virtual, and as we all know are capable of causing serious harm. By way of example, in May 2017 a strain of ransomware called Wannacry spread around the world, breaching the defences of numerous targets (It is estimated that over 200,000 computers in 150 countries were attacked) including public utilities and large corporations. Notably, the attack temporarily crippled National Health Service hospitals and facilities in the United Kingdom, disabling emergency rooms, delaying vital medical procedures and creating chaos for many British patients.

2018 is predicted to see even more sophisticated types of ransomware attacks and the Defence Secretary for the United Kingdom, Gavin Williamson, has warned recently that State actors such as Russia could launch a cyberattack

targeting the UK’s critical energy infrastructure. The Foreign minister for UK cyber security, Lord Ahmed of Wimbledon, has also spoken out about the involvement of Russian military in malicious cyber activity alluding to the fact that UK intelligence agencies have discovered evidence indicating their involvement (UK Media February 2018).

State actors are obviously not the only concern. Recent press reports clearly show that as Islamic State continues to lose physical territory, the group’s supporters are taking the battlefield to cyberspace, targeting critical infrastructure and online Western websites. During 2017, many Western websites, and especially government sites, were hacked by Caliphate Cyber Ghosts, a pro-Islamic State hacktivist group. While it is believed that this group and others still have poor technical skills, they are continually struggling to improve their cyber capabilities

Such are the concerns of governments internationally that we have seen a call for those operating our critical infrastructure to continue to develop robust safeguards to protect themselves from cyberattacks. In the UK those involved in critical industry and essential services have been warned that they may face fines and sanctions if their cybersecurity preparations are not up to standard as the government implements the Network and Information Systems (NIS) Directive.

It is likely that making organisations pay up for failing to meet cybersecurity standards would only be a “last resort” and the expectation is voluntary uptake of the new rules before they come into effect on the 10th May. To help support industry the UK’s National Cyber Security Centre (NCSC) has also published detailed guidance on the security measures which will assist organisations to meet the compliance standard.

The bottom line here is, that on a global scale, we want our essential services and infrastructure to be primed and ready to tackle cyberattacks and be resilient against major disruption to services. If that means a more robust stance from governments then that, in my opinion, is not a bad thing.

# To Protect and Protect Again



Vehicle Security Barriers are becoming a recognised sight in our cities around the world.

In January 2018, the Mayor of New York, Bill de Blasio and the City's Security Infrastructure Working Group announced plans to bring permanent perimeter barriers, or bollards, to high-profile sites and to create a process to streamline their design and construction. With funds exceeding \$14 million for permanent bollards in Time Square and in excess of \$50 million to commence the broader rollout of new protective measures in phases.

Mayor de Blasio said, "In 2017, New Yorkers witnessed the horrible capacity of people willing to do us harm, whether it was in our subways, on our bike paths or in Times Square. But we will not be cowed and our expanded investment today in barriers and bollards in our public spaces underscores our resolve in keeping New York City safe from future attacks. In this new year, we can and will protect our iconic public spaces while New Yorkers go on living our lives, including by hosting a record number of tourists."

"These additional safety bollards will allow New Yorkers and visitors to be more secure at landmark locations and other sites throughout our City," said Police Commissioner James P. O'Neill.

And with vehicles seemingly becoming the weapon of choice for terrorists, the need to protect citizens from "people willing to do us harm" has dawned on most large cities, leaving many still trying to find the best way to protect their citizens.

Admittedly in many cases, it seems to be "after the horse has bolted" so to speak.

In 2016 a lorry was driven into crowds celebrating Bastille Day in Nice, killing 87 people and injuring 458. This was an awful, cowardly and devastating attack that had a huge impact on so many lives. The stark reality is however, after two previous vehicle attacks in France, if there had had been tougher security measures in place, rather than an increased police presence, and a plastic temporary barrier, then many of those citizens would still be alive today.

Reacting to these devastating events, Metropolis Nice Côte d'Azur decided to install a safety barrier along the



Promenade des Anglais.

The new barrier, or vehicle incursion prevention system, MacSafe, was tailor-made for the Promenade des Anglais by Maccaferri and J&S Franklin. It was inaugurated in July 2017. It is crash test rated to stop a 19-tonne truck travelling at 50km/h and impacting at 20°, equivalent to the vehicle used by the terrorist in Nice in 2016 and can withstand two successive impacts. The system is also accredited by the UIAU (University of Venice).

The MacSafe system consists of two high tensile steel cables supported on tubular steel posts and anchored at each end with our patented energy dissipation system. The posts are secured to ground foundations and all external fixings are designed to prevent them being easily removed.

The force of the vehicle impact is distributed through the cables and posts and absorbed within the patented energy dissipaters. The energy is absorbed through compressive deformation and not by friction. This ensures better and more reliable performance throughout the long-life of the barrier.

On the 19th December 2016, a truck was deliberately driven into the Christmas market next to the Kaiser Wilhelm Memorial Church at Breitscheidplatz in Berlin, killing 12 people and injuring 56 others. One year on, and the Christmas Market in Berlin is protected by large concrete barriers, armed police patrols and stop and search checks.

January 2017 – In Melbourne, 6 people were killed and 37 injured when a car sped down a footpath crashing into pedestrians, by June 2017 \$10 million had been allocated, and temporary concrete barricades and bollards had been installed around the City of Sydney.

In January 2018, the City of Gold Coast began installing heavy duty retractable bollards capable of repelling the force of a large heavy goods vehicle. They had previously resolved to spend \$515,000 on bollards which met the Australian standard, but on the advice of the QPS Commonwealth Games security adviser, it was recommended that the bollards comply with a European standard bringing the cost of the project to \$1.095 million.

Las Vegas, plan to have their existing 800 bollards, updated to some 7,000 by the end of 2018, in an effort to increase the safety of those walking The Strip in Sin City.

However, some Cities are still concerned about the aesthetics of concrete bollards on their historic cities, a case of balancing security over protecting tourism.

Take for instance, Barcelona in Spain.

On the 17th August 2017, a van was driven into pedestrians strolling along Las Ramblas, in Barcelona, killing 13 people and injuring at least another 130. Advice was given that bollards were needed, warnings of impending threats were given, and yet, the action

taken was to increase policing levels on the streets. Now, thankfully, there are a few bollards and increased police on the streets, and going forward they are “studying the possibility of installing physical barriers to prevent further attacks with vehicles”

In London on 22nd March, 2017, a car was driven into pedestrians on Westminster Bridge, killing 5 people and injuring 49 others. The driver also stabbed a policeman to death. Again, in London, on 3rd June 2017, a van was driven at pedestrians in the London Bridge Area. Three attackers began stabbing people, before being shot by police. 8 people died. 48 were injured, 21 critically. Controversially previously installed “Guard Rails” had been removed from London’s Streets in an effort to protect cyclists and make the Capital more “attractive”. Although Guard Rails would not have stopped either London attack they could have limited the results. However, today, protective barriers are erected on Thames bridges and from London’s experience of previous terrorist activities (IRA) there are very few buildings or indeed public spaces that don’t have “counter-terrorism” design inbuilt.

The UK Government has produced



*Mayor de Blasio Announces Extensive Plan to Install Security Bollards to Protect New Yorkers, Tourists and City's Infrastructure*



a 174 page guide, Crowded Places Guidance, that highlights the threat as a vehicle being used as a weapon, but also highlights that these threats can be “mitigated by installing physical measures (including blending into the landscape or streetscape) which may be passive (static) or active (security controlled). These measures can be installed either on a permanent or temporary basis. All such measures should meet appropriate standards in terms of their vehicle impact performance, design and installation.”

Vehicle Security Barriers, need not be ugly concrete monstrosities. Nor do they need to be concrete lumps that need huge lifting gear to place them. They can be totally inconspicuous, letting everyday life continue and forgetting they are there, or full on “in your face” shouting a warning to would be terrorists that this area is safe.

They come in many guises;

Active Retractable Bollard, like the Avon SB970CR Scimitar Security Bollard which provides a high level of security against unauthorised vehicle access without the need for an outwardly aggressive appearance.

The PAS 68 impact tested bollard is an active bollard that is hydraulically operated, it stands 1000mm in its fully raised position and retracts to

road level to allow authorised vehicles access.

Passive Static Bollard, like The Heald Mantis from Ross Technology. Their PAS 68 shallow mount fixed bollards are designed with a unique shape for contemporary style and architectural appeal. It offers a high crash rating, while still providing a shallow excavation depth of only 10” and structural frame with integrated rebar.

Planters, like the PAS68 Street Planters from Securiscape, which have an attractive floral display whilst cleverly acting as a security barrier. These planters can be installed quickly and are sited to allow pedestrians to pass through while vehicles can't, but due to intelligent design, incorporating a surface mounted, reinforced structure which can stop a vehicle if it is used as a battering ram.

Street Furniture, like the Monoscape Igneo PAS rated seat, by Marshals.

The Igneo seat has been successfully crash tested in accordance with PAS 68 using a 7.5 tonne vehicle travelling at 40mph. It can be specified in any length, using any number of modules. It is manufactured from Marshalls' fibre reinforced precast concrete and further strengthened by RhinoGuard technology, which is cast into the individual modules.

But if none of that appeals, then there are many Landscaping options, including, ditches, bunds and berms.

DefenCell by J&S Franklin, is a lightweight geotextile welded mesh gabion that once filled with locally available materials, can be incorporated into security measures for public places and protection. Filled and stacked, these gabions can be covered and planted, maintaining the aesthetic and environmental considerations of high profile or sensitive locations.

Sadly, people with “evil intent” are a fact of life. Which makes Vehicle Security Barriers a permanent part of our city landscapes. So whether hidden or in plain sight they will be there to Protect and Protect again.

## Europol's European Cybercrime Centre (EC3) supported the countries in their efforts to identify EU citizens by providing analytical support and by facilitating information exchange in the framework of the Joint Cybercrime Action Taskforce, hosted at Europol's headquarters in The Hague.

The OSCE, because of its comprehensive approach to security, is well positioned to support States on their national Security Sector Governance and Reform programmes, said speakers at today's joint meeting of the Forum for Security Co-operation and Permanent Council in Vienna.

The discussions focused on what the OSCE can do to continue to strengthen the effectiveness and coherence of its approach

in assisting participating States in their nationally-led governance and reform efforts in the security sector.

The joint meeting was opened by Ambassador Alessandro Azzoni, Chairperson of the OSCE Permanent Council and Italy's Permanent Representative to the OSCE, and Ambassador Radomír Bohá, Chairperson of the Forum for Security Co-operation and Slovakia's Permanent

Representative to the OSCE.

Azzoni highlighted Italy's involvement in the OSCE Group of Friends of Security Sector Governance and Reform, a topic which is receiving particular attention by Italy's current OSCE Chairmanship.

OSCE Secretary Thomas Greminger said that the

concept of Security Sector Governance and Reform has much to offer when it comes to strengthening the OSCE's ability to effectively prevent and respond to complex and interconnected modern-day challenges.



## EU plans to create a data base to enable EU countries to exchange non-EU citizens' criminal records faster

The Civil Liberties Committee approved plans on Thursday to create a new centralised data base on third country nationals to complement the European Criminal Records Information System (ECRIS), which EU countries already use to exchange information on previous convictions of EU citizens.

The ECRIS Third Country National (TCN) system, will:

- enable national authorities to establish quickly whether any EU member state holds criminal records on a non-EU citizen,
- contain data such as names, addresses, fingerprints and facial images (which, however, may only be used to confirm the identity of a

non-EU national who has been identified based on other data), and comply with EU data security and data protection rules.

MEPs stressed that, in addition to judges and prosecutors, Europol, Eurojust and the future European Public Prosecutor's Office should also have access to the ECRIS-TCN system.

MEPs see this system an important cross-border crime fighting tool for European prosecutors, judges and police forces, who currently often rely solely on data available from their own national criminal record systems.

Rapporteur Daniel Dalton (ECR, UK) said: "The

fast, reliable exchange of information is key in the fight against crime at all levels. This measure will close the loophole allowing third country nationals to hide their criminal records, while protecting peoples' rights and information."

These negotiations, which can start as soon as Parliament as a whole gives its green light, will also include talks on a related directive for which Parliament has already given its negotiators a mandate.

ECRIS was put in place in 2012 to exchange

information on criminal convictions in the EU. However, using the current system to check the criminal records of a non-EU citizen is cumbersome and inefficient. According to the European Commission, national authorities have used information available in other countries' criminal records only in less than five percent of conviction cases of third country nationals, between 2010 and 2014.



## INTERPOL and UN chiefs address global security issues



### INTERPOL

With an increased risk of foreign fighters returning home or joining other conflicts following the liberation of Da'esh-held territories transforming the global threat landscape, international security was high on the agenda during discussions between the heads of the United Nations (UN) and INTERPOL.

In their first meeting, Secretaries General António Guterres and Jürgen Stock addressed areas of common concern where the two organizations can further streamline and strengthen their cooperation for the benefit of their member countries.

Areas for enhanced collaboration have been identified in a number of UN resolutions, including protecting critical infrastructure, preventing foreign terrorist fighter travel as well as combating all forms of transnational crime such as maritime piracy, human trafficking and drug smuggling.

In addition, there are currently nearly 600 valid INTERPOL-UN Special Notices for entities and individuals who are the targets of UN Security Council Sanctions Committees.

Secretary General Stock said today's complex security landscape combined with increased pressure on resources highlighted the value of INTERPOL's communications system and databases as a 'global early warning system'.

"We are all too well aware of the threats which face us, and

indeed for the foreseeable future, these threats are increasing rather than diminishing.

"The partnership between INTERPOL and the UN provides a unified response in supporting law enforcement and the maintenance of international peace and security," said Mr Stock.

Among the tens of millions of pieces of data held in INTERPOL's global databases accessible to law enforcement across its 192 member countries, are more than 43,000 foreign terrorist profiles.

In 2017, law enforcement officers around the world conducted some 4.5 billion searches against INTERPOL's databases resulting in one million 'hits', with each match potentially a key piece in an investigation.

INTERPOL has a long history of cooperation with the UN which was formalized in a 1997 agreement. The Office of the Special Representative of INTERPOL to the United Nations in New York was opened in 2004, which has further strengthened the relationship between the two organizations.



## INTERPOL facial recognition nets most wanted murder fugitive

Police in Buenos Aires have arrested an internationally wanted murder suspect after his image was identified as a likely match by INTERPOL's facial recognition unit.

Kristian Danev, a Slovak national aged 33, is wanted internationally by Czech authorities under an INTERPOL Red Notice following a murder ten years ago.

As part of an investigation by police in Argentina, INTERPOL's National Central Bureau in Buenos Aires submitted images of the suspect to INTERPOL's

General Secretariat headquarters for comparison against records in its facial recognition database.

After the search result came up as a potential match, police in Argentina detained the suspect for further questioning, resulting in the suspect confirming his identity.

"In less than 48 hours, INTERPOL's global police cooperation platform helped locate, identify and arrest an international fugitive who had evaded justice for a decade," said Harald Arm, Director of Operational Support and Analysis at INTERPOL.

"This illustrates the fundamental role of INTERPOL's policing capabilities and forensic data in international police investigations. We need to ensure that vital information moves faster than fugitives," added Mr Arm.

INTERPOL's Fugitive Investigative Support unit was supported by its Command and Coordination Centre and its Regional Bureau in Buenos Aires. They worked closely together with the INTERPOL National Central Bureaus in Bratislava, Buenos Aires and Prague to ensure the quick

exchange of information on the case.

Authorities in Argentina are now holding Kristian Danev subject to his extradition to the Czech Republic.

INTERPOL launched its facial recognition biometric service in November 2016. It already contains more than 44,000 images from 137 countries.

Police forces across the globe use INTERPOL's facial recognition tool daily to make connections between criminals and crime scenes, identify fugitives and missing persons or to compare mugshots.

## Europol, Thomson Reuters and the World Economic Forum Launch Coalition to Fight Financial Crime and Modern Slavery

The fight against financial crime and modern slavery has been given fresh impetus at the Annual Meeting of the World Economic Forum with the launch of a new public/private coalition comprising Europol, Thomson Reuters and the World Economic Forum. The perpetration of financial crimes has a devastating socio-economic impact on individuals and communities around the world. Every year, the estimated \$2.4 trillion in proceeds from this and other causes of human misery such as forced prostitution, terrorism and drug trafficking will be laundered through the world's financial markets and banking systems. Despite substantial amounts of human and economic capital deployed at stopping financial crime, less than 1% is detected and confiscated via existing mechanisms.

The amount of money laundered globally in one year is estimated by the United Nations to account for 2-5% of global GDP (around \$2 trillion). Criminal networks are becoming increasingly connected, global and technologically sophisticated. Against this



backdrop, additional collective action must be brought to bear to combat financial crime in order to achieve the Sustainable Development Goals target 8.7 to eradicate forced labour, end modern slavery and human trafficking, and secure the prohibition and elimination of the worst forms of child labour. Public-private cooperation is key for the identification and implementation of innovative strategies that address this challenge while avoiding unintended consequences, such as a further retrenchment in access to the global financial system for individuals and institutions. The coalition, which is seeking additional members, will work to mobilise and influence decisions-makers at the highest levels to achieve the following objectives:

- raise awareness among global leaders on the topic of financial crime as a critical challenge with grave financial and human consequences
- promote more effective information sharing between public and private entities on a coordinated, global level

- establish enhanced processes to share compliance best practice and approaches to more robust customer due diligence

Rob Wainwright, Executive Director of EUROPOL, said: "Europol launched in December 2017 the first transnational financial information sharing mechanism, the Europol Financial Intelligence Public Private Partnership. All the members of this partnership, comprising experts from financial institutions and competent authorities, have actively started to share financial intelligence in a trusted environment. Ultimately, our objective is to facilitate, in accordance with the applicable domestic legal frameworks, the exchange of operational or tactical intelligence associated with on-going investigations. We also aim to identify ways in which the regulations for information sharing could be improved. Europol welcomes any idea of a complimentary public-private sector coalition to encourage more policy

commitment for a more efficient fight against financial crime."

David Craig, President of Financial & Risk at Thomson Reuters said: "In 2011, the UN report estimated that less than 1% of criminal funds flowing through the international financial system every year are believed to be frozen and confiscated by law enforcement. Move forward six years and those of us dealing with this issue day in day out expect to find a similarly low percentage. The fragmentation we witness across global political, regulatory, economic and social spheres is creating barriers to our success. Meanwhile criminal networks are becoming more connected, more global and more technologically sophisticated. Now more than ever there is a pressing need for public and private organizations to work together across borders to secure our future by developing new strategies for sharing data and adopting new technologies in the fight against financial crime. We must not accept being one step from failure – it's time for a fresh approach."

## International Crackdown on Anti-Spyware Malware

A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. This case was investigated by the South

West Regional Organised Crime Unit and coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America.

Once installed upon a

victim's computer, a user of the Luminosity Link RAT was free to access and view documents, photographs and other files, record all the keystrokes entered and even activate the webcam on the victim's computer – all of which could be done without the victim's knowledge.

Europol's European Cybercrime Centre (EC3) supported the countries in their efforts to identify EU citizens by providing analytical support and by facilitating information exchange in the framework of the Joint Cybercrime Action Taskforce, hosted at Europol's headquarters in The Hague.

## The True Cost of Flooding

In 2016, worldwide, there were 342 reported natural disasters

- The total number of Hydrological disasters in 2016 was 177 (164 floods and 13 landslides)
- The total number of people affected by Hydrological disasters in 2016 was 78.1 million
- The total number of deaths from Hydrological disasters in 2016 was 5,092\*

Insurance company Munich Re, released their Natural Catastrophe Review which shows that 2017 had the highest insured losses, ever, at 330 billion USD, (the second highest figure ever recorded for natural disasters.)

In 2017, worldwide, there were 710 reported natural disasters.

The figures of people affected, and the number of deaths has not yet been reported, but it is estimated to be substantially higher than 2016

Each year scientists gather information to predict global weather forecast. They study historical weather patterns, the behaviour of the atmosphere, effects of climate change, the oceans movement, watching radars, and satellites all to forecast when and where natural disasters may occur.

And yet each year, more and more people are being



affected by flooding in some way, be that the loss of livelihoods, homes or indeed lives.

Torsten Jeworrek of Munich Re said, "For me, a key point is that some of the catastrophic events, such as the series of three extremely damaging hurricanes, or the very severe flooding in South Asia after extraordinarily heavy monsoon rains, are giving us a foretaste of what is to come. Because even though individual events cannot be directly traced to climate change, our experts expect such extreme weather to occur more often in future."

If the extreme weather that we are witnessing is to continue to occur more often, then solutions need to be found to minimize the effect of flooding on communities.

One such solution currently operational, with notable success is DefenCell, an effective and easily installed

Flood Protection Barrier.

DefenCell Barriers are a cellular textile containment system that can be filled with various materials; soil, sand, gravel or small rocks whilst the heavy-duty geotextile fabric construction adapts to the terrain, offering excellent structural strength and durability. The easy-to-deploy cellular confinement system is well suited for irregular terrain and the addition of an integral or external impervious layer makes an effective flood barrier for temporary or permanent installation.

DefenCell has been proven in action and undergone thorough testing. DefenCell can be used to build new defences, enhance existing protection measures or reinforce weakened levees ensuring that communities, towns and farms are protected.

A simple one metre high (or just 0.50m) wall will be sufficient to stop all but the

most extreme flooding. Adding this to an existing levee or embankment is a quick and easy solution and many times faster than installing the equivalent barrier using sandbags and much faster and easier to remove when the threat has passed. DefenCell proved its operational capabilities on two flood prevention deployments on the Ohio River in the US and in Ontario, Canada.

In 2017, J&S Franklins DefenCell products were installed in two separate areas in South Australia for environmental applications including Ground Stabilisation, Flood Protection and Erosion Control with great success.

Andrew Cole, Chief Executive Officer, District Council of Barunga West, South Australia, said, "Whilst its normal use is military protection, security and flood/erosion barriers, we saw DefenCell as a flexible, cost-effective solution in front of the caravan park. We ran a coastal trial and monitored DefenCell's performance in tidal sea movement including high tides."

"DefenCell maintained its integrity and we are very confident moving to a full deployment of DefenCell along the caravan park foreshore. It is an easy product to use and there is potential for us to use it elsewhere on Council tasks."

## Changi Airport's new Terminal 4 has already processed more than 1.5 million departing passengers using facial recognition systems from IDEMIA



In the context of soaring world airport passenger numbers (2016: up 6.3% to 3.7 billion and 700 new routes), the need for passenger identification coupled with demanding safety standards is becoming ever more critical.

In October last year Changi Airport's latest Terminal -

Terminal 4 opened its doors to the travelling public and has already processed more than 1.5 million departing passengers. Passengers are processed using a system based on facial recognition from IDEMIA, enjoying a secure and innovative seamless experience as part of Changi's FAST and

Seamless Travel program.

Selected by Changi Airport in 2015, IDEMIA has deployed its MorphoPass Airport Solution to automated passenger ID checks using facial recognition at all departure control points. The system includes a centralized platform used by airlines and the airport to manage the various steps required for passenger authentication and identification, MorphoFace and MorphoWay (a fully automated gate for both border control and smart boarding).

Changi Airport was ranked the world's top airport for the fifth year in a row in 2017, and for the eighth time since the award was first introduced in 2000. T4 has been created to

be its most innovative terminal and can handle up to 16 million passengers per year increasing Changi's overall annual capacity to 82 million passengers.

Philippe BARREAU, Group Executive Vice President, Citizen Identity & Public Security, spokesperson for IDEMIA said "IDEMIA is thrilled that it has already helped more than 1.5 million passengers enjoy the best customer experience for travellers in the world at Terminal 4. IDEMIA strives to protect passengers so they travel in complete safety, backed by novel and convenient solutions to ensure there is no let-up in security standards while increasing convenience."

## Tanzania is using Facial Recognition to expedite cross-border mobility

The solution by Vision-Box is being used by Tanzania Immigration Services at some of the largest airports of the country

Dubai, 25th January 2018 – The Tanzania Immigration Services Department (TISD) has started using new Facial Matching Systems (FMS) to improve border control procedures end of last year.

The purpose of the integration of Vision-Box advanced technology was to enhance border security in Tanzania. How? By strengthening the capacity of immigration authorities at both land and air entry points in the country to detect irregular migration,

while adhering to data protection best standards.

The new desktop automated immigration control solutions integrate advanced document authentication and biometric recognition features. They are capable of identifying fraudulent travel documents such as passports, visas and identity cards, as well as detect identity fraud by travelers trying to enter or stay in the country irregularly. The solution matches the information contained in the travel document against the live face image capture of the traveler to guarantee a reliable traveler identification.

The Vision-Box-developed solutions are at use at two of the busiest Tanzania airports, the Kilimanjaro International Airport, in northern Tanzania serving the cities of Arusha and Moshi, and Julius Nyerere International Airport in the largest city Dar es Salaam.

Commissioner Samuel Magweiga received the equipment on behalf of the Commissioner General of Immigration and advanced "we need more of its kind for all our land, air and maritime entry points to combat irregular Migration which is becoming rampant along our borders".



## Automated, Driverless Security Robot to Help Protect the World's Highest Capacity Sports Venue

Sharp INTELLOS A-UGV provides an added layer of safety and security protection for what is known as the "highest capacity sports venue in the world."

"Technological innovation is in our DNA," says IMS President, J. Douglas Boles. "Dating back to the very first Indy 500 where the rearview mirror was pioneered, IMS values, invests, and nurtures high-tech advancements in all aspects of our operations. Evolving our security force to include automated, robotic integration enables us to better safeguard patrons, drivers, and staff."

"Sharp Electronics' outdoor security robot is ideally



suiting to help safeguard the Indianapolis Motor Speedway's expansive, fenced property," states Cliff Quiroga, Vice President for Sharp Robotics Business Development. "The Sharp

INTELLOS A-UGV is a multi-terrain, mobile sensor, data-gathering robot that can capture video, audio, and environmental information, while providing a visible deterrent without the aid

of a human driver. It utilizes a navigation surveillance platform to patrol predefined routes, extending the property coverage and impact of a traditional security force, while keeping manpower safely protected from direct threats. The Sharp INTELLOS A-UGV can also act as a sentry, monitoring in a stationary position, for an extra layer of protection and has a semi-autonomous mode for incident response. Included are standard information gathering tools, plus optional observation and sensor equipment configurable to meet the Indianapolis Motor Speedway's changing safety needs."

## International Crackdown on Anti-Spyware Malware

A hacking tool allowing cybercriminals to remotely and surreptitiously gain complete control over a victim's computer is no longer available as a result of an UK-led operation targeting hackers linked to the Remote Access Trojan (RAT) Luminosity Link. Coordinated by the UK National Crime Agency with the support of Europol, this operation saw the involvement of over a dozen law enforcement agencies in Europe, Australia and North America.

Once installed upon a victim's computer, a user of the Luminosity Link RAT was free to access and view documents, photographs and other

files, record all the keystrokes entered and even activate the webcam on the victim's computer – all of which could be done without the victim's knowledge.

These joint actions were carried out back in September 2017, the details of which can now only be released due to operational reasons.

Europol's European Cybercrime Centre (EC3) supported the countries in their efforts to identify EU citizens by providing analytical support and by facilitating information exchange in the framework of the Joint Cybercrime Action Taskforce, hosted at Europol's headquarters in

The Hague.

Victims across the world

The investigation uncovered a network of individuals who supported the distribution and use of the RAT across 78 countries and sold it to more than 8 600 buyers via a website dedicated to hacking and the use of criminal malware. Luminosity Link cost as little as EUR 40.00 and required little technical knowledge to be deployed.

Victims are believed to be in the thousands, with investigators having already identified evidence of stolen personal details, passwords, private photographs, video

footage and data. Forensic analysis on the large number of computers and internet accounts seized continues.

Steven Wilson, Head of Europol's European Cybercrime Centre, said: "Through such strong, coordinated actions across national boundaries, criminals across the world are finding out that committing crimes remotely offers no protection from arrests. Nobody wants their personal details or photographs of loved ones to be stolen by criminals. We continue to urge everybody to ensure their operating systems and security software are up to date".



## Banning Smoking in Prisons

As Prison Authorities the world over are considering the damage of second hand smoke within our jails, a blanket ban on smoking within our Prison systems is gradually being introduced. There is an overshadowing worry of litigation and compensation claims coming down the track of health damage caused by second hand smoke.

However, the Prisoners themselves are none too happy.

In the United States, 24 states prohibit indoor smoking and 4 prohibit smoking on the entire prison grounds. And in the UK, around 66 prisons have introduced a smoking ban, but plans to make all 136 prisons in England and Wales are well underway.

According to the World Health Organisation (WHO) "Tobacco use is the single most preventable cause of death and disease claiming over 100 million lives worldwide in the 20th Century." They also claim that tobacco is the psychoactive substance most widely used by prisoners, with phenomenal usage rates ranging from 64% to more than 90% depending on the country and the setting.

But, tobacco use is so totally entrenched in prison life; it helps cope with boredom, deprivation, stress, anxiety and tension. It is a source of pleasure, and of course not to mention the monetary value in an environment without



currency. Introducing a tobacco ban is not going too easy nor welcome in prison communities.

In the UK, riots have occurred within prisons over newly enforced smoking bans.

Prisoners caught with tobacco products or smoking can face disciplinary measures, such as loss of privileges as well as potentially extra time added on to a sentence. However, a couple of days added on to a 5, 10 or maybe lifetime sentence, is neither here nor there, and worth risking for a daily cigarette.



All of this makes cigarettes, big business creating an underground trade in tobacco products.

In the US, just one whole cigarettes worth of tobacco, rolled in toilet paper covering can make 5 or 6 "pinners" (small hand rolled cigarettes), this can net the seller \$30. Whilst in the UK, prisoners pay £20 for a single cigarette, and a small pouch of rolling tobacco can cost £200

Of course, it's not just tobacco that is banned, any associated accoutrements, like lighters and matches

are also banned. However, prisoners can make their own fire sources, with simply 2 AA batteries and a strip of foil!

And, where there is a will, there is a way.

Which is why, stopping contraband items before they get into the prison system is all the more imperative. Items as small as AA batteries, or foil, or even one cigarette, all need to be detected.

One system that is currently operational in prisons in over 30 countries is the SOTER RS Body Scanner. This ultra-low radiation full body scanner can find contraband that has been hidden on a person, and more frequently, in, a person.

Jan Steven Van Wingerden, CEO of ODSecurity, manufacturers of the SOTER RS Body Scanner said, "One of the strengths of our system is that regardless of how small an item is, and whether it has been ingested or inserted, the SOTER will find it. We pride ourselves on our products ability to find items that cannot be detected by conventional metal detectors or strip searches."

He continued, "It is important when searching for contraband that you can differentiate between human and other materials, to limit false positives, and wasted time. SOTER RS comes with its own software, and any hidden object, regardless of what material it is made from is found within 10 seconds!"

## City of Leon Continue to Build Their Sepura Network Rollout.

Following the successful implementation of a Sepura TETRA network in the Mexican State of Guanajuato, the city of Leon has added another 757 Sepura radios to its existing stock of more than 800 terminals through Sepura’s in-region partner Jomtel. Following a successful implementation in December 2017, the city of Leon has now achieved its goal of upgrading its communications capability for 2018.

The Municipal Public



Security Secretariat of the city of Leon purchased the radios to further enhance public safety communications for officers

in the field. One of its focus points is to streamline the portfolio of radios in use within the force, thus reducing training costs.

Sepura are pleased to be selected to support the Mexican Government in this process through our partner Jomtel.

Sepura’s TETRA STP9000 radios have an IP67 environmental rating - ensuring the radio remains operational even after submersion in water. Powerful audio, exceptional battery life and haptic feedback enable officers to physically feel when actions are registered on the device.

## Optim Awarded Five Year Contract from Department of Homeland Security Customs and Border Patrol division

Optim has announced it has been awarded a five-year, sole-source contract to supply its FreedomView Videoscope to the United States Customs and Border Patrol (“CPB”) division. The FreedomView provides law enforcement agents the ability to search for illegal contraband, such as drugs, people, and weapons of mass effect hidden in hard-to-reach-and-see areas of vehicles, containers, and other conveyances.

“We believe the FreedomView Videoscope is the best-in-class for contraband detection” stated Paul Joyce, President and CEO of Optim. “We are extremely excited that Department of Homeland Security and the CPB selected our cutting-edge equipment to enable agents to effectively



police, maintain, and protect our nation’s borders. This continues the long, exclusive relationship we’ve had with CBP that dates back to 2010. The FreedomView is about enabling effective search and seizure in vehicles and hazardous environments, while still offering simplicity and safety to the agents using the equipment.”

The CPB is tasked with utilizing small-scale detection

systems like the FreedomView Videoscope to further their mission of preventing illegal contraband from entering the United States. The FreedomView is designed for easy, portable use and feature state-of-the-art optical quality. A robust, durable construction of the videoscope enables field agents operating at ports of entry and checkpoints to conduct searches safely and efficiently.

Optim’s pioneering FreedomView line for contraband detection features a one-handed operation, outstanding image quality, and made-in-America craftsmanship and durability. The FreedomView line is UL-certified for use in hazardous environments such as gas tanks and incorporates one-touch image/video capture for reference and evidence usage. Empowered for highly protected use, the FreedomView includes AES 256-bit hardware encryption with FIPS 140-2 Level 3 validation – enabling file transfer with secure USB drives. Intended for the rigors of every day law enforcement, the video systems can sustain the harsh elements with its water, dust, and high temperature resistant design.

## MARSS announce Middle East contract for its RADiRguard smart perimeter surveillance system

MARSS have announced an important contract for its RADiRguard smart perimeter surveillance system. The contract, with an unspecified Middle Eastern Government, is for a critical national infrastructure installation and provides for the protection of a 12km high security perimeter.

RADiRguard is a smart perimeter surveillance system combining multiple sensors and complementary technologies inside a single intelligent unit.

It is the first, all-in-one perimeter surveillance solution, which can reliably detect and classify objects in advance of reaching a perimeter, thanks to its combination of a built-in radar, video imaging and radio frequency detection. It is then able to intelligently classify the threats and issue notifications using its integral behavioural analysis software.



RADiRguard is a cost effective, easy to deploy and scalable solution which can be configured to a wide variety of surveillance scenarios such as; airports, ports, borders, fuel storage facilities, power stations, water treatment plants, nuclear facilities, bridges and high value buildings.

RADiRguard coverage shape and extension is highly adaptable by changing the number and configuration of sensors installed. In a typical configuration, a single RADiRguard unit provides 400m x 100m of coverage

along a perimeter wall or fence. The system can detect and track multiple known and unknown objects including humans, animals and vehicles.

The initial detection and tracking is achieved by compact micro-radar. Behavioural algorithms provide the first level of classification. Camera footage is then analysed by Artificial Intelligence for object recognition to provide additional and more precise classification, and this classification is further augmented by analysing

GSM/Wi-Fi/VHF signals emitted by object and other intelligence data bases.

This provides a risk level for each tracked object and if the object is deemed a risk then the system automatically notifies security personnel with the exact location and a live video feed supporting interception.

This layered decision hierarchy reduces the instances of false alarms.

RADiRguard operates autonomously 24/7 and is a robust, stand alone, modular and scalable system which is low maintenance and as such is extremely cost effective.

RADiRguard can be integrated into an existing security system or as part of the MARSS NiDAR advanced long-range surveillance system for protecting borders, coastal and land-based critical infrastructure from air, surface and underwater threats.

## Radiflow has revealed the first documented cryptocurrency malware attack on a SCADA network of a critical infrastructure operator

Radiflow has revealed the first documented cryptocurrency malware attack on a SCADA network of a critical infrastructure operator

Radiflow discovered this cryptocurrency malware attack as part of routine and ongoing monitoring of the OT network of a

water utility customer. The company reports that this attack infected several servers in the OT network in order to mine the Monero cryptocurrency.

A cryptocurrency malware attack increases device CPU and network bandwidth consumption, causing the response times of tools

used to monitor physical changes on an OT network, such as HMI and SCADA servers, to be severely impaired. This, in turn, reduces the control a critical infrastructure operator has over its operations and slows down its response times to operational problems.

Radiflow's research team

uncovered that this cryptocurrency malware was designed to run in a stealth mode on a computer or device and even disable its security tools in order to operate undetected and maximize its mining processes for as long as possible.

## IPS Announce Firmware Update for OSCOR Spectrum Analyzer



The new Firmware update is a free download available on the REI website, for existing OSCOR operators. In addition to performance improvements in the new Firmware update, two file and data operations have been added:

When generating a signal list, the OSCOR will automatically populate the comments field with information about the frequency band that a signal might be a part of for the currently selected ITU region. This information contains known regulatory or other uses of given frequency bands. Depending on the frequency there may be multiple allocations given. The frequency allocation information is also provided anytime that a signal is added to an existing signal list.

The file dialogs on the OSCOR, such as the file open and file save dialogs,

now contain Cut, Copy, Paste, Delete, and Rename operations which allow users to copy or move files from a compact flash card to a USB flash drive, as well as other file operations within the OSCOR firmware.

OSCOR Blue is a portable spectrum analyzer with a rapid sweep speed and functionality suited for detecting unknown, illegal, disruptive, and anomalous rogue transmissions across a wide frequency range. The OSCOR Blue Spectrum Analyzer is designed to detect illicit eavesdropping signals, perform site surveys for communication systems,

conduct radio frequency (RF) emissions analysis, and investigate misuse of the RF spectrum.

OSCOR Green Spectrum Analyzer is designed to detect illicit eavesdropping signals, perform site surveys for communication systems, conduct radio frequency (RF) emissions analysis, and investigate misuse of the RF spectrum. The OSCOR Green is a portable spectrum analyzer that sweeps 24 GHz in one second to quickly detect transmitting electronic surveillance devices and ensure that spectrum activity is captured.

## L3 WESCAM Launches Smarter, More Accurate Imaging and Processing Technologies

L3 WESCAM announced that it has created smarter, more technologically advanced electro-optical and infrared (EO/IR) systems by incorporating high-performing imaging and processing technologies into its MXTM-Series product line. These new technologies will enable MX operators to conduct missions with enhanced image processing and greater visual capabilities than ever before.

“Today’s environments are more complex, and missions need to be executed with more assurance,” said Paul Jennison, Senior Vice President of Strategy and Business Development for L3 WESCAM. “L3’s newly incorporated smart technologies provide a portfolio of capabilities that will help operators succeed



though a combination of ease-of-use and robust performance.”

Newly launched imaging technologies include the addition of higher-sensitivity cameras that offer advanced imaging capabilities across a much wider range of illumination conditions, thereby advancing operator capabilities in low-visibility and no-visibility environments.

Advancements to L3’s MX image processing technologies include WESCAM’s embedded Advanced Video Engine (WAVE) and a newly embedded Graphics Processing Unit (GPU). L3 WESCAM’s new Automated Video Tracker (AVT) and embedded Moving Target Indicator (MTI) technologies are supported by this new architecture and provide automatic target acquisition

of multiple targets with significantly improved target lock performance in challenging mission scenarios.

L3’s significant investment in its image processing technologies has made the MX product line smarter, as the WAVE’s architecture supports future growth and allows for the rapid deployment of future image processing techniques.

L3 has more than 40 years of experience in the design and delivery of stabilized imaging and targeting solutions. Systems range in size from 8 to 25 inches in diameter, portray clear sighting capabilities across the visible and infrared spectrums, and operate with outstanding stabilization and leading range performance.



smiths detection

Checkpoint security solutions for today and tomorrow

[www.smithsdetection.com](http://www.smithsdetection.com)

### World Security Report



World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to over 150,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, security and armed forces and civilian services and looks at how they are dealing with them. It aims to be a prime source of online information and analysis on security, counter-terrorism, international affairs and defence.



**HIDDEN TECHNOLOGY**  
systems international ltd.

Discrete tracking devices for personal protection and vehicle security.

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

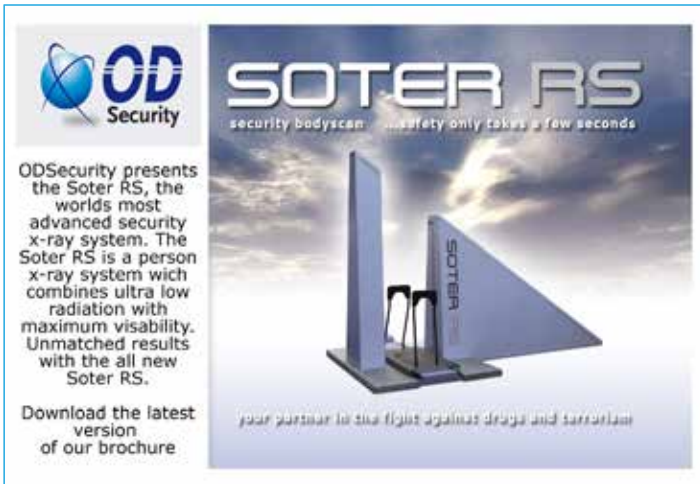
In use by Police, Military and Government organizations worldwide.

[www.hiddentec.com](http://www.hiddentec.com)

### Border Security Report



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



**OD Security**

**SOTER RS**  
security bodyscan... safety only takes a few seconds

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

Download the latest version of our brochure

*your partner in the fight against drugs and terrorism*



2003-2013  
**WAGTAIL**  
UK LIMITED  
SPECIALIST DOG SERVICE  
**10 YEARS**

**Wagtail International**  
leading specialists in detection dogs and dog handler training

Click here to view our profile



**DEFENCELL**

PROFILE 300 & DC BARRIERS  
HOSTILE VEHICLE MITIGATION

[www.defencell.com](http://www.defencell.com)



**International Procurement Services (IPS)**

Electronic Countermeasures  
Equipment Sweep Teams  
Training

[www.SECURITYSEARCH.Co.UK](http://www.SECURITYSEARCH.Co.UK)

**March 2018**

5-6

Defence Logistics Eastern Europe  
Prague, Czech Republic  
[www.defence-logistics.eu](http://www.defence-logistics.eu)

6-7

Security & Policing  
London, UK  
[www.securityandpolicing.co.uk](http://www.securityandpolicing.co.uk)

6-7

Security & Counter Terror Expo  
London, UK  
[www.counterterrorexp.com](http://www.counterterrorexp.com)

6-8

Major Events Safety & Security Summit (ME3S)  
Dubai, UAE  
[www.isnrabudhabi.com/ME3S](http://www.isnrabudhabi.com/ME3S)

14-15

Behavioural Analysis  
Cardiff, Wales, UK  
[www.behaviouralanalysis.com](http://www.behaviouralanalysis.com)

20-22

World Border Security Congress  
Madrid, Spain  
[www.world-border-congress.com](http://www.world-border-congress.com)

**April 2018**

5-7

Secutech India 2018  
Mumbai, India  
[www.secutechexpo.com](http://www.secutechexpo.com)

10-12

LAAD Security 2018  
Sao Paulo, Brazil  
[www.laadsecurity.com.br/en](http://www.laadsecurity.com.br/en)

11-13

International Security Conference West  
Las Vegas, NV, USA  
[www.iscwest.com](http://www.iscwest.com)



To have your event listed please email details to the editor [tony.kingham@knmma.com](mailto:tony.kingham@knmma.com)

18-19

IoT Tech Expo Global 2018  
London, UK  
[www.iotevents.org](http://www.iotevents.org)

**May 2018**

1-3

Civil Security Congress & Expo 2018  
Melbourne, Australia  
[www.civsec.com.au](http://www.civsec.com.au)

**July 2018**

17-19

Critical Infrastructure Protection & Resilience Asia  
Sarawak, Malaysia  
[www.cip-asia.com](http://www.cip-asia.com)

**September 2018**

25-27

Critical Infrastructure Protection & Resilience Europe  
The Hague, Netherlands  
[www.cipre-expo.com](http://www.cipre-expo.com)

**December 2018**

4-6

Critical Infrastructure Protection & Resilience North America  
Florida, USA  
[www.ciprna-expo.com](http://www.ciprna-expo.com)

# WorldSecurity-index.com

## The Homeland Defense and Security Database

# BORDER SECURITY REPORT

VOLUME 9  
MARCH / APRIL 2018

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

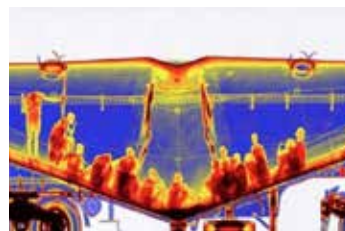


## SPECIAL REPORT



Adolfo Suárez Madrid Barajas Airport p.16

## AGENCY NEWS



A global review of the latest news and challenges from border agencies and agencies at the border. p.29

## SHORT REPORT



order Pass Management System Facilitates Cambodian-Thai Border Crossing p.28

## INDUSTRY NEWS



Latest news, views and innovations from the industry. p.40

## Walls, development or both?

In the world of border management much time, effort, money, intellectual and political capital is invested in how to protect borders and not nearly enough on how we can prevent the problem of mass migration, the evils of terrorism, human and drug trafficking and the whole range of other cross border crimes in the first place.

Fences are going up in the US and all over Europe and indeed it was that promise of a border wall that probably put President Trump in the White House.

Some would say that when the have's live next door to the have not's the 'draw' of a better life will inevitably lead the have not's trying to join the world of the have's legally or otherwise. And so, the logic goes, inevitably the have's will be overwhelmed by the have nots leading the have's to ultimately become have nots themselves.

So, we need walls!

Personally, I'm all for tightening up our borders, but I can't help thinking that more needs to be done to address the issue of 'the draw'.

The EU is doing some good work in this area with its EU Emergency Trust Fund for Africa. It was set up to address the root causes of trans-Saharan migration, and its purpose is to finance projects that create employment opportunities, support basic services for local populations and support improvements in overall governance, as well as projects that

improve migration management.

But some would say that the investment is not enough and too much focus is put on improving border security issues and not enough on development.

It is in this context that this year's World Border Security Congress in Madrid, the African Union and ECOSOCC will be hosting of Side Event with the theme of "Migration - Creating Opportunities for Young People in Africa".

No doubt, it should generate plenty of discussion for the next issue!

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](http://www.world-border-congress.com/BSR)



# CONTENTS

## BORDER SECURITY REPORT



» p.5

### 5 TRAVELLER IDENTIFICATION

ICAO TRIP - The Importance of Reliable and Secure Traveller Identification

### 10 AGENCY REPORTS

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

### 16 ILLEGAL MIGRATION IN EASTERN EUROPE AND UKRAINE

A look into the latest challenges facing Ukraine and Europe's Eastern front.



» p.16



» p.28

### 20 MADRID BARAJAS AIRPORT

An overview of the measures in place to promote Integral Management for Border Security at the Airport.

### 20 IOM NIGER: IMMIGRATION AND BORDER MANAGEMENT

Exploring what the IOM Niger mission is doing to help tackle border management challenges..

### 26 CARICOM'S REGIONAL BORDER SECURITY ARCHITECTURE

The CARICOM Implementation Agency for Crime and Security (IMPACS) is the regions "nerve center" of the Security Management Framework.

### 29 AGENCY NEWS

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

### 36 WORLD BORDER SECURITY CONGRESS

Details of the next gathering of the international border security community in Madrid, Spain on 20th-22nd March 2018.



» p.22

## Joint Statement from INTERPORTPOLICE and AIRPOL Announcing Continued International Airport Law Enforcement Cooperation

Commissioner Peter Nilsson, Project Manager and Head of the European Union's AIRPOL and Secretary General Jay Grant, of the INTERPORTPOLICE announced continued cooperation in airport security and law enforcement initiatives. In 2017 two meetings were held, the first in April hosted by the Port Authority of New York and New Jersey Port Authority Police at the World Trade Towers, and in September at London Heathrow International Airport, hosted by the Metropolitan Police. Eight countries with police authorities from Canada, France, the Netherlands, Spain, Sweden, Denmark, United Kingdom, and the United States participated along with several experts from intelligence to counterterrorism and cyber reviewed current global incidents and risk mitigation requirements to address today's global security risks.

Peter Nilsson stated, "Europe's airports are working cooperatively to ensure the safety of the traveling public. Preventative measures are a primary aspect of our security. All of us are aware of how common air travel is, internationally and regionally. At any one time there are millions of people at airports all over the world, passing as travellers or working there. The Airpol work is to ensure that the critical infrastructure, connected to the Airport Community, is protected in the best manner possible at all times. This is what our police strive for each and every day."

Jay Grant stated, "Although we look at the whole security picture of prevention, protection and preparedness, our primary focus has too been prevention. This is the first line of defence in security and recent incidents have shown us we needed to rethink our methods. Discussions will include the best practice Project Griffin International (<https://projectgriffin.net>) and operational aspects including critical communication management as we endeavour to strengthen community intelligence, operational interactivity, interoperability, and public safety connected collaborative communications for environment protection and communication efficiently."

Both police leaders expressed efforts on a joint basis are not only practical they are imperative. We learn from each other; although we may address things differently in our many countries the efforts of protection are mutual and common. Although this was assumed, our meetings have

proved this out. These next meetings will move towards a broader discussion on operational practices and we expect to include other responder organizations, as when there is a crisis it takes everyone's experience and cooperation within the Airport Community.

### AIRPOL

The AIRPOL Network, financed and appointed by The European Union (EU) strives to enhance the cooperation between Police and Border Guard Units at EU Airports. Airpol's scope are three aviation and airport related themes: Airport Policing, comprising all first-line police functions in and around airports, such as airport crime, contingency management, counterterrorism strategies, VIP-protection, protection of critical infrastructure, Aviation Security, which consists of all necessary actions and regulations to secure civil aviation. Examples of relevant issues are: engagement of air marshals, dealing with unruly passengers, access and security checks, airport badges management, and Air border Security in all of its aspects: immigration issues, return operations and document fraud. Airpol has four expert groups working: Behaviour Detection, Insider/radicalization, Intelligence/Information sharing and an expert group taking a holistic perspective on Security issues in the Airport Community.

### INTERPORTPOLICE

An International Organization of Airport and Seaport Police that was established in 1969 by police authorities from Canada, Netherlands, United Kingdom, and the United States to facilitate global authority cooperation addressing terrorism and transnational crime within the transportation security and border sector. Today we collectively work as a global force to protect our local communities, our nations, and the world. The INTERPORTPOLICE holds consultative status with the United Nations International Maritime Organization; and MOU and partnerships with the Organization of American States, AIRPOL, European Association of Airport and Seaport Police, BorderPol, and the United Kingdom's Project Griffin. Also, annually support the International Police and Public Safety 9/11 Medal, given to police and public safety offices who have distinguished themselves in the fight against terrorist activities. (<https://911center.org>)

# TRAVELLER IDENTIFICATION: KEY COMPONENT OF BOTH TRAVEL FACILITATION AND AVIATION SECURITY

Following the successful introduction of MRTDs in the eighties, which has dramatically enhanced the security features used in passports, ICAO has started implementing an ambitious initiative aimed at improving both the overall integrity of travel documents and the processes involved in their issuance as well as security at border control.

## **Context: The Importance of Reliable and Secure Traveller Identification**

The ability of terrorists and criminals to operate with anonymity—beyond the knowledge or even suspicion on the part of relevant State and international authorities about their true identity and movements—is

a powerful tool and weapon in enabling those with ill intents to further their unlawful and illegitimate activities.

Conversely, the ability of authorities to confirm the true identity and to monitor certain movements of travellers—and to do so speedily, cost-effectively, securely and

responsibly—is vital for a wide range of purposes:

- maintenance of effective national and global security
- facilitation of personal and business travel and trade
- determination and discharge of treaty and other obligations and rights related to the cross-border movement and admission of people
- cost-effective deployment of security and border admission and clearance personnel and resources on a risk-management basis
- detection and prevention of crime, including money laundering, smuggling, illegal drug trade, child abduction and human trafficking

### Drivers for Enhanced Traveller Identification

The following are factors and trends that encourage and support the sharing of knowledge, insights and technologies amongst diverse States and international authorities with mandates and interests in the issuance and/or use of traveller identification.

There is strong consumer and business pressure for expedited travel, trade and tourism, and corresponding public resistance to security, border control and other processing activities that add avoidable costs, delays, and restrictions to movement. Conversely, security threats in many sectors—including, but not limited to, the aviation sector—are real, significant and continually evolving

In the meantime, innovative technologies and protocols offer new opportunities for cost-effective deployment of security resources where they are most needed, based on risk-management principles, thereby enhancing both security and facilitation objectives.

In that context, the ICAO Traveller Identification Programme (ICAO TRIP) Strategy was approved by the ICAO Council and endorsed by the 38th Session of the ICAO Assembly in 2013. The TRIP Strategy aims to enhance the integrity of the passport-issuance process and to ensure robust identification-management processes in order to prevent exploitation by terrorists and maximize the effectiveness of border security and the benefits of enhanced facilitation of travel across borders.

The efforts of ICAO to ensure the legitimacy of secure travel documents depends on a holistic, and integrated

approach to the traveller identification-management and issuance process. The integrity of travel-document issuance is severely compromised if appropriate safeguards are not incorporated into the traveller-identity management process in order to ensure confirmation of the identity of the individual to whom the passport is issued.

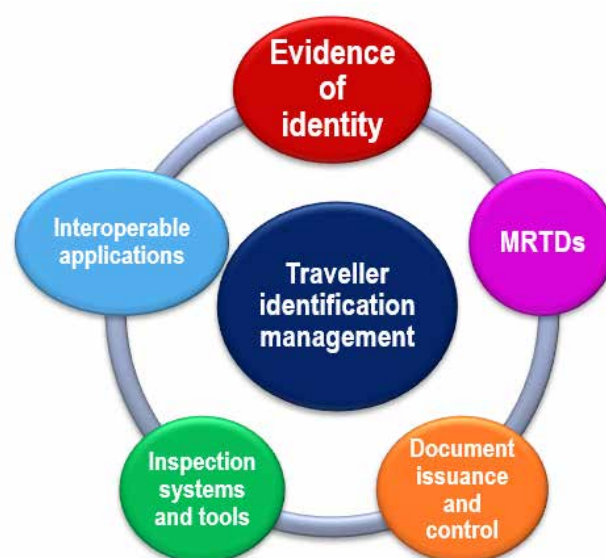
### Nature of a robust Identification Management

For purposes of this Strategy, a comprehensive and cohesive approach to traveller identification entails five closely linked and mutually-complementary identification management activities (Graph 1).

i) *Evidence of Identity*: ensure authenticity of the identity of an applicant seeking issuance of a travel document, confirming for that individual a unique identity linked to the applicant, the identified individual's status as still living and the applicant's status as an active user of that unique identity.

ii) *Machine-Readable Travel Documents (MRTDs)*: ensure that the design and manufacture of standardized machine-readable passports (MRPs), visas, and identification (ID) cards for travel that meet internationally-accepted standards and practices with respect to global interoperability and effective biometrics as well as high integrity against counterfeiting and forgery.

Graph 1: The 5 elements of the ICAO TRIP strategy



iii) *Document Issuance and Control*: implement effective processes and protocols for the issuance of MRTDs to authorized holders only, including emergency issuance where warranted while ensuring the security against theft, tampering and loss.

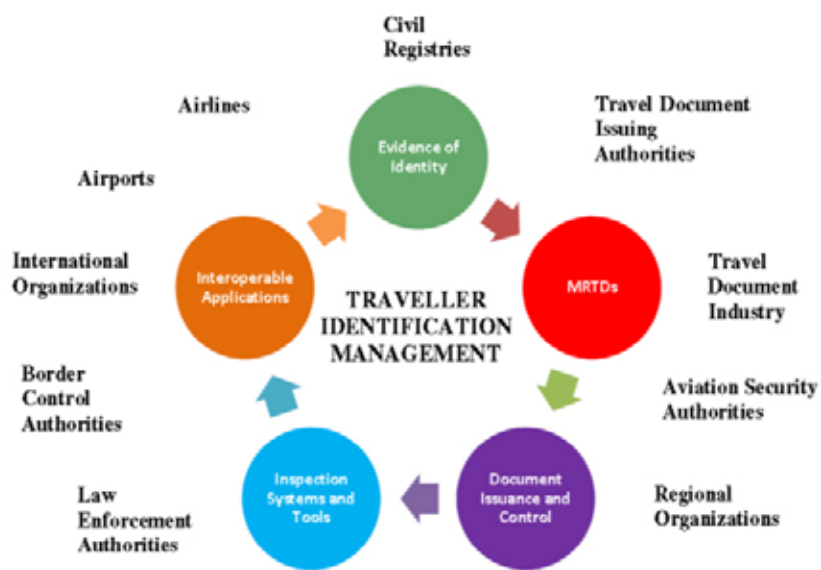
iv) *Inspection Systems and Tools*: Implement technologies, supporting infrastructure, information-sharing and related protocols and procedures to support timely, efficient, secure and reliable reading of MRTDs at borders and verification of the validity of the MRTD for the holder, including by the use of the ICAO Public Key Directory (PKD) to confirm that e-passports presented to authorities remain legitimately-issued and active (i.e., not lost, stolen, compromised or revoked)

v) *Interoperable Applications*: Implement systems, technologies and protocols that provide for the ready, secure and reliable linkage of MRTDs and their legitimate holders to relevant intelligence and information about the holder and/or his/her background, movements and actions of interest, in support of security and travel facilitation. Interoperable applications include such functions and linkages Passenger Name Record data (PNR), Advance Passenger Information (API), State-managed security “watch lists” and State-recognized “known,” “trusted” and/or “expedited” travellers and shippers (or equivalent).

**Main challenge: Involvement of different stakeholders**

As shown in Graph 2 wide array of Contracting State authorities/ministries and other entities have mandates and interests in traveller identification. These include State-level agencies, regional and international organizations concerned with these issues and services such as civil registries, passport issuance, visa issuance, security, trade and tourism, immigration/migration, border controls, law enforcement, treaties—human rights, refugees, stateless persons, special events (Olympics, international meetings e.g., G7/G20) and emergencies (identification of victims and survivors).

Graph 2: Different stakeholders involved in the ICAO TRIP strategy



All Contracting States have mandates for, and interests in, the efficient and effective operation of their immigration/migration, trade and travel (including tourism) and border control functions, all of which have requirements for secure, reliable and efficient traveller identification.

In addition to the organizations concerned with the above issues and applications, there are the individual travel document applicants and holders who use formal travel documents (most notably passports) for a wide range of purposes well beyond border crossing and international travel. These include a wide range of routine transactions where credible sources of identification are either required or expeditious, such as banking, currency exchange, vehicle and equipment rental, domestic travel, and application processes for access to civil programs, services and benefits.

As noted above, the interests in, and needs for, secure travel documents and related technologies, tools and processes, extend well beyond the world of international civil aviation. A diverse array of travel document issuers and users require and/or can benefit from the leadership, engagement, support and/or collaboration and cooperation of ICAO.

Notably, travel documents and related technologies and processes that meet the needs and standards of international civil aviation security and facilitation will typically also readily meet diverse other

identification needs and standards, for example, with respect to security, functionality, credibility, interoperability and efficiency. In some cases ICAO-compliant travel documents can be directly used for such other applications. In other cases, ICAO's knowledge, technologies, insights and experiences in the production, management and use of secure identification documents, tools and processes can be shared and efficiently adapted and applied to the needs of other travel document issues and users.

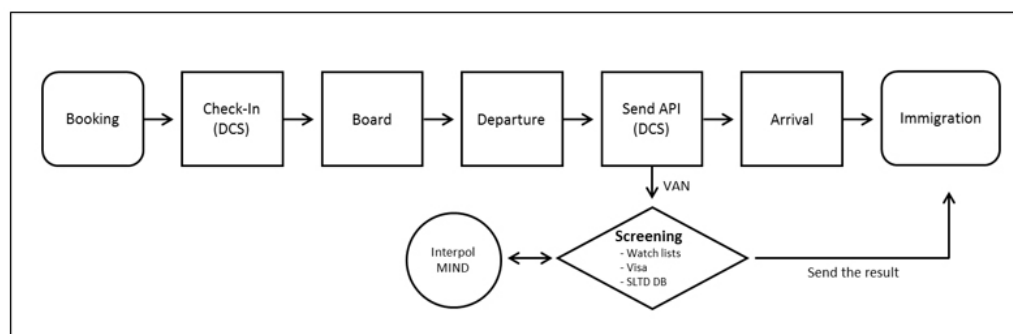
### The need for a TRIP roadmap to assist States in their implementation efforts

The 39th Session of the Assembly endorsed the priorities for the ICAO TRIP Strategy and expected outcomes for the 2017-2019 triennium. Assembly Resolution A39-20, *Consolidated statement of continuing ICAO policies related to facilitation*, identified national and international action in ensuring the security and integrity of traveller identification and border controls. Specifically, the Assembly urged Member States, through their travel document and border control programmes, to uniquely identify individuals to maximize security and facilitation benefits, including preventing acts of unlawful interference and other threats to civil aviation. Furthermore, the Assembly endorsed the development of a roadmap for the implementation of the ICAO TRIP Strategy.

The ICAO TRIP roadmap has been developed in the context of the *No Country Left Behind initiative* but also in light of the two UN Security Council Resolutions 2178 and 2309 that were approved in 2014 and 2016 respectively. The two resolutions address notably the acute and growing threat posed by foreign terrorist fighters (FTF). The relevant parts of the resolution are: "Reaffirms that all States shall prevent the movement of terrorists or terrorist groups by effective border controls and controls on issuance of identity papers and travel documents, and through measures for preventing counterfeiting, forgery or fraudulent use of identity papers and travel documents..." and "...calls upon all States to require that airlines operating in their

territories provide advance passenger information to the appropriate national authorities in order to detect the departure from their territories, or attempted entry into or transit through their territories, by means of civil aircraft, of individuals designated by the Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015);"

The UN Security Council has thus mandated States to request, in fact "require" as the resolution states, advance passenger information from airlines in order to match passenger data against the UN Security Council's travel ban lists for terrorists.



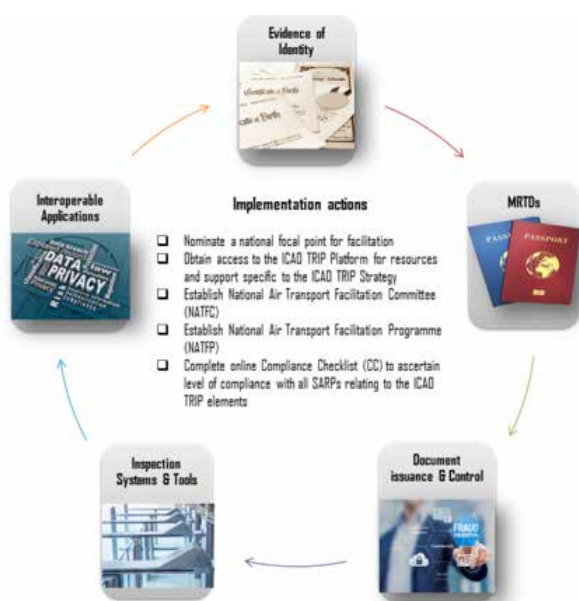
Following the resolution 2178, the UN counter-terrorism bodies also included a non-binding recommendation on the use Passenger Name Records(PNR), namely encouraging airlines to provide, where appropriate, to the appropriate national authorities. Since most FTFs use legitimate travel documents the use of PNR will allow States to better understand travel patterns of terrorist fighters, and to share practices in evidence-based traveler risk assessment and border screening. It is likely that more countries will begin to demand PNR data as well.

Clearly resolutions 2178 and 2309 have increased the political and legal impetus for States and airlines to implement passenger data exchange programs, while it is noteworthy that under Annex9 – Facilitation, API/PNR aim to provide target milestones for the implementation by States of the ICAO TRIP Strategy.

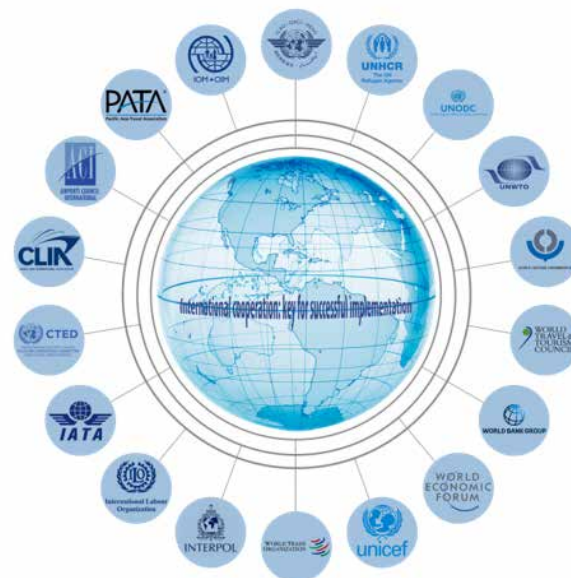
The ICAO TRIP roadmap is primarily based on the global analysis of the Universal Security Audit Programme Continuous Monitoring Approach (USAP-CMA) results for Annex 9 security-related Standards and Recommended Practices (SARPs) from 178 second-cycle audit results. In implementing the TRIP roadmap, Member States will first need to continue focussing on

implementing the TRIP-related SARPs in Annex 9 and the associated technical specifications for machine readable travel documents contained in Doc 9303. The Secretariat has identified 48 SARPs in the fourteenth edition of Annex 9 that relate to the elements of the TRIP Strategy. These are listed in the ICAO TRIP roadmap.

At the national level, implementation of the roadmap will require coordinated action between many government and industry entities, such as passport issuing offices, aviation security authorities, civil registries, border control and law enforcement agencies, airlines, airport authorities, the travel document industry, immigration authorities and other interested parties. The mechanism and requirement for such coordination on matters relating to facilitation already exist in Annex 9 through national air transport facilitation programmes and their related committees as shown in the graph 3.



Governments, in pursuant with their laws, regulations and national programmes on aviation security, and according to the relevant ICAO SARPs, will seek to develop appropriate legislation enabling them to implement effectively the ICAO TRIP Strategy. In the international context, the aim is to systematically collaborate with all interested stakeholders to implement each element of the TRIP Strategy. Importantly, ICAO's leadership is essential to the



success of the achievement of this roadmap, focusing on enhancing aviation security and improving facilitation with the objective to provide States with a blueprint that sets out the elements that must be in place in order to move, for example, from Machine Readable Passports (MRPs) to ePassports, and possess excellent breeder documents and sufficient financial resources.

To this end, there is a need to ensure both national coordination and international cooperation (as shown in Graph 4) for each action linked to the effective implementation with a view to achieving the effective implementation of the ICAO TRIP roadmap.

By definition, this is a constantly-changing and evolving work effort which is supported by the guidance published at <https://www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx>.

There are a number of broader cross-cutting initiatives that are being pursued, including most notably those dealing with outreach to all the involved stakeholders, promotion of the integrity and benefits of secure traveller identification, expansion of assistance and capacity building efforts for States in need, and enhancement of assessment missions and assistance from the Regional Offices

*Dr Narjes Abdennebi  
Chief Facilitation Section (C/FAL), Aviation Security and Facilitation (ASF), Air Transport Bureau (ATB), ICAO*

## Spanish National Police and Guardia Civil Join Forces with EUROPOL in Hit Against Iraqi Illegal Immigration to EU

Europol supported seven mixed teams of Spanish National Police (Policía Nacional) and Guardia Civil in a successful strike against Iraqi illegal immigration in which six individuals were arrested in Spain. The criminal organisation transferred Iraqi illegal immigrants from their country into the Schengen Zone.

The investigation began last February when Spanish police officers found six individuals from Iraq inside a refrigerated truck in Teruel (Spain). On the same day and later on in March they located two people concealed in the same conditions in Valencia, alongside eight illegal immigrants in Teruel, who called the emergency services as they feared they were dying from the cold inside the truck.

The network transferred the Iraqi illegal immigrants from Spain to the UK inside refrigerated trucks. The criminals took advantage when the drivers were sleeping to introduce the people inside the vehicles. They were a group composed of six to eight individuals or families with children and they had to stay in the truck for 30 or 40 hours under temperatures that were not higher than 4°C.

Spanish police officers carried out six house searches in Spain. As a result, a large amount of documents, several electronic devices and EUR 15.000 plus USD 8.000 were confiscated. Five individuals were arrested in Valencia, alongside one in Bilbao. Currently, the suspects are being interrogated while the forensic teams are performing the extractions of the mobile devices.

## Eighth Arrests in Hit Against Criminal Network



Operation YEHYA was carried out by the Aliens Division of Attica, Greece with the support of Europol's European Migrant Smuggling Centre (EMSC). Eight persons were arrested, of which seven were members of the organised crime group. Travel documents, computers and money were

confiscated. The participating countries worked together in the framework of the EMPACT project targeting Facilitation of illegal immigration in the EU.

Members of an organised crime group, involved in producing and circulating false/falsified travel documents, which facilitated the illegal movement of migrants from Greece to other countries, was arrested today in Greece.

For the successful outcome of Operation YEHYA, specialized analytical support was provided by Europol's European Migrant Smuggling Centre (EMSC) and the EMSC experts in the office of Europol in Piraeus, Greece. Europol also provided on-the-spot support through the deployment of a mobile office, enabling real-time access to Europol's databases.

## Big Hit Against Sexual Exploitation

Spanish National Police and the Romanian Police have joined forces, supported by Europol and Eurojust, to dismantle an organised crime group involved in trafficking women for sexual exploitation in different EU Member States. In total, 11 individuals were arrested and 13 victims were safeguarded.

The investigation began in November 2015. The members of the criminal network recruited their victims in their country of origin using the Loverboy method, by a man who purported to be the victim's boyfriend and promised

her a better life. Once in Spain, the victims were forced into prostitution in Madrid, Ibiza and Asturias. During the course of the investigation, police officers unveiled that some of the victims were forced to undergo plastic surgery. Furthermore, the women had to pay a tax in return of being protected on the street. The organised group extended their activity to Germany, the Czech Republic and the Netherlands.





## Nigerian police getting increased access to INTERPOL information



Getting INTERPOL's vital global policing information into the hands of frontline law enforcement officers throughout Nigeria is part of an ongoing expansion programme by national authorities.

Nigeria's work to ensure agencies at key border control points, including the immigration service and customs, can access INTERPOL's global databases was a key part of discussions during INTERPOL Secretary General Jürgen Stock's first mission to the country.

The INTERPOL Chief met with Minister of the Interior Lt Gen Abdulrahman Bello Dambazau and the Comptroller General of the Nigerian Immigration Services (NIS), Muhammed Babandede.

Connectivity between the INTERPOL National Central Bureau (NCB) in Abuja with other agencies such as the NIS, the Economic and Financial Crimes Commission (EFCC) and the National Drug Law Enforcement Agency (NDLEA) were highlighted as good practice in ensuring a seamless transfer of policing information.

## INTERPOL facial recognition nets most wanted murder fugitive



Police in Buenos Aires have arrested an internationally wanted murder suspect after his image was identified as a

likely match by INTERPOL's facial recognition unit.

Kristian Danev, a Slovak national aged 33, is wanted internationally by Czech authorities under an INTERPOL Red Notice following a murder ten years ago.

As part of an investigation by police in Argentina, INTERPOL's National Central Bureau in Buenos Aires submitted images of the suspect to INTERPOL's General Secretariat headquarters for comparison against records in its facial recognition database.

After the search result came up as a potential match, police in Argentina detained the suspect for further questioning, resulting in the suspect confirming his identity.

## INTERPOL Chief and Kuwait Interior Minister discuss terrorism at Global Coalition meeting

INTERPOL Secretary General Jürgen Stock met with Sheikh Khaled Al-Jarrah Al-Sabah, Deputy Prime Minister and Minister of Interior of Kuwait to address terrorism and organized crime.

The discussions took place on the sidelines of the Ministerial Meeting of the Global Coalition to Defeat ISIS/ Daesh.

Attended by Ministers of Foreign Affairs from the 70 coalition countries, as well as from the European Union, NATO and the Arab League, Secretary General Stock underlined INTERPOL's continued commitment as the key law enforcement partner.

## Work of international actors in preventing proliferation of nuclear weapons



The work of international actors, including the OSCE's contribution, in supporting the implementation of the 2004 United Nations Security Council Resolution 1540 on preventing the proliferation of nuclear weapons was explored at the OSCE Forum for Security Co-operation (FSC) meeting in Vienna, held under Slovakia's Chairmanship.

"Recognizing the threat to international peace and security posed by nuclear weapons, UNSCR 1540 represents a landmark decision and marks an important step towards limiting this threat by outlining provisions and measures and providing a framework for preventing the proliferation of nuclear weapons," said Ambassador Radomír Boháč, Chairperson of the Forum and Permanent Representative of Slovakia to the OSCE. "Sadly, the importance and necessity of this resolution is particularly relevant in the light of today's volatile and unpredictable nuclear environment."

He added OSCE fully supports the implementation of UNSCR 1540, as the Organization's vision to promote peace and ensure security across the OSCE region is inextricably linked to the resolution's aim of maintaining a system that regulates the spread and use of nuclear weapons.

## OSCE parliamentarians discuss Belgium's migration experience with focus on sustainable solutions for unaccompanied minors

Senior members of the OSCE Parliamentary Assembly were in Brussels to learn more about Belgian migration and asylum policies as well as measures to promote the integration of refugees.

Extensive discussions addressed the different reception options available to unaccompanied foreign minors in particular, from dedicated units within federal reception centres to small care facilities managed by NGOs, foster care and independent living. Committee members noted that, as the estimated numbers of unaccompanied children arriving in Belgium had dropped significantly to

about 2,000 each year compared to a peak of over 5,000 in 2015 at the height of the migration crisis, it was now possible to implement this needs-based approach which seeks to provide adapted care suited to the needs of the individual.

Members said however that a number of challenges remain with regard to procedures for determining the best interests of the child and for correctly assessing age due to the lack of a common European approach in these areas. One main obstacle to family reunification remains the high cost of the DNA tests, they observed.

## Increasing expertise in combating illicit drugs

Afghan law enforcement officers completed an OSCE-organized two-week train-the-trainer course on combating illicit drug trafficking and drug-related crime, at the Russian training facility in Domodedovo, near Moscow.

The training course for 13 trainees, organized jointly with the All-Russian Advanced Training Institute, increased the participants' capacity to deliver training courses in search operations, including in the use of modern techniques for identifying illicit drugs, their precursors and countering

drug-related crimes. The course included practice in searching residential areas and vehicles and in effectively using special equipment.



## Mediterranean Migrant Arrivals Reach 8,154 in 2018; Deaths Reach 401

Arrivals by sea in Italy January - December 2018/2017/2016 (source: Italian Ministry of Interior)			
	2018	2017	2016
January	4,182	4,468	5,273
February	549 (as of 11/02)	8,971	3,828
March		10,853	9,676
April		12,943	9,149
May		22,993	19,925
June		23,524	22,371
July		11,459	23,552
August		3,914	21,294
September		6,291	16,975
October		5,979	27,384
November		5,641	13,962
December		2,268	8,047

IOM reports that 8,154 migrants and refugees entered Europe by sea through the first six weeks of 2018. This compares with 12,358 arrivals across the region through the same period last year.

IOM Rome reported Italy's official Ministry of Interior figures indicate some 4,731 migrants arrived by sea to Italy this year, which represents a steep decline compared to the 9,448 arrivals recorded during the same period last year.

After tracking January arrivals similar to those of 2017 and

2016 through the first week of February, Italian authorities have recorded just 549 arrivals in February 2018.

Since the start of December, the Western Mediterranean has recorded over 100 deaths at sea. Total deaths in the Mediterranean in 2018 now stand at 401 migrants since the start of 2018, compared with 261 at this time last year. The Western Mediterranean already has recorded 86 deaths in just 42 days this year—nearly three times the total at this time on that route last year.

Worldwide, IOM's Missing Migrants Project (MMP) has recorded 589 migrant fatalities in 2018.

In the Horn of Africa, 25 Ethiopian migrants are missing and presumed dead, after being forced into the water off the coast of Yemen on 8 February. They were travelling on one of four boats that brought over 600 Ethiopian men and women to the coast of Yemen's Shabwa governorate.

On the Myanmar/Bangladesh border, three Rohingya children drowned as they were trying to cross from Mangdaw in Myanmar to Teknaf in Cox's Bazar, Bangladesh.

On the US/Mexico border, one young man drowned crossing the Río Bravo near Reynosa in Tamaulipas, Mexico – bringing to eight the known drownings on the river so far, this year.

## Launch of \$96.2 Million Appeal to Support Yemenis and Migrants Impacted by Conflict

The IOM has launched an appeal for USD 96.2 million to fund its 2018 response for what is being called 'one of the worst humanitarian crises in the world' in Yemen.

Due to a protracted economic crisis, intermittent conflict, and weak rule of law, Yemen was already facing chronic

vulnerabilities even prior to the escalation of conflict.

The conflict has also displaced some 2 million Yemenis within their own country, according to the Task Force on Population Movement.

## Facilitates Release of Refugees from Indonesian Detention Centres

The IOM has facilitated the release of over 500 refugees from immigration detention centres in North Sumatra, Riau, and Riau Island provinces to community housing.

The release of the Afghan, Somali and Sudanese migrants took place recently and was organized in close cooperation with Indonesia's Immigration Department, local government officials and police.

All of the released migrants had been intercepted and detained by the Indonesian authorities while trying to reach Australia. While in detention they were identified as

refugees by UNHCR. This made them eligible for release and housing in the community, where they will await third country resettlement or voluntary return to their home countries when it is deemed safe to do so.



## CBP Announces First Automated Passport Control System On Board a Ferry Vessel

Ferry transports passengers and cargo between the ports of San Juan, Puerto Rico and Santo Domingo, Dominican Republic



U.S. Customs and Border Protection (CBP) announced Friday, along with the vessel operator of Ferries del Caribe, the implementation of the first Automated Passport Control (APC) System on board the San Juan-Santo Domingo ferry.

The formal announcement was made on Jan. 26 at the Pan American Dock in San Juan, with participation from leadership of America Cruise Ferries, parent company of Ferries del Caribe, and representatives from the Commonwealth of Puerto Rico's Department of State, Department of Economic Development, Tourism Company and Port Authority.

"APCs have been adopted at international airports around the Nation providing travelers shorter wait times, less congestion, and faster processing," indicated Edwin Cruz, Area Port Director. "With this APC on board the ferry, passenger clearance is facilitated in such a complex operation while sustaining our security standards."

The APC is a program that expedites the entry process for U.S. citizens, U.S. legal permanent residents, Canadian citizens, Visa Waiver Program eligible international travelers, and travelers entering with a B1/B2 or D visa, by providing an automated process through CBP's Primary Inspection area.

Travelers use self-service kiosks to respond to CBP inspection related questions and submit biographic information. APC is a free service, does not require pre-registration or membership, and maintains the highest levels of protection when it comes to the handling of personal data or information..

People scan their passport and submit answers to the custom's declaration in the kiosk. This Information is collected and compiled by the site server and transferred to a secure server on the CBP network for a quick response. A receipt is then printed from the kiosk which the traveller takes to a CBP Officer upon arrival who verifies the document and makes the final approval to allow a traveller into the country.

CBP maintains a strict security protocol for any system that collects or contains personally identifiable information (PII) including meeting all privacy requirements. No information is stored on or shared by the site server/kiosk.

APC kiosks onboard the M/V Kydon are developed by Innovative Travel Solutions, an independent business unit within Vancouver International Airport (YVR). These particular BorderXpress kiosks were configured to meet the immigration needs of CBP for Ferries del Caribe. The ferry navigates between the ports of San Juan, Puerto Rico and Santo Domingo, Dominican Republic, transporting passengers, vehicles and cargo, three times a week.

During the announcement, America Cruise Ferries, shared that two of its strategic business units, Marine Express and Priority Ro Ro, became part of the Customs-Trade Partnership Against Terrorism (CTPAT) a voluntary public-private sector partnership program which recognizes that CBP can provide the highest level of cargo security only through close cooperation with the principle stakeholders of the international supply chain such as importers, carriers, consolidators, licensed customs brokers, and manufacturers.

When an entity joins CTPAT, an agreement is made to work with CBP to protect the supply chain, identify security gaps, and implement specific security measures and best practices. Applicants must address a broad range of security topics and present security profiles that list action plans to align security throughout the supply chain.

## FRONTEX Launching New Operation in Central Med



Frontex, the European Border and Coast Guard Agency, is launching a new operation in the Central Mediterranean to assist Italy in border control activities.

The new Joint Operation Themis will replace operation Triton,

which was launched in 2014. Operation Themis will continue to include search and rescue as a crucial component. At the same time, the new operation will have an enhanced law enforcement focus. Its operational area will span the Central Mediterranean Sea from waters covering flows from Algeria, Tunisia, Libya, Egypt, Turkey and Albania.

“Operation Themis will better reflect the changing patterns of migration, as well as cross border crime. Frontex will also assist Italy in tracking down criminal activities, such as drug smuggling across the Adriatic,” said Frontex Executive Director Fabrice Leggeri.

The security component of Operation Themis will include collection of intelligence and other steps aimed at detecting foreign fighters and other terrorist threats at the external borders.

## Spanish National Police and Guardia Civil join forces with Europol in a hit against Iraqi illegal immigration to the EU



Europol supported seven mixed teams of Spanish National Police (Policía Nacional) and Guardia Civil in a successful strike against Iraqi illegal immigration in which six individuals were arrested in Spain. The criminal organisation transferred Iraqi illegal immigrants from their country into the Schengen Zone.

The investigation began last February when Spanish police officers found six individuals from Iraq inside a refrigerated truck in Teruel (Spain). On the same day and

later on in March they located two people concealed in the same conditions in Valencia, alongside eight illegal immigrants in Teruel, who called the emergency services as they feared they were dying from the cold inside the truck.

The network transferred the Iraqi illegal immigrants from Spain to the UK inside refrigerated trucks. The criminals took advantage when the drivers were sleeping to introduce the people inside the vehicles. They were a group composed of six to eight individuals or families with children and they had to stay in the truck for 30 or 40 hours under temperatures that were not higher than 4°C.

Spanish police officers carried out six house searches in Spain. As a result, a large amount of documents, several electronic devices and EUR 15.000 plus USD 8.000 were confiscated. Five individuals were arrested in Valencia, alongside one in Bilbao. Currently, the suspects are being interrogated while the forensic teams are performing the extractions of the mobile devices.

# ILLEGAL MIGRATION IN EASTERN EUROPE AND UKRAINE

Lieutenant-colonel Olga Derkach is Senior officer, International Cooperation and Eurointegration Department, Administration of the State Border Guard Service of Ukraine, PhD in Public Administration



Ukraine with more than 1.400 km of border with the European Union, taking into account its geographical location, is traditionally defined as one of the transit migration countries.

At the same time with recall on agency statistics and FRONTEX data (annual analysis of threats on the eastern borders of the EU) it is worth to emphasize:

- The migration situation in Ukraine is not threatful. Illegal migration has not become a significant problem (issue) for the Ukrainian state.
- Ukraine is not the main transit route for migrants, who are going to Europe,

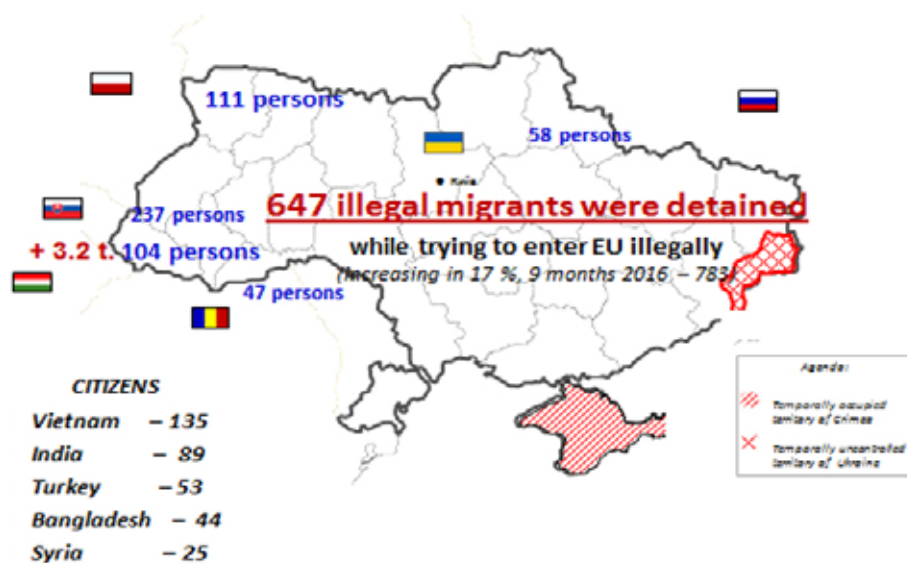
because of its geographical position.

Across the common Ukrainian-EU border and borders with other Eastern Partnership states, not a big number of migrants reach the European Union.

It means that the so called "eastern" route of illegal migration flow, which crosses the territory of Ukraine, is not dangerous for Ukraine.

In 2017, Ukraine faced the tendency of a decreasing of number of illegal migrants detained for trying to enter European Union illegally (10 months of 2017 – 553, 9 months of 2016 – 783).

Most of the illegal migrants were



detained on the border with Hungary – in 3.2 times (9 months 2017 – 104, 9 months 2016 – 337), which can be explained by the changes of migration policy – more severe than it was before 2015.

At the same time, there was an increasing number of migrants detained on the border with the Republic of Poland (on 42%, 9 months 2017 – 111, 9 months 2016 – 78), Slovakia

(on 39%, 9 months 2017 – 237, 9 months 2016 – 171), and Romania (on 15%, 9 months 2017 – 47, 9 months 2016 – 41).

This was due to not only the changes of migration flows but also as the consequences of effective enhancement of the border and the fulfillment of joint coordination measures.

Because of the capacity enhancement on the eastern borders the number of apprehended illegal migrants on the border with the

Russian Federation, i.e. on the main channels of migrants' arrival to Ukraine (in 2.5 times, 9 months 2017 – 58, 9 months 2016 – 25).

The main category of illegal migrants, detained at the trial to enter the EU via the territory of Ukraine, were citizens of Vietnam (135), India (89), Turkey (53) and Bangladesh (44).

It should be mentioned that under the certain circumstances the illegal migration flows changed not only in figures, but also in quality.

In 2016, the main category of illegal migrants were citizens of Afghanistan, in 2017 – only 8 Afghans were detained (increasing in 20 times)

Mainly this was the result of effective and efficient counteraction of Ukraine law-enforcement bodies against an organized "Afghan" channel.

Last year the main efforts were concentrated on combating the

organizers of a transit "Vietnamese channel", first of all to Slovakia.

In close cooperation with Slovak colleagues, the State Border Guard Service of Ukraine detained 143 citizens of Vietnam.

On legal channels migrants use:

a) valid passports and visas, issued on faked invitation of educational establishments and touristic vouchers of not existing firms and offices;

b) forged and false passports, passports which do not belong to the holders and temporarily residence permissions;

c) scheme of "transit via the territory of Ukraine" using aviation direction, which foresees change within the transit zone one of Ukrainian place of destination for the flights towards the EU states and usage of new passports (more often forged).

In 2017 the number of cases with usage of forged documents on the border with European Union increased, first of all on the border with Romania, Poland and on the marine sector of border.

More often, the citizens of Turkey (35) and India (14) used forged and false documents.

Besides that also 207 citizens of Ukraine.

The efficient system of advanced warning about potential illegal migrants entering into Ukraine decreases the migration pressure on the EU border (10 months 2017 – 3 648, 10 months 2016 – 2 754)



## IMPROVING BORDER SECURITY



**The operational border protection ROAD MAP is implemented**

### JOINT CONTROL

Is conducted on the border with **Poland (4 BCPs)** and **Moldova (6 BCPs)**

Legal regulation with **Slovakia** is approaching conclusion



### JOINT PATROLING

Is implemented with **Slovakia, Poland, Hungary, Romania and Moldova**



### CONTACT POINTS

At the border with **Poland (2 CPs)**, **Romania, Hungary and Belarus.**

At the same time, we define activation of the usage of legal channels to enter Ukraine by the potential migrants from India (297), Alger (176), Morocco (111), Livia (85), Pakistan (73), and Turkey (71).

Ukraine as a country of migration origin is estimated frequently within the context of searching of illegal opportunities to enter the EU states and very rarely in the context of illegal migration.

In its resume for the last year, FRONTEX counts only 57 cases connected with illegal migration of citizens of Ukraine.

Under the conditions of the visa liberalization regime for Ukraine, the significant incensement of declining entrance to Europe for the citizens of Ukraine did not happen.

True, illegal migration remains the challenge to Ukraine, but to tackle

it the State Border Guard Service of Ukraine:

- Implements the operational border protection ROAD MAP with EU-neighboring countries,
- Conducts JOINT CONTROL on the border with Poland (4 BCPs) and Moldova (6 BCPs)
- Enhances a COMPLEX SYSTEM OF STATE BORDER PROTECTION AND CONTROL and reaction capacity
- Organizes JOINT PATROLING with Slovakia, Poland, Hungary, Romania and Moldova
- Opens CONTACT POINTS at the border with Poland (2 CPs), Romania, Hungary and Belarus.



## CBP & Cayman Islands Partner for Airport Fast Track Pilot Program



U.S. Customs and Border Protection (CBP) and the Government of the Cayman Islands reached an agreement Tuesday to implement a pilot program that will permit screening of passengers traveling from the Miami International Airport (MIA) to the Owen Roberts International Airport (GCM).

“This pilot is an important element to address our international engagements particularly with partners in the Caribbean” stated Todd C. Owen, Executive Assistant Commissioner for the CBP Office of Field Operations. “With this agreement we can enhance aviation security, detect fraudulent documents and facilitate air travel between the two countries without inhibiting legitimate lawful travelers.”

The program, called the Airport Fast Track (AFT) Pilot, will allow for Grand Cayman immigration and custom officers to screen passengers at the Miami airport, without any law enforcement or other executive authority in the United States. Upon arrival in Grand Cayman, passengers who volunteer to be pre-screened in Miami will be expedited through the arrival process, saving time and making the Cayman entry process simpler.

“It is the first time that the US has entered into such an arrangement with another country and will be the first time that our Customs and Immigration officers will be deployed overseas in such a role. It will introduce a new fast track procedure at the airport and help to improve customer experience at peak weekend times,” stated Premier Hon. Alden McLaughlin.

The AFT is similar to CBP’s Immigration Advisory Program (IAP) implemented at various international airports. The IAP is designed to protect air travel and improve security by sharing techniques and information with partnering host governments.

In screening both foreign visitors and returning U.S. citizens, CBP uses a variety of techniques to intercept narcotics, unreported currency, weapons, prohibited agriculture, and other illicit products, and to assure that global tourism remains safe and strong.

## Working Visit by Malaysia Marine Police Force to ASEANAPOL



The ASEANAPOL Secretariat received a working visit by SAC Dato’ Abdul Rahim bin Abdullah, Malaysia Marine Police Force and his entourage. They were warmly welcomed by Executive Director, Police Colonel Kenechanch Phommachack, Director for Plans and

Programmes, ACP Aidah Othman, Director for Police Services, Supt. Jim WEE and officers of the Secretariat.

During the meeting, Malaysia Marine Police Force (MMPF) shared on their first Trilateral cooperation among MMPF, Singapore Police Coast Guard (SPCG) - Indonesia Marine Police (IMP) towards the maritime security along the South Malacca Straits. The meeting had been fruitful and both parties have agreed on the importance of having mutual collaboration and cooperation amongst members country and future capacity building needs. ASEANAPOL Secretariat also encouraged the sharing of this successful project via e-ADS.

Executive Director further expressed his sincere thanks for the cooperation and continued support given by Malaysia Marine Police Force.

# ADOLFO SUÁREZ MADRID BARAJAS AIRPORT

Adolfo Suárez Madrid Barajas Airport is the main airport in Spain but is also as one of the main air hubs in Europe, with an ever-increasing number of passengers.

Jesús Gómez, Chief Commissioner of Madrid Barajas Airport and Police HQ for the Spanish National Police gives an overview of the measures in place to promote Integral Management for Border Security at the Airport.

The increasing number of passengers poses particular challenges, primarily meaning having less time for the entire process of person identity verification, document authentication, and efficiently detecting those passengers which should undergo a more thorough check.

Great efforts have been undertaken to facilitate the travel of bona-fide passengers whilst simultaneously maintaining a high level of security; making the border control processes more efficient and secure.

The security issues we are facing in terms of immigration, come in an almost endless variety of forms, from document fraud (fake documents, document swapping, undocumented passengers), impostors, transit abuse, increasing numbers of asylum seekers, smuggling and trafficking in human beings.



To ensure we are in a position to face these security issues we have implemented a range of security developments including:

- Smart Borders: because of the increasing efficiency of these machines the number of Automated Border Control gates or e-gates has steadily been increased. There is a ongoing project to increase the number of e-gates in many Spanish airports, both to enter and to exit the Schengen territory.
- Technological renewal: new verifiers, with the latest software, have been put in place in every control booth.
- The use of the API system (Advanced Passenger Information) is vital to control all passengers coming from a 3rd country airport entering the Schengen State.
- The Passenger Name Record (PNR) is a tool we are also using to identify how many passengers can be sensitive to be victims of smuggling or THB.
- Visa Information System (VIS) a database containing information, including biometrics, on visa applications by Third Country Nationals requiring a visa to enter the Schengen area.

- Gate checks as a countermeasure to prevent cases of transit abuse and also to prevent the destruction of documents in order to arrive undocumented at the border control.
- Cooperation with airlines companies to control, in a 3rd country airport, passengers with a certain profile that may want to destroy their passports upon arrival, so nobody arrives undocumented.
- Cooperation with liaison officers is also a key factor in terms of document fraud.

New security technologies we are planning to implement for the future are based and in line with EU projects:

- ABC4EU: This programme is complimentary to Smart Borders, to develop a database with frequent passengers, and these passengers

Madrid Barajas Airport operator AENA, has been steadily investing in new security measures at the airport over a number of years.

The CGA (Centro de Gestión Aeroportuario - Airport Coordination and Management Center), located in T4, is the coordination centre for the entire airport.

When it came to selecting a video surveillance system, AENA needed a flexible solution that was capable of integrating all the existing systems while offering sufficient capacity to manage the huge increase in traffic anticipated in the new and existing terminals.

This project therefore represented an enormous challenge considering the huge surface area, the number of buildings to monitor and the amount of programmed equipment involved.

Bosch systems were the chosen solution for the airport, thanks to the large capacity of the 8 Allegiant Matrix Switcher, providing distributed architecture and ease of integration, combined with the high quality offered by both the fixed (approximately 500 Dinion) and PTZ (approximately 500 AutoDome) cameras. The global management system consists of various matrix switchers, each with a capacity of over 4000 inputs and 500 outputs, more than 3000 cameras distributed across all four terminals and, at peak times, more than 10,000 accesses an hour.

Spanish information technology company, Indra was awarded the contract to install multi-biometric electronic access kiosks. Indra selected VeriFinger, VeriLook and MegaMatcher from Neurotechnology to be the multi-

biometric engines for the airport access-control kiosks.

The solution developed by Indra allows passengers, after being identified in a kiosk, to perform a quick and simple procedure that includes the automatic reading of the electronic document and validation of its authenticity. The passenger is at the same time identified and matched to their document through biometric recognition and verification. Upon completion of this process the traveller is issued an entry permit. Each individual process is supervised by officials of the National Police.

While similar systems have been established in other countries using a single biometric feature, such as the iris, fingerprint or face to verify the passenger identity, the Spanish system performs a more secure dual-biometric test using facial and fingerprint recognition. It is for this multi-biometric verification that Indra chose the Neurotechnology product line.

No prior passenger registration is required to use this system, the biometric information present in the document is sufficient. This enables the use of the national electronic ID card to enter the Schengen area.

Smith's Detection won the contract to supply 10 Spanish airports, including Madrid, with more than 120 high-speed X-ray scanners to check hold baggage for explosives and other threat items. The HI-SCAN 10080 EDX-2 which accepts baggage sizes of up to 100 x 80 cm, can screen as many as 1,800 bags per hour. Its dual view feature allows the operator to 'look around' objects for rapid and accurate evaluation, sharply cutting re-inspection rates and saving on time and labour costs.

will be able to cross the Spanish border quicker and easier as nowadays.

- RTP (Registered Traveller Program): Bilateral agreements with 3rd country nationals to share lists of frequent passengers.
- Entry / Exit System: Schengen data base with the aim to improve border management and fight against illegal immigration by also calculating and not exceeding the length of stay. Replacement of manual stamping.



## Mexican Federal Police foil 11,500 illegal cargo of diamonds



As part of the surveillance and verification work against different types of contraband at the International Airport of Mexico City, the Federal Police arrested a subject of Spanish nationality, who was carrying an estimated

shipment of 11,500 diamonds, of which He could prove his legal provenance.

Staff from the Regional Security Division, attached to the air terminal, when conducting an analysis of the behavior of passengers who were about to board a flight to Colombia, identified some nervousness in the Spanish citizen who was asked to perform a check on his carry-on baggage.

The federal agents detected a double bottom in his backpack where he hid several plastic bags with hundreds of small crystals, and in a body check it was also discovered that he had attached to his body, other bags with more of these precious stones.

Since he did not document the shipment, in addition to not proving his legal provenance, this person was presented before the Public Ministry of the Federation and the immigration authorities, where an estimated 11,500 pieces of what is considered the hardest mineral was counted. of the planet.

## Hundreds of drug seizures made in joint Australian-Dutch operation

Over 270 attempts to import illicit drugs into Australia were foiled after the Australian Border Force (ABF) and the Netherlands Tax and Customs Administration (Dutch Customs) joined forces to target international mail items between the two countries.

During a week of action from 5-11 February, the two agencies coordinated their intervention activities in mail centres to stop attempted importations of illicit drugs and precursors such as MDMA, methamphetamine, cannabis, cocaine and ephedrine.

The ABF devoted additional resources at the International Mail Gateway Facilities in Sydney, Melbourne, Perth and Brisbane to support the activity and together with Dutch Customs carried out over 1000 detailed physical examinations.

The officers detected a range of illicit drugs including methamphetamine, GBL, cocaine and MDMA.

ABF Assistant Commissioner, Strategic Border Command, Kaylene Zakharoff said the operation provided a great opportunity to build on the already strong relationship with the ABF's Dutch counterparts.

"We work closely with customs and law enforcement agencies around the world, and operations like this allow

officers from both nations to share information, resources and expertise," Assistant Commissioner Zakharoff said.

"Together we have stopped a significant amount of illicit drugs from reaching the Australian community and we thank our Dutch friends for their assistance. We look forward to continuing our longstanding partnership with this key international partner.

"This operation demonstrates the ABF's commitment to disrupt the international supply of methamphetamine ('ice') and chemical precursors to Australia by strengthening international engagement. These substances pose a significant security and health threat to Australia and our region."

Bert Wiersema, Acting General Director Dutch Customs stressed the importance of international Customs cooperation to combat drug trafficking from and to Europe.

"This cooperation with Australian Border Force is a splendid example of joining forces and intelligence to disrupt this kind of illegal activity," Wiersema said.

Both ABF and Dutch Customs are committed to undertaking further joint initiatives in the future.

# IOM NIGER: IMMIGRATION AND BORDER MANAGEMENT

Niger, a country still in the initial phases of development (187/188 UNDP HDI 2016), is located on the southern edge of the Sahara at the center of the West African Sahel region spanning 1,267,000 km<sup>2</sup>, three quarters of which are occupied by the Sahara desert. Niger is affected by surrounding conflicts, periodic episodes of drought and floods, and has faced a massive influx of migrants coming mainly from other ECOWAS countries.



With 5,697 kilometers of borders with Burkina Faso, Mali, Algeria, Libya, Chad, Nigeria and Benin, Niger is the main crossroads for migration and exchange in West and Central Africa, and faces multiple persistent challenges. The main challenge remains the security threat of regular incursions by armed groups, notably along the borders with Nigeria and Mali. These recurring incidents weaken the state and negatively impact the security of populations living at the border. The adverse socio-economic consequences of these incursions make the resilience of these communities uncertain. Instability in neighboring countries also assists in the development of

trafficking and smuggling at Nigerien borders.

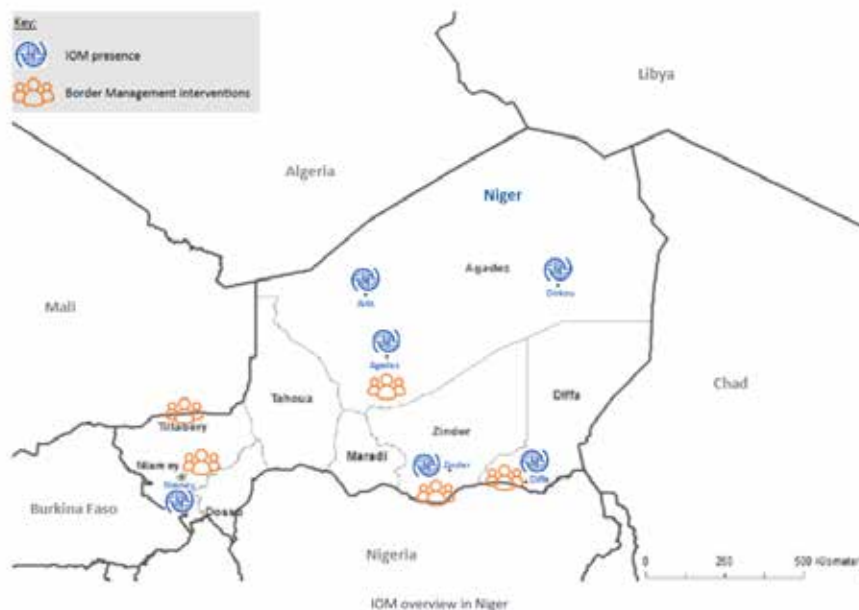
Thus, the surveillance and security of Niger's borders are essential in reducing the risk of incursions which can threaten the stability of the State of Niger. Effective border management requires both an optimization of strategies to streamline socio-economic exchanges and the transportation of goods and persons, as well as the development of border zones to combat issues of desertification. In total, supporting communities on both sides of the border is essential for combatting the desertification of these zones, which can enable the

mobility of transnational criminal activity.

Over the course of the past few decades, the movement of goods and persons has considerably increased, requiring improved structures for immigration and border management in order to more effectively manage cross-border flows. As a result, States are faced with a common objective: to better facilitate the legitimate movement of persons and goods while maintaining secure borders.

Thus, the Immigration and Border Management unit supports IOM's global strategy, and implements activities which aim to assist States in reinforcing their structures and procedures in the management of borders and migration; to reduce irregular migration and trafficking of migrants; to reinforce the protection of migrants' rights; to reinforce international cooperation; and to harmonize national policies and practices both internally and in a regional context.

In Niger, the IOM Immigration and Border Management Unit has been active since 2015 and implementing projects with the aim of reinforcing border management in Niger and the Sahel. Thus, border management projects notably aim to assist the Government of Niger in developing the human, infrastructural, material, and institutional capacities of the National Police and all of the border security forces. Additionally, border communities are regularly assimilated into border management activities in order to facilitate dialogue with the administrative and



cultural authorities in Niger, thus increasing their resilience when faced with criminal activities.

**Research and Studies**

In order to allow for a better understanding of the context, security challenges, economic issues, and movement of communities living near the borders in Niger, IOM engages in research and publishes studies.

Since 2015, the IOM Niger Immigration and Border Management unit has published four studies, first 'Cartographie et présentation de la gestion des frontières au Niger', which gave an overview of the security and migration context, with the aim of illuminating the political, regulatory, and institutional framework.

The second study published,

'Communautés transfrontalières au Sahel – Enjeux économiques et défis sécuritaires', explored communities' understanding of and relationships to the border, as its sometimes superficial and occasionally restrictive nature affects their everyday lives, yet provides enriching cultural exchanges and business opportunities.

The third publication, the 'Etude des flux sur les frontières Niger-Nigéria et Niger-Tchad dans la région de Diffa', had the goal of observing the nature and the ins and outs of migration flows through Diffa, the crossroads region of the Lake Chad Basin.

Finally, the last study, 'Border security: Communities' integration and perception – Diffa and Zinder regions', has illuminated the perceptions of communities in Diffa and Zinder on border security management, and the security risks

and terrorist threats which affect this part of the Niger basin.

### Trainings

IOM supports the Government of Niger in developing of technical knowledge and reinforcing institutional capacities in a sustainable manner. In addition, the Immigration and Border Management unit promotes and organizes the training of police officers in Niger through the development of training modules, training of trainers, and the organization of trainings for police agents. In Niger a variety of themes are addressed, including migration, border security, infractions at the borders, documentary fraud, smuggling and trafficking of migrants, information technology (including the MIDAS system – see the 'MIDAS System' section below), and the use of topographic maps and GPS.

Since 2015, the IOM Immigration and Border Management has supported the development of five training modules which have been incorporated into the initial training of police officers at the National Police Academy in Niamey. Four agents from the Nigerien border police were trained as trainers by international experts in February 2016, allowing for the subsequent training of other police agents. By the end of 2016, over 130 agents had been trained.

In addition, the work of the border police has been supported through the development of a practical guide on border control procedures, which contains instructional tools to

train agents on topics pertaining to national security and respecting the rights of migrants and travelers.

### Construction

Faced with the challenge of managing Niger's long and porous borders, IOM also supports the Government of Niger in the sustainable reinforcement of infrastructural capacities. This component aims to reinforce crucial infrastructure in Niger due to its strategic importance in maintaining security at sensitive points along the border. Thus, buildings which are rehabilitated or constructed (such as Police Border Posts) are identified and architectural plans are drawn up jointly with the National Police, with the aim of reinforcing the capacities of the Directorate of Territorial Surveillance (DST) in exercising their mandate.

In 2016, the IOM Immigration and Border Management unit constructed its first Police Border Post in Niger at Kongokiré (Tillabéry region), followed by a second construction at Gaidam (Diffa region), which was inaugurated in May 2017. In order to be entirely and immediately operational, each post was constructed with an administrative building, booths, solar panels, drilling, a generator, and exterior bathrooms.

### Equipment

IOM supports the Government of Niger in reinforcing material capacities, with a view towards quality and efficacy. IOM thus supports the National Police in performing their functions through

the provision of materials such as office and computer equipment, as well as equipment for mobility, communication, and detecting and combatting documentary fraud.

Since 2015, the IOM Immigration and Border Management unit has donated six vehicles to the National Police for border patrols in Diffa region, UV lamps (some of which were given to the National Police Academy for training), night vision goggles, metal detectors, GPS units, and satellite phones (allowing for better communication with the populations, and the administrative and customary authorities who also received satellite phones), as well as office and computer supplies to equip the two Police Border Posts which were constructed.

### MIDAS System

IOM supports the Government of Niger in collecting data and information on migration. Well-designed information management systems can considerably improve the capacity of the State in managing its borders and in forming evidence-based migration policies.

IOM has developed its own information system for border management, called the Migration Information and Data Analysis System (MIDAS), which allows for the collection and analysis of information on travelers/migrants. Already used in more than 23 countries around the world, MIDAS collects, processes, stores and analyzes data on travelers in real time, thanks to an extensive network at borders. It permits States to more effectively control



persons entering and exiting their territory, all while providing a solid statistical basis for migration policies. IOM guarantees to Governments complete and exclusive ownership of all data registered with MIDAS.

The MIDAS system was installed by IOM in Niger in 2016 at the central level, within the Directorate of Territorial Surveillance (DST), and at the Kongokiré Police Border Post (Tillabéry region). In 2018, IOM plans to equip 3 other posts with this system. The installation of the system at police posts is accompanied by a MIDAS training for the police agents who will be maintaining and/or using the system on a daily basis.

### **Regional Cooperation**

Regional cooperation promotes and supports the harmonization of policies and strategies on border management in order to support the development and implementation of joint border management strategies in the Sahel. As they are faced with numerous security threats in the Sahel, States must exchange information, coordinate their actions, and share best practices with the objective of improving security in the region. Thus, the governments of the Sahel have on numerous occasions insisted on the creation of a more concrete operational framework for coordination between the directors of border security forces.

Since 2015, the IOM Immigration and Border Management unit has organized regional meetings between Niger and the other countries of West and Central Africa. The central level meetings include



regional workshops on border management, meetings of directors in charge of border security, and one meeting focusing on border management coordination in the Lake Chad region. Additionally, meetings have taken place at the local level, notably bilateral meetings between the police of Niger and neighboring countries.

### **Integrated Border Management**

In order to assure free movement of goods and persons, as well as safe migration within the Sahel region, IOM supports the Government of Niger in the necessary establishment of integrated and inclusive border management. Integrated border management requires all relevant authorities to work together in an efficient manner. Thus, IOM assists the Government of Niger in reinforcing operational capacities at key crossing points on the borders, and in improving concerted cooperation on border management between various actors (inter-service, interagency, and international

cooperation).

In 2017, the IOM Immigration and Border Management unit supported integrated border management in Niger through the organization of a study visit to Tanzania for the DST and the General Directorate of National Customs in order to exchange best practices, constraints to be respected, criteria to observe and objectives to be attained within the domain of interoperability between services in charge of border management. This study visit allowed the Nigerien delegation to benefit from the example already implemented at the Holili border post in Tanzania.

### **Humanitarian Border Management**

Humanitarian Border Management (HBM) is a notion conceptualized and elaborated by IOM, concerning operations at the border before, during, and after humanitarian crises which precipitate mass migration movements. The objective

of this concept is to guarantee the protection of vulnerable persons affected by the crisis and the respect of their interests and human rights, all while respecting national sovereignty and security. Humanitarian Border Management takes note of the need to bring appropriate responses in border management during humanitarian crises resulting from a natural or man-made disaster. The objective is to improve preparation and responses in order to protect those who cross borders in emergency situations and guarantee border security.

In 2016 and 2017, the IOM Immigration and Border Management unit organized two regional workshops on Humanitarian Border Management, bringing together for the first time institutional partners from Burkina Faso, Mali, Niger, Mauritania, and Côte d'Ivoire from the Ministries of Interior, Foreign Affairs, Health, and Humanitarian Action, and for a second time the institutional partners from Niger and Nigeria from the Ministries of the Interior and Humanitarian Action. These workshops provided a forum for international and inter-ministerial exchanges on legal frameworks and current national mechanisms for crisis response. They allowed participants to engage in dialogue on the sustainability of regional emergency coordination structures, and to formulate recommendations for the governments of participating States.

In addition, the IOM Immigration and Border Management unit organized two crisis simulation

exercises in 2017. These exercises, based on fictitious scenarios of mass population displacement, aimed to observe the reaction of regional and local authorities in order to identify the capacities of the current crisis management system as well as the areas in need of additional technical and material support. Additionally, the exercises aimed to put the representatives from the Nigerien authorities and state services present in the field in direct contact with the local population, all engaged in the same response to a major crisis. Based on the results of the first exercise, an inter-ministerial group drafted a national contingency plan to be applied in cases of sudden changes at the border in Niger, which was then implemented and tested at the second simulation exercise.

### Community Engagement

With the goal of ensuring the free movement of goods and persons, as well as safe migration within the Sahel region, IOM assists the Government of Niger in the establishment of integrated border management, which is crucially supported by community development activities. IOM assists communities living at the borders in Niger in order to encourage the

population to collaborate with Nigerien defense and security forces, as well as to improve resilience to violent extremism and prevent desertification. To do this, IOM organizes sensitization campaigns, supports socioeconomic activities in communities with material donations, and provides communication equipment to administrative and traditional authorities.

Since 2015, the IOM Immigration and Border Management unit has organized sensitization campaigns on life at the border and the role of local populations in border security. The unit has also encouraged the resilience of border communities through the provision of economic materials (carts, motorcycle tricycles, grain mills, motorcycle pumps, etc.) and through the implementation of community works (stabilization of dunes). Finally, the Immigration and Border Management unit has put in place community prevention committees in border villages in Diffa and Zinder regions, which relay pertinent information concerning border security, including health and humanitarian concerns, to communal, departmental, and regional authorities.



# CARICOM'S REGIONAL BORDER SECURITY ARCHITECTURE

The CARICOM Implementation Agency for Crime and Security (IMPACS), established in 2006, is the “nerve center” of the Security Management Framework with primary responsibility for the implementation of the regional crime and security agenda.



Primary amongst these is “Border Security”. IMPACS inclusive of its two (2) sub-agencies - the Joint Regional Communications Centre (JRCC) and the Regional Fusion Centre (RIFC) - plays a vital role in providing support to the national security entities and by extension, protecting the security of Region.

The JRCC manages the only multilateral Advanced Passenger Information System (APIS) in the world. Currently the JRCC receives the submission of APIs for eleven CARICOM Member States and by the end of 2018, the Agency will receive and analyse the APIs for the remaining four full CARICOM Member

States thanks to the support from the Government of the United States of America and the European Union under the 10th EDF, bringing the total to fifteen states. This is a critical achievement because the analysis which takes place is supported by regional and international watchlists and Third State partners. The result is that the analysis not only supports the receiving countries but it allows macro-level trends to be identified in a timely manner supporting early warning systems for the Region.

For 2017, the Agency received and processed in excess of 64 million crew and passenger movements; resulting in 4,363 Nominal & SLTD

Hits being identified against the CARICOM Watch List Databases with a number of subsequent arrests and refusals.

Under its mandate to develop the Region's human resource capacity and to support the current regional mechanisms, the Agency over the period December 2016 to present has conducted training for border security official (immigration and customs) under the theme - "Strengthening CARICOM Capacity to prevent and detect illegal activity at its borders and to enable increased prosecution and higher conviction rates." Under the aegis of the 10th European Development Fund (10th EDF) and with technical support from the US Customs and Border Protection (CBP), approximately three hundred and sixty (360) officials have received training in areas such as Targeting Air & Sea Passengers and Cargo; Travel Documents Analysis; Imposter Detection and Behavioural Analysis; Human Smuggling & Human Trafficking and Integrity: Ethics and Corruption, to name a few. This training included a train-the-trainer component which supported the Region's mandate to develop a cadre of border security trainers and, as a result, the Agency utilises this body of trainers to continue some of its border security training. However, it has been recognized that there is a need to take this training a step further, therefore IMPACS is currently negotiating with regional tertiary institutions to not only certify the trainers but to accredit future training courses being offered in the Region. The intent is to ensure that training for CARICOM Border Security



Joint Border Security Training in Jamaica- 1-5 May, 2017 (Kingston, Jamaica)

is harmonized and that approaches, where possible can be harmonized as the Region is moving towards the seamless free movement of persons, goods and services under the CARICOM Single Market and Economy (CSME).

Under this programme, along with others under the CARICOM Crime and Security Strategy; the CARICOM Counter Terrorism Strategy and the CARICOM Counter Illicit Trafficking Strategy, IMPACS will continue to seek to address the threats of transnational organized crime with respect to illicit activities such as human trafficking, migrant smuggling and trafficking of other commodities such as illegal drugs, guns and ammunition. This will be achieved through better management of our borders and enhancement to existing systems that manage and analyze information

to ensure the timely and efficient dissemination of same to all stakeholders and Member States alike.

## Border Pass Management System Facilitates Cambodian-Thai Border Crossing



Cambodia's General Department of Immigration has launched a new border pass management system at the Doung International Border Control Post, in Battambang province on the Cambodian–Thai border. The system will use software developed by IOM, the UN Migration Agency.

The Migration Information and Data Analysis System (MIDAS) has been installed, with financial support from Canada, to allow Cambodia to more effectively manage cross-border movements of local residents and migrant workers traveling with border passes.

Expediting border procedures is an important element of economic cooperation between the two countries. People using border passes need to be quickly and accurately identified and registered, within the mixed flow of migrants moving back and forth across the border. This calls for a cost-efficient solution that balances security with facilitation.

MIDAS is a powerful border management information system that processes and records all information about border pass travellers, including their biographical data and facial images. It also provides a systematic registration of all entries and exits, allowing for analysis of statistics and trends to inform evidence-based migration policies.

“MIDAS answers a real need,” said General Sok Phal, Cambodia's Director of Immigration. “It allows for more effective border management of local Cambodian border residents entering and leaving Cambodian territory, while providing a solid statistical basis for migration policies and strategies.”

The new system can also register minors (in Cambodia, this is any person under the age of 12) travelling with a legal parent or guardian. Photos and birth certificates are captured and stored in a database, which allows immigration officers at the border to verify the identity of both the adults and the children travelling with them. This offers protection against child trafficking and identity fraud when issuing border passes.

“The system, which was installed in November and now processes on average 1,000 crossings a day, is already demonstrating significant potential to provide Cambodian immigration and provincial authorities with an overview of border pass movements,” said IOM project manager Brett Dickson. “Feedback from frontline immigration officers is also positive, showing that it makes identity checks and processing of border pass travellers easier and faster.”

“We hope MIDAS will help to optimize Cambodian border control posts and border operations for effective border management, and promote orderly cross-border migration,” added IOM Cambodia Chief of Mission Dr. Leul Mekonnen. “It should also help to reduce irregular migration by facilitating and expediting regular movements, ultimately helping to ensure the safer movement of migrant workers and border residents.”

Currently, MIDAS is only installed in Battambang Province on a pilot basis. The Cambodian Government and General Department of Immigration have asked for the system to be scaled up and extended to five other border control posts along the Cambodian-Thai border.



# AGENCY NEWS AND UPDATES

## Mongolian border force team being trained by BSF



The Border Security Force (BSF) is giving sniper weapon training to the Mongolian border protection agency GABP.

“A ten-member team, comprising officers from the rank of sergeant to that of lieutenant colonel of Mongolia’s General Authority for Border Protection (GABP), is being trained in the use of sniper weapons,” said inspector general B K Mehta of the BSF’s Central School of Weapons and Tactics here.

## Indian police arrest most-wanted terrorist from Nepal border

Indian police claimed to have arrested one of its most-wanted terrorists who

carried a reward of 20,000 U.S. dollars on his head.

Officials said that Aariz Khan, alias Junaid, a member of home-grown terror outfit Indian Mujahideen, was nabbed by a special team of Delhi Police from the India-Nepal border.

“It’s a big catch as Khan had been absconding since 2008,” P.S. Kushwaha, deputy commissioner of Delhi Police, told the media..

## 562,961 expats arrested for violating Saudi labor, residency and border security laws



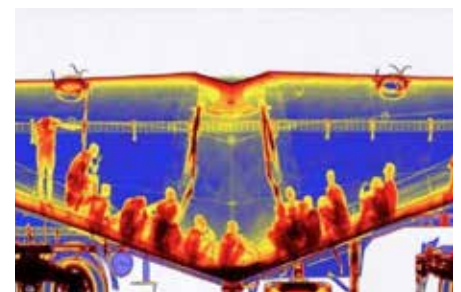
A total of 562,691 expatriates have been arrested since November last year for violating the labor, residency

and border security regulations of the country.

The program was carried out under the nationwide campaign dubbed “A nation without violators.”

According to an announcement from the Public Security Division in the Kingdom, those arrested included 382,921 who did not have valid residence permits (Iqama), 127,566 without valid work permits, and 52,204 people who had violated the border security system..

## UAE border police catch 22 people hiding inside concrete mixer



Border authorities have captured 22 people who tried to enter the United

Arab Emirates hiding inside a concrete mixer loaded on a truck, the country's WAM news agency reported.

The agency said that the Federal Customs Authority in the Emirate of Sharjah were able to stop the people smugglers at the customs center of the border shipping.

Capturing the illegal migrants reportedly took place in February, after the truck was inspected by the thermal and X-ray images as part of routine inspections at the border..

**B**order protection fence is a guarantee and a symbol



The border protection fence is the guarantee of Hungary's security, and a symbol of the fight against illegal immigration, the Parliamentary State Secretary at the Cabinet Office of the Prime Minister said at a press conference held on Monday at the Tompa border crossing station.

Csaba Dömötör stressed that the fence is also a symbol of the fact that it is possible to defend our communities and our culture.

He highlighted that the Hungarian people had stated their opinion on immigration on several occasions in the past few years. Their will points in a single direction: they want strong border protection..

**O**ne more border crossing point reopens along the Tajik-Uzbek border



One more border crossing point has reopened along Tajikistan's common border with Uzbekistan bringing the number of operational border crossing points (BCPs) along the Tajik-Uzbek border to four.

The "Qushtegirmon" border crossing point reopened in the Spitamen district (Sughd province) several days ago but official media outlets have not reported about that.

Recall, the "Patar" border crossing point reopened in the Konibodom district (Sughd province) on February 10.

**M**EPs visit Bulgaria to inspect Frontex operations at Turkish border



Members of the European Parliament's civil liberties committee are on a three-day visit to Bulgaria to see first-hand

how Frontex operations work at the border with Turkey.

The MEPs are to visit the region of the Kapitan Andreevo border checkpoint, where Frontex supports national authorities in carrying out border checks and gathering intelligence, the European Parliament said.

During the visit the committee members will meet, among others, Interior Minister Valentin Radev, representatives of the Border Police, international organisations as well as NGOs.

Addressing the meeting, Bulgarian Interior Minister Radev said: "We rely on the agency to strengthen the capacities for protecting the EU's external borders.

"Border security is one of the most important issues for the Union and for European citizens."

**B**order management: European Border and Coast Guard Agency strengthens operational cooperation with Albania

Commissioner for Migration, Home Affairs and Citizenship Dimitris Avramopoulos and Fatmir Xhafaj, Minister of Interior of the Republic of Albania, initialled the draft status agreement for operational cooperation between the European Border and Coast Guard Agency and Albania.

Once in force, the agreement will allow the Agency to provide assistance in the field of external border management and will enable European Border and Coast Guard Agency teams to be swiftly deployed on Albanian territory in case of a sudden shift in migratory flows.

## Canada to launch new border security app that could go global



The federal government is embarking on a new pilot program that will allow people to cross borders faster if they create a digital profile filled with their personal information on their mobile devices.

The Known Traveller Digital Identity is a joint venture between the governments of Canada and the Netherlands, and will be tested first on travellers going between those countries. The plan is to have it ready for a wider global rollout by 2020.

According to the World Economic Forum document outlining the program, international traveller arrivals are expected to jump from 1.2 billion in 2016 to 1.8 billion by 2030. This will increase risk and security requirements for the aviation and travel and tourism sectors.

Much like other trusted-traveller programs, the Known Traveller Digital Identity program will ask travellers for detailed personal information for pre-screening, including university education, bank statements and vaccination records.

## DHS budget includes funds for wall, cyber and border tech

President Donald Trump's fiscal year 2019 budget would give the

Department of Homeland Security significant money for technology to support a border wall, maintain the ongoing Einstein and Continuous Diagnostics and Mitigation cybersecurity programs and support a key online immigration data portal.

In addition to the almost \$18 billion to construct a border wall, the president wants \$2.2 billion for high-priority investments in border security technology, infrastructure and equipment to help Customs and Border Protection prevent, detect and interdict illegal border crossings.



The \$2.2 billion request also includes \$182 million for surveillance technology, such as towers, radars, cameras and sensors to give the Border Patrol situational awareness in high-risk areas, as well as \$149 million for critical equipment and facility needs, such as Border Patrol stations, vehicles and radios.

## ACLU Wins Suit Over Individuals' Right to Protest and Monitor Border Patrol Checkpoint Operations

the Ninth Circuit Court of Appeals issued an opinion siding with ACLU clients in a case involving the First Amendment right to protest and monitor law enforcement activities in public. After plaintiffs Peter Ragan and Leesa Jacobson encountered harassment and retaliation from Border Patrol agents while attempting

to monitor a checkpoint in rural Arizona, the ACLU of Arizona, ACLU of San Diego & Imperial Counties, and Covington & Burling, LLC filed suit.

## Sudan, S. Sudan resume cross-border trade after 7 years



Sudanese Trade Minister Hatem al-Sar on Wednesday announced the resumption of cross-border commercial traffic with South Sudan following a seven-year hiatus.

According to local media reports, the two countries have now resumed full border services in Sudan's White Nile Province and South Sudan's Upper Nile region.

Al-Sar told reporters in Khartoum that the decision to reopen the border to commercial traffic had been ordered directly by President Omar al-Bashir.

"The resumption of legal cross-border commerce will strike a blow against smuggling," the trade minister said, adding that Sudan was "open to dialogue with all its neighbors".

Cross-border trade had remained suspended since South Sudan declared independence from its northern neighbor following a popular referendum in 2011.



# THE ROLE OF EXPERT SUPPORT IN NUCLEAR SECURITY

November 2017: Estonian and Finnish intelligence services have received information that illegal transport of radioactive materials is underway via the Baltic countries. The final destination of these sources is unknown but there are reasons to believe that Finland may be the intended target for further illicit trafficking. The information alerts hint that international terrorist group has declared its malicious intentions to use these materials in an attack against the EU Member States.

This scenario – fortunately just an exercise – possess a real challenge across the country borders to fight against nuclear terrorism.

## **Cross Border Reachback Demonstration**

Estonian and Finnish authorities decided to cooperate and stop the attempted illicit trafficking in Tallinn. It was agreed that Finland sends to Estonia a multi-disciplinary expert support team consisting of authorities and radiation detection experts from the private sector. As known, there is a consensus at the

European and international level that one of the most efficient ways to enhance the national capability is to collaborate with others. This demonstration shows that two EU Member States can carry out a joint field operation in nuclear security with advanced expert support across the country borders. This kind of demonstration between two States, with the given scope, technology and expert support, has not been undertaken before. This was a unique opportunity to learn.

## Aims and Objectives

This action was aimed at enhancing the awareness and understanding on the level of operative and technological readiness we have at hand to address the contemporary nuclear security threats efficiently at local, national, regional and international levels. Information sharing during a nuclear security event or emergency is of vital importance to ensure an appropriate and timely response by the authorities.

The demonstration was focused on a search operation of radioactive material with emphasis on timely alarm adjudication. The motivation to organize this demonstration was three-fold:

1. Awareness raising on the importance of real time expert support
2. Promotion of the development of regional cooperation
3. Demonstration how the existing technology can meet the above demands

## Roles and Responsibilities

The Societal Security Solutions Ltd, contracted by the Ministry of the Interior of Finland, organized this demonstration in collaboration with the Estonian Rescue Board. The operation took place simultaneously at two reachback centers. The Finnish Radiation and Safety Authority (STUK) was on duty at their facilities in Helsinki, Finland. While HT Nuclear Ltd provided the scientific support to the local reachback centre in



Tallinn which was established in the premises of the Estonian Rescue Board, who hosted the demonstration and lead the search operation of radioactive material out of regulatory control.

Environics Ltd built the reachback infrastructure locally and provided the radiation monitoring equipment to the field team.

The Estonian and Finnish observers of the demonstration included persons from security, law enforcement and rescue operations.

## Operative Concept

This demonstration provides a firm enough basis for the development of a new operative concept for the provision of assistance and for receiving assistance in a given threat situation.

Further relevance and timeliness are underlined in the new national Finnish CBRNE Strategy as well as in

EC Action Plan that has recently been published on CBRNE security risks. Also, one of the three focus areas of the European Commission Joint Research Centre ERNCIP RN Thematic group is the expert support of field teams.

The Finnish-Estonian demonstration contributes to the implementation of these action plans by enlightening the importance of bilateral, regional and international cooperation across the borders to fight nuclear terrorism.

For the demonstration, an illicit trafficking scenario involving radioactive substances was developed. Both countries, Estonia and Finland were engaged to address the given situation. According to the scenario, the Estonian authorities launched a search operation to detect the substances in Tallinn with assistance and support from Finland. A local reachback centre was established in the premises of the Estonian Rescue Board, where also



the command center was located. The Finnish Radiation and Nuclear Safety Authority (STUK) was in readiness to provide assistance in the form of expert support should there arise a need for that during the search operation.

**Action**

As per scenario, an information alert was received that radioactive materials are stored in a warehouse in Tallinn and there were reasons to believe that the sources would be transferred to Finland.

A large-scale search operation was launched. All traffic in the Tallinn harbor was monitored by relocatable portal monitors and several search teams were formed to work under the Estonian Command Center (CC).

The demonstration itself followed in detail the operation from the point of view of one search team. The CC/reachback center could follow the

movement of the patrol in real time and discuss the relevance of its findings.

At the early stages of the demonstration the search team was involved with the radioactive threat situation. The first alarm was quickly confirmed by the operator and reachback centre as Co-60. In addition, the experts concluded from the spectral data that only trace amounts of Co-60 is present and it causes no threat to the population, nor to the environment. The patrol was instructed to mark the site for a rescue team which was tasked to take control of the source and transport it to a safe and secure place.

After further instructions from the command center the team moved forward in the predefined direction and soon got new indication of radioactive material nearby. This time it seemed to be a situation with multiple radiation sources.

The automated software of the backback identified immediately the radionuclides Co-60 and Am-241 near the vehicle parked at site. The alarm was also confirmed by the local reachback center in Tallinn. However, the spectra seemed to contain signatures from other materials which looks like Cs-137. Without clear identification of this complex situation, the Estonian command center decided to ask a second opinion from STUK in Helsinki.

After consultation, the experts from Estonia and Finland both confirmed that Cs-137 material is also involved in this situation. Additionally, STUK concluded that Co-60 is an unshielded small source and so is Cs-137. Furthermore, STUK informed that Am-241 cannot be a very large source. In brief, STUK summarized that the sources are no threat to the population, nor to the environment.

Command center at RB EOD Centre concluded that the information received from STUK is vital and contributes to the balanced response.

At this stage, the demonstration process came to an end, and the field team was asked to come to the operations centre for immediate wrap-up.

The local reachback centre was successful in its analysis of the given radiation situation. The sources were detected and correctly identified and located. Source characterization is not a simple task, requires much experience, and advanced analysis tools. In this work, the scientific help from the experts was of vital importance for correct response which shall be in balance – not

underestimating the threat, nor an overreaction with unjustified countermeasures.

An opportunity was taken to offer to the participants a demonstration of some additional capabilities that are essential in responding to evolving security events. As the demonstration was carried out with very small gamma emitters that cannot cause any hazard in any circumstances, some of the features were not possible to demonstrate in the field. The RanidPro200 backpacks from Environics used for the demonstration had an integrated spectrometric radiation source locator (RanidSOLO) installed and ready to use. A decision was made to demonstrate the source localization capability inside the Rescue Board facilities. 370 kBq Cs-137 source was used to demonstrate this capability by simply placing the source one meter away from the detector. The user interface of the backpack quickly pointed the correct direction of the source.

## Conclusion

After the demonstrations there were active joint discussion with the participants. Questions, such as the legal and procedural actions including data security were elaborated. The demonstration included sending security related information to another country, which is not a simple matter. Technical, scientific and operational cross-border cooperation, involving sharing sensitive information, is only possible if this is agreed in advance at high political level in both States, and secure means for information

transfer have been adopted.

As a concluding remark, the capabilities were demonstrated to assist another State in a nuclear security event. The Finnish-Estonian joint action represents the first fully real-time demonstration of the centralized alarm adjudication and reachback concept at the European and international level. It was demonstrated in an operative environment, how real-time cross-border collaboration between two countries of European Union can be efficiently facilitated by the use of existing technology.

The management activities associated with the radiation incident, looking from the technological and expert service point of view, were well carried out. However, the demonstration understandably did not cover all aspects relevant to administering a complex task in a given evolving situation, due to limited scope and allocated time.

Further point to discuss would be the radiation source localization, which has been a missing functionality in the field operations. This demonstration also proves that locating the source accurately and timely is already possible. When the source is located and its activity is calculated, it is possible to decide upon the next operational steps, which are in balance relative to the threat.



# THE MOST ENGAGING DISCUSSIONS IN BORDER MANAGEMENT

## EVENT UPDATE



**20<sup>th</sup>-22<sup>nd</sup> March 2018**  
**Madrid, Spain**  
[www.world-border-congress.com](http://www.world-border-congress.com)

**World Border Security Congress Congress Programme opens in Madrid, Spain on 20th March for 3 days of great discussions, meetings, workshops and networking for the global border security experts.**

As the international border security community gathers from 20th-22nd March the opportunity to discuss the latest issues, challenges and solutions facing the industry will see over 50 countries, currently pre-registered, meet to share

knowledge and experiences to enhance collaboration and co-operation in international border management.

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.



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.

**ENHANCING BORDER SECURITY THROUGH CONSTRUCTIVE DIALOGUE**

2018 Congress Topics include:

- Identifying and understanding the latest and evolving threats and challenges for border agencies
- Coordinating Coastal and Maritime Border Surveillance
- Counter-Strategies for Human and Drug Trafficking
- Implementation of Advance Passenger Information
- Big Data and how to use it at the border
- Surveillance Systems and Technologies on the Border
- Future trends in International Border Management

2018 World Border Security Congress Supported by:



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!

Supported by the Spanish Ministry of Interior, National Police and Guardia Civil, support is also delivered by the Organisation for Security & Cooperation in Europe (OSCE), the European Association of Airport and Seaport Police (EAASP), the African Union Economic, Social and Cultural Council (AU-ECOSOCC), National Security & Resilience Consortium, International Security Industry Organisation and International Association of CIP Professionals, the World Border Security Congress is the premier multi-jurisdictional



**AU-ECOSOCC Workshop:**

**Workshop 1: Tuesday 20th  
March - 9am-12.30pm**

**Workshop 2: Weds 21st  
March - 9am-12.30pm**



The African Union Economic, Social and Cultural Council (AU-ECOSOCC) will be hosting a Workshop on the margins of the Congress to understudy the situation and proffer necessary solutions that will address the issues of Migration in Africa.

Africa is continuously losing its young, vibrant human resources and future through irregular migration, leading through the path of death to Europe and other developed Nations. This has continued to lead to loss of thousands of lives, brain drain and depletion of Africa's human resources.

The Side Event with the theme "Migration - Creating Opportunities for Young People In Africa" will be highly interactive with Keynote presentations, Panel discussions centered on a meaningful dialogue among participants and stakeholders.

Further details on AU-ECOSOCC can be found at <http://auecosocc-ng.org/world-border-congress.html>



**Site Visit**



Courtesy of the Spanish Police Nacional, the World Border Security Congress 2018 site visit will be to the Madrid Barajas International Airport, offering the opportunity to view Spains Smarter Borders Project with the latest technologies and systems installed at the country's busiest airport.

The site visit will take place on Tuesday 20th March and with high demand and limited places, early

booking is recommended.

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.

With conference presentations will be conducted in English with Spanish and French simultaneous translation services, this years Congress is set to be the biggest gathering of border agencies and agencies at the border.

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](http://www.world-border-congress.com/PSG)

Silver Sponsor:



Welcome Reception Sponsor:



Networking Reception Sponsor:



Lanyard Sponsor:



Sponsor:



Media Partners:



## 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](mailto: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?*  
Chair: Spanish Ministry of Interior

### Leading Line Up of International Expert include:

- Mike Stepney, Deputy Chief Operating Officer, Border Force UK
- Jesus Gomez, Chief Commissioner, Madrid Barajas Airport and Police HQ, Spanish National Police
- Abdunnasser Segayer, Head of Libyan Border Guards
- Ian Waterfield, Director of Operations, UK Gangmasters and Labour Abuse Authority
- Nuria Feroso, Regional Manager Passenger Experience & Facilitation Europe, IATA
- Dr. Tunji Asaolu, Chairperson, Social Affairs and Health Cluster Committee of the African Union-Economic, Social and Cultural Council
- Major Michael Jones, Chief Operations Officer and Acting Executive Director, IMPACS Joint Regional Communications Centre (JRCC)
- Antonio Doblaz Jimenez, Lieutenant Colonel Head of the National Coordination Centre-EUROSUR Spain
- Gregor Pelzl, Head of Coordination Office for Migration and PNR, German Federal Police
- Bjorn Clarberg, Team Leader, Border Management & Migration Team, EUBAM Libya
- Rasa Ostrauskaite, Director, Transnational Threats Department, OSCE~
- Myria Vassiliadou, EU Anti-Trafficking Coordinator, European Commission
- Florian Forster, Head, Immigration and Border Management (IBM), Department of Migration Management (DMM), International Organization for Migration
- BG Col. Sławomir Markowski, Head of Unit for Border Infrastructure and Information, Border Management Department, Polish Border Guard HQ
- Babatunde Olomu, Assistant Comptroller of customs, Nigeria Customs Service~
- James Shaw, Senior Legal Officer, United Nations Interregional Crime and Justice Research Institute (UNICRI)
- Justice Amevor, Assistant Commissioner Immigration, Ghana Immigration
- Jim Nye, Alliance Operations Commander, Devon & Cornwall Police, UK
- Lasma Stabina, National Anti-Trafficking Coordinator, Ministry of the Interior, Latvia
- James Douglass IPM, Ports Protective Security Lead, National Counter Terrorism Policing HQ, UK & Chairman European Association of Airport & Seaport Police



## everis presents new ABC (Automated Border Control) solution as part of its Smart Borders service catalogue

everis Aerospace, Defense and Security, a company of everis Group, has recently presented its latest gate solution for Automated Border Control. As part of the suite of Smart Borders developed by everis Aerospace, Defense and Security, the solution integrates the eGate module, with an interface that enables users to follow the verification steps required intuitively and autonomously; and the Monitoring and Videosurveillance modules, to enable the officers in charge to monitor the activities at all times and make decisions regarding border crossing.

This product was designed to simultaneously gather biometric and documentary data in order to ensure their veracity. It comprises a password and national eID reader, as well as a system for live facial image collection, which captures the passenger's face and introduces it in the biometric verification system right away. Depending on the requirements, the gates also allow to integrate a fingerprint reader. All these features make it possible to quickly and safely verify the identity of individuals and the authenticity of their documents in areas with high public traffic.

everis' new ABC solution is based on the use of compact gates that require little space, thus increasing the amount of

units that can be deployed in the same area, and reducing installation times. Their modular and stackable configuration allows rapid expansion, and their transparent design makes it easier to visually monitor both the passenger's and the officer's premises at all times.

This product has already been approved by the National Police Forces of Spain within a framework contract with AENA. This way they acknowledge the compliance of the gates with all necessary security requirements and endorse their suitability for border control purposes.

The new ABC gates are included in the catalogue of the Identity area, which is part of the Security department. The Identity area at everis Aerospace,

Defense and Security designs and implements projects for clients in the public and private sectors by integrating technological capabilities

in biometric identity systems, document issuance and verification, identity fraud control, or digital signature.

## Rapid Deployment for Secure Borders

With the PNR Directive coming into effect this year, the demands on governments and carriers to provide and process passenger data is increasing dramatically. SITA, a global provider of border security and IT solutions to governments, airlines and airports, has designed some robust solutions to fulfil these demands and deliver a secure border experience for all.



SITA's iBorders® FastStart is the world's first all-in-one passenger screening system, capable of being implemented to protect any country in just 12 weeks. It provides a single view of all intelligence in real-time and beyond borders; seamless access to air transport industry carrier feeds; a customisable solution for government's changing needs and compliancy with international legislation (including EU) and all government agency requirements.

FastStart's advanced design automatically identifies persons of interest, whether known or unknown, in real-time and facilitates vital information sharing between agencies, allowing for faster clearance of low-risk travellers.

With airlines processing passenger data in many ways, and different governments requiring API and PNR data in different formats and with different timings, the

complexity of sending and receiving passenger data is increasing dramatically. SITA's iBorders®

GovernmentGateway resolves this complexity for both carriers and governments and improves and monitors the quality of the data transmitted.

High quality data feeds automate risk assessments beyond borders, allows real-time vetting for every passenger and crew

member and accesses a single window view for all data; plus generates reports on carrier data quality.

This real-time access to all intelligence turns unreadable multiple data formats into one uniform readable format, normalises, correlates and stores all data and identifies unknown linkages between passengers.

## U.S. Customs and Border Protection Accepted Elbit Systems of America's Third Successfully Deployed Border Security System

U.S. Customs and Border Protection (CBP) accepted the latest Integrated Fixed Tower (IFT) border security system deployed by Elbit Systems of America, LLC. This IFT system, located in the Sonoita, Arizona, Area of Responsibility (AoR), marks the company's third successful deployment of the system. Other previous deployments of IFT accepted by CBP were for the Douglas and Nogales, Arizona AoRs.



"Our advanced technologies provide U.S. Customs and

Border Protection with trusted border security capabilities," said Raanan

Horowitz, president and chief executive officer of Elbit Systems of America. "America's Border Patrol agents rely on our operationally proven solutions for greater situational awareness and enhanced safety."

As the system integrator, Elbit Systems of America furnishes the sensor towers with radar, day/night cameras, and command and control software that combines data into a single operating picture. Information from all the towers is networked into Border Patrol Station command and control centers, which increases situational awareness for Border Patrol Agents. IFT has proven to be a reliable system and provides CBP

with 24/7 surveillance coverage. The system also provides CBP with a platform to integrate existing and future sensors to further improve border protection and agent safety.

On the path to system acceptance, significant milestones must occur. Several months of construction, integration, test activity, and system verification ensure each IFT meets performance requirements. Each system must detect, track, identify, and classify border activity. Elbit Systems of America continues to meet customer performance and schedule requirements, as well as adhering to cost goals for this program

## Meteksan Defence to deliver Retinar PTR Perimeter Surveillance Radar for border protection application to a foreign customer

Turkish manufacturer Meteksan Defence won the contract with an undisclosed foreign customer after a competitive tender process and the system will be delivered between March and May this year.

Retinar PTR is a high resolution advanced technology ground and perimeter surveillance radar system optimized for human detection and recognition.

With its small size and

light weight, Retinar PTR is the man-portable model of Meteksan Defence's Retinar Perimeter Surveillance Radar Family. The high-technology radar system is developed for surveillance operations



such as perimeter security of critical facilities, border security, and agile surveillance carried by patrolling mobile personnel.

Retinar PTR can be carried by two personnel in its special backpacks and can be used mobile on tripod with its batteries. It also generates the doppler signature of the target and provides classification information whether it's

vehicle, human or animal with micro-doppler spectrogram analysis. Retinar PTR has been made ready for operation after extensive tests made in the field. It had been also tested by the customer in different areas and weather conditions during the tender process which the radar performed fully successful during all tests.

## Princeton Identity has announced the deployment of its Access500e™ identity management kiosk module within the Dubai International Airport (DXB)

The Princeton Identity solution identifies DXB travelers within one to two seconds, reducing time spent in security lines and enhancing the overall travel experience.

The Emirates Airlines terminals are the largest terminals within one of the world's busiest passenger airports. Dubai saw nearly

14.9 million international visitors in 2016, and is expected to surpass 20 million visitors by 2020. There are currently about

100 Access500e products in operation across DXB's Emirates Airlines terminals, with plans to deploy about 40 more in the near future in order to support the influx of new international tourists.

the "Eyen" gate system, which captures biometric signatures—eliminating the need for visitors to check in with a customs agent, and saving time for passengers as well as airport staff. This helps



"Princeton Identity and the Dubai International Airport share a goal of simplifying and speeding access to keep people and business moving, and the Access500e deployment at the DXB marks a new standard in passenger security," said Mark Clifton, chief executive officer at Princeton Identity. "Iris recognition is most reliable form of biometric identification, and the Access500e turns what used to be a slow process for travelers into a convenient, quick and more secure experience." Access500e is a fast, high quality face and iris biometric capture device designed for integration into a variety of application solutions. At DBX, it is integrated into a new Smart Gate, commonly referred to as

ensure verification of all travelers entering and leaving the country, seamlessly and efficiently. Princeton Identity partnered with the tech company Emaratech in fostering the implementation of Access500e into the terminals at DBX.

"DXB has always set a high bar in terms of innovative and future-forward experiences and we applaud the leadership team's decision to tap the power of iris recognition to further enhance both traveler satisfaction and security," added Clifton.

A newly opened Princeton Identity International office in Dubai is dedicated to ensuring the continued success and expanded implementation at DXB.

## Border Security and Digital Intelligence

Border control officials share two basic goals: secure their borders and protect their citizens.

An increasingly imposing obstacle to these goals has been criminals exploiting the Internet and mobile devices to commit terrorist activities, facilitate human and drug trafficking, import counterfeit or unsafe goods, etc.

According to a recent report by PWC, the techno-ingenuity of these criminals has transformed border crime into something much more sophisticated with border security adopting technology solutions such as "surveillance drones and data-led predictive patrolling."

It is clear that border security teams need innovative digital solutions to enable them to collect data from multiple and traditional sources, screen against watchlists as well as verifying identities, monitoring and surveillance. However, the path is covered with digital challenges including encrypted devices and language translation impede data review; identity fraud requires deeper examination and analysis at ports of entry, field offices

or HQ and the need to store and share actionable information between entry points, field offices, HQ and other agencies to improve situational awareness

To help border security teams answer these challenges, Cellebrite provides end-to-end digital solutions to action information retrieved from mobile devices and open source data at the point of engagement; enable agents to immediately extract mobile and public domain cloud data and analyze both together; conduct deeper examinations to substantiate threats or concerns, when further vetting is required and correlate device data with intel information already available to improve screening and profiling.

## CONTACTS

### Editorial:

Tony Kingham  
E: [tony.kingham@knmmedia.com](mailto:tony.kingham@knmmedia.com)

### Contributing Editorial:

Neil Walker  
E: [neilw@torchmarketing.co.uk](mailto:neilw@torchmarketing.co.uk)

### Design, Marketing & Production:

Neil Walker  
E: [neilw@torchmarketing.co.uk](mailto:neilw@torchmarketing.co.uk)

### Subscriptions:

Tony Kingham  
E: [tony.kingham@knmmedia.com](mailto:tony.kingham@knmmedia.com)

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



Copyright of KNM Media and Torch Marketing.

## ADVERTISING SALES

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

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

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

Isaac Shalev  
(Israel)  
E: [isaac@itex.co.il](mailto:isaac@itex.co.il)  
T: +972 (3) 6882929

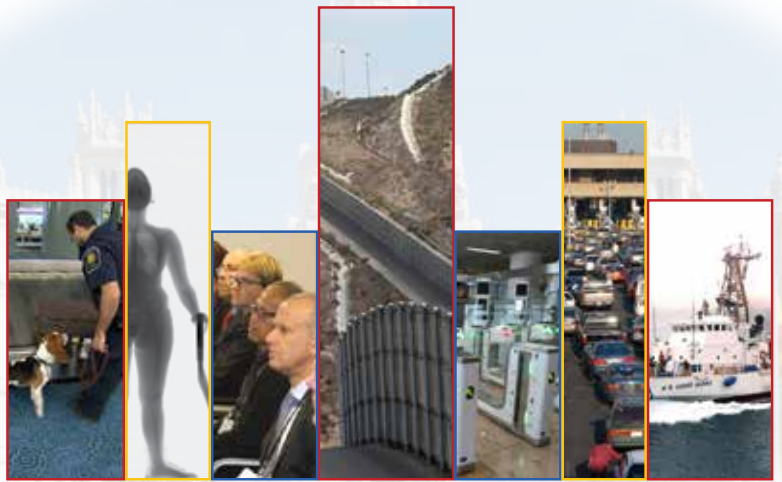


# World Border Security Congress

20<sup>th</sup>-22<sup>nd</sup> March 2018

Madrid, Spain

[www.world-border-congress.com](http://www.world-border-congress.com)



Supported by:



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

## Co-operating towards Collaborating

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](http://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](http://www.world-border-congress.com)

### Speakers include:

- Mike Stepney, Deputy Chief Operating Officer, Border Force UK
- Jesus Gomez, Chief Commissioner, Madrid Barajas Airport and Police HQ, Spanish National Police
- Abdunnasser Segayer, Head of Libyan Border Guards
- Ian Waterfield, Director of Operations, UK Gangmasters and Labour Abuse Authority
- Nuria Feroso, Regional Manager Passenger Experience & Facilitation Europe, IATA
- Dr. Tunji Asaolu, Chairperson, Social Affairs and Health Cluster Committee of the African Union-Economic, Social and Cultural Council
- Major Michael Jones, Chief Operations Officer and Acting Executive Director, IMPACS Joint Regional Communications Centre (JRCC)
- Antonio Doblaz Jimenez, Lieutenant Colonel Head of the National Coordination Centre-EUROSUR Spain
- Gregor Pelzl, Head of Coordination Office for Migration and PNR, German Federal Police

For full speaker list visit

[www.world-border-congress.com](http://www.world-border-congress.com)

*...for the international border management and security industry*

Also Supported by:



Silver Sponsor:



Media Partners:

