INCORPORATING BORDER SECURITY REPORT

WORLD SECURITY REPORT

Official Magazine of

International Association of CIP Professionals

MAY / JUNE 2018
www.worldsecurity-index.com

FEATURE:
An Integrated Approach Used in Nuclear Security can be Adapted for Protecting Critical National Infrastructure
PAGE 9

FEATURE:
The Predator's View: The Imperative for Critical Infrastructure Resilience
PAGE 14

FEATURE:
World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down
PAGE 19

COVER STORY

STOPPING FOREIGN TERRORIST FIGHTERS – CAN API AND PNR PLAY A PART?

Strategic Partner:

NACSA
AGENSI KESELAMATAN SIBER NEGARA
NATIONAL CYBER SECURITY AGENCY

In Partnership with:

CyberSecurity MALAYSIA

17th-19th July 2018

The Waterfront Hotel,
Kuching, Sarawak, Malaysia

www.cip-asia.com

ONE-DAY SPECIALIZED TRAINING COURSE
brought to you by:
CyberSecurity MALAYSIA
further details at
www.cip-asia.com

Developing resilient infrastructure for a secure future

Register Today for Early Bird Rates

Early Bird Deadline 17th June 2018
Register online at www.cip-asia.com/onlinereg

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

On behalf of the Organising Committee and co-hosts, the National Cyber Security Agency, CyberSecurity Malaysia and the State of Sarawak, you are invited to participate in the 3rd Critical Infrastructure Protection & Resilience Asia, taking place at The Waterfront Hotel, Kuching, Sarawak, Malaysia on 17th-19th July 2018.

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.

Register online at www.cip-asia.com/onlinereg

Leading the discussion on securing critical infrastructure across ASEAN

Gold Sponsor:

sarawak energy

Media Partners:

World Security-index.com

WORLD SECURITY REPORT

Supported by:

SARAWAK CONVENTION BUREAU

Supporting Organisations:

KeTTHA KEMENTERIAN TENAGA, TEKNOLOGI HIJAU DAN AIR

sains Envision. Innovate. Advance

NS&RC

SPF

Expert 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
- Sameer Sharma, Senior Advisor, BDT/International Telecommunication Union
- Sim Ko Sin, Vice President, ICT, Sarawak Energy, Malaysia
- Munies Pillai, Director, Global E2C Pte Ltd and Senior Vice President of the Chartered International Institute of Security And Crisis Management
- Senior Representative, Metropolitan Electricity Authority, Thailand
- Albert Chai, Managing Director, CISCO Systems Malaysia
- Fazlan Abdullah, Head, Government Engagement, International & Government Engagement Division, CyberSecurity Malaysia
- Benjamin Ang, Senior Fellow & Head – Cyber, Centre of Excellence for National Security (CENS)
- Henry Ee, Chairman for Asia Chapter, Business Continuity Institute
- Kenneth Chen, Managing Director, ASEAN, Symantec Asia Pacific, Singapore
- JP Dunning, Principal Security Consultant, APAC Lead for Foundstone Services, McAfee, Australia
- Ian Yip, Chief Technology Officer, Asia Pacific, McAfee, Australia
- Ir. V.R.Harindran, Sr. Custodian, I&C, Mechanical & Process Section, Group Technical Solutions, PETRONAS

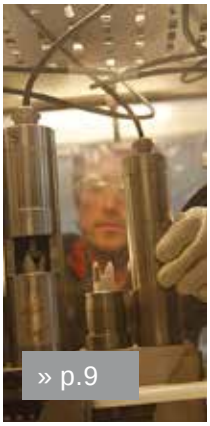
For full conference programme visit www.cip-asia.com

CONTENTS

WORLD SECURITY REPORT

» p.5

» p.12


» p.9

» p.17

5 STOPPING FOREIGN TERRORIST FIGHTERS – CAN API AND PNR PLAY A PART?

Andrew Priestley takes a look at the impact API and PNR could have in identifying and stopping of foreign terrorist figters.

9 AN INTEGRATED APPROACH USED IN NUCLEAR SECURITY CAN BE ADAPTED FOR PROTECTING CNI

How the nuclear industry uses an approach to threat that articulates the Design Basis Threat (DBT).

14 THE PREDATOR'S VIEW

The Imperative for Critical Infrastructure Resilience.

18 ASSOCIATION NEWS

News and updates from the International Association of CIP Professionals.

19 WORLD'S BIGGEST MARKETPLACE SELLING DDOS ATTACKS TAKEN DOWN

With over 136 000 registered users and 4 million attacks, Webstresser.org was considered the world's biggest marketplace to hire DDoS Services.

21 SECURITY TECHNOLOGY, PROTOCOLS AND PEOPLE IN SYNC THROUGH TRAINING

Today's security plans include a wide variety of technology and techniques and require multiple levels of skill and knowledge for peak performance.

23 AGENCY NEWS

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

26 INDUSTRY NEWS

Latest news, views and innovations from the industry.

DO WE EVER LEARN LESSONS FROM THE PAST?

During the 90's and 00's, in the post-cold war world, politicians busied themselves talking about the 'new world order', and consequently spending less and less on defence and security, cashing in on the so-called 'peace dividend'.

Then 9/11 caused shockwaves around the world and was responded to with the 'war on terror'. Indeed, it was in response to 9/11 that we ourselves launched our own online news media www.WorldSecurity-index.com in 2002.

But throughout that period, I would continue to bore anyone who would listen with warnings that whilst terrorism was a dangerous menace that had to be confronted, the really big worries were still the old worries, primarily Russia.

I would argue that despite being a shadow of its former Soviet self and having become a fledgling democracy; that democracy was only a fragile veneer which could be shattered at any time. And, that the Russian "Bear" still had huge teeth and fangs and a historical appetite for attacking its neighbours.

Now we all know that western politicians can only see five years into the future, but what I found most disappointing during that period was that a whole generation of senior military leaders seemed to either share, or collude with the view that the old threats really were a thing of the past.

Now 28 years on, we live in a world with a belligerent and resurgent Russia and another old enemy lobbing missiles into the South China Sea.

So, strangely, I now find myself worrying about the same thing, but in reverse. And that is, that as the so-called Caliphate collapses and operations against ISIS and Al Qaeda in Syria and Iraq wind down, that perhaps attention will shift away from terrorism and focus back on those bigger issues, the threats posed by Russia, North Korea and Iran, without properly finishing the job of defeating the terrorists and their perverse ideology.

As fighters disperse around the world and merge back into the societies they came from, they will exploit local grievances and reinvigorate local conflicts seeking to absorb these into their transnational ideology.

We need to learn the lessons of the past and make sure we continue to devote enough resources to ensure that the battle against ISIS and AQ is ultimately won and not simply displaced, to be fought somewhere else.

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/WSRMay18

www.worldsecurity-index.com

Editorial:
Tony Kingham
E: tony.kingham@knmmedia.com

Contributing Editorial:
Neil Walker
E: neilw@torchmarketing.co.uk

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

Subscriptions:
Tony Kingham
E: tony.kingham@knmmedia.com

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

Copyright of KNM Media and Torch Marketing.

critical infrastructure PROTECTION & RESILIENCE ASIA
17th-19th July 2018
Sarawak, Malaysia
www.cip-asia.com

2nd-4th Oct 2018
The Hague, Netherlands
critical infrastructure PROTECTION AND RESILIENCE EUROPE
www.cipre-expo.com

critical infrastructure PROTECTION AND RESILIENCE AMERICAS
4th-6th Dec 2018
Orlando
Florida, USA
www.ciprna-expo.com

World Border Security Congress
19th-21st Mar 2019
Casablanca
Morocco
www.world-border-congress.com

Stopping Foreign Terrorist Fighters – can API and PNR play a part?

Andrew Priestley, Director of Agile Borders takes a look at the impact API and PNR could have in identifying and stopping of foreign terrorist figters across borders, and whether streamlining operations at airports can benefit national security away from airports.

I recently returned from a four-week assignment in Central Asia where I was engaged by a regional organisation to assist the local authorities in developing a roadmap to help with the implementation of an API system. The authorities I was working with in Central Asia have a concern their country is being used to facilitate the return of Foreign Terrorist Fighters (FTFs) from terrorist training grounds. In the aftermath of terrorist attacks, attention is always turned to the background of the perpetrator and whether or not they travelled overseas to be trained in their deadly craft. If they were, questions are always asked about how this was possible and why the terrorist wasn't identified and stopped before they carried out their attack. The United Nations has issued three resolutions mandating member states implement API systems in the fight against terrorism.

How useful is API and PNR in identifying and stopping terrorists crossing borders when it is mainly used at airports?

API is Advance Passenger Information – the data airlines collect from the machine-readable zone of passengers' passports and other travel documents. This data is sent to the authorities before a passenger's arrival at a border, allowing checks to take place in advance of them presenting themselves at passport control.

PNR is the Passenger Name Record, this is information which the government can request from airlines and relates to an individual's booking details. PNR will contain information about other flights booked as part of the same journey, details about how and when the ticket was bought and the method of payment, and other information which can be very useful for identifying passengers who may of interest to borders, customs and even intelligence agencies.

API and PNR are very useful tools in assisting with the management

of borders and are used in many countries around the world. According to the International Air Transport Association, IATA, around seventy countries globally have either implemented API or are in the process of doing so. Many countries are implementing or have plans to implement PNR.

Global terrorism is well organised and funded and has a lot of experience in moving people, money, and weapons across borders without detection. Most of this smuggling takes place at land borders. During a recent conversation a senior border guard explained to me that a large section of his country's border was controlled by an infamous global terrorist organisation and that his focus was trying to overcome this issue. The airport border was easy to manage as it was a 10-metre-long line painted on the floor inside a building. This border was well manned, located in a controlled environment, and traveller flow was determined by the predictable arrival of international flights. How could the use of passenger data improve the situation at his country's land border?

Well the answer is that API is only really of use if you can register each traveller before they arrive at a border. It is difficult to collect and process API from people arriving at checkpoints sporadically on foot or in private vehicles. There may be an opportunity to register passengers on international bus and train services. In this particular scenario, of a an environmentally hostile mountain range with no official border crossing points, API and PNR is of little of no use.

One of the key benefits of good use of API and PNR at

suitable locations is that it allows passengers to be pre-screened prior to arrival. This means each traveller can be checked against a number of data sources held by governments: Terrorist watchlists can be analysed, criminal databases checked, and the Interpol Stolen and Lost Travel Document database can be consulted. This is all well and good as an attempt to stop travellers who are using their own identities and documents, but what happens when a terrorist deliberately attempts to hide their identity and uses a forged document?

It is often simpler to change an existing identity rather than to assume a completely new one. Many wanted travellers trying to avoid detection base their false identity on their genuine details, sometimes changing their date of birth, misspelling their name, or perhaps changing their passport number, in attempts to avoid detection. Wanted persons who have changed their identity like this will not ordinarily show up when checking their passenger data against watchlists unless smart matching and analytics tools are used.

Analytics tools compare passenger data with watchlists of wanted persons. Smart analytics tools use fuzzy logic and smart matching techniques to suggest people who may be trying to avoid detection by changing their identity. Analytics tools are at the heart of API and PNR projects, turning passenger data into information, and then potentially into actionable intelligence.

A number of options are available to governments looking for such tools: There are several companies offering proven analytics systems on a commercial basis. Some of these use very advanced and complex matching techniques to identify people who may be trying to avoid detection and come with a price tag to match their capabilities and investment made in their development. Some governments are in the fortunate position of being able to develop their own intelligence systems, the main benefit being that a system designed by the organisation that will use it should meet all requirements perfectly. The downside of this approach is that such systems are complex and

make take many years to perfect and fine tune. There are a number of governments who donate systems to other countries in an effort to increase global security, some of these donated systems come with strings attached in the form of data sharing agreements with the recipient of the system having to share passenger data with the donor country.

There are plenty of options to consider when employing API and PNR solutions in the fight against global terrorism, but are these solutions which are deployed mainly at air borders really helping catch terrorists? Some will be caught travelling by air either under their genuine or an assumed identity. Many will continue to try to travel avoiding the now heavily secured air borders chancing their luck at land and sea borders, sometimes crossing at recognised entry and exit points, sometimes not.

API and PNR allow agencies working at the border to pre-screen travellers before they arrive. This means that travellers who are not of interest can be processed very quickly on arrival by means of a travel document and identity check, before being allowed to proceed with their journey. The vast majority of travellers are of no interest to border authorities whatsoever.

While API and PNR can be very useful tools in assisting authorities with proactive border management, these data sets may not be the silver bullet some governments are expecting. Even the most advanced analytic tools rely on accurate, good quality data being delivered on time. If data contains errors, is not correctly formatted, or is false, then no amount of analysis is going to yield useful results, to use a well-worn phrase analytics is definitely a case of 'junk in – junk out'.

API is usually collected when a passenger checks in for a flight. If this happens at a check-in desk at an airport, the machine-readable zone of traveller's passport or other travel document is scanned and the data collected. As a result of the automatic reading of the travel document the data collected is certain to be correct. Of course, the travel document needs to be genuine, but if it is, API collected by scanning the machine-readable zone is accurate.

Challenges to the accuracy of API arise when travellers check-in online and are travelling with hand luggage only. Many countries, including the UK, have removed physical exit checks for passengers departing their country. An identity check is made of a passenger before boarding a flight to ensure the name on the boarding pass matches the name on the travel document, but no attempt to collect or verify API is made. Travellers who check-in away from the airport and travel without hold luggage often encounter a border official for the first time on arrival at their destination. There could be errors in the accuracy of the API they provided while checking in online; the travel document number could be incorrect – especially if the traveller has more than one passport. The date of birth and document expiry may be incorrect. This may be easy to spot if someone's date of birth is listed as being an impossible date, such as 30th February 1999 entered as 30/02/1999. Such an error would be less obvious if plausible entries had the month and the day transposed, for example 03/02/2001 is 3rd February 2001 according to international convention, but in some parts of the world this date could equally be March 2nd 2001. People seeking to avoid detection may deliberately enter incorrect data. Validation of API is key to ensure accuracy of the data, some less capable analytics tools may miss a potential match against a watchlist.

Technology may be able to play a part in improving the accuracy of API. Most frequent travellers make use of smart phones and computers when checking in for flights. Some airlines are developing their mobile applications to use the camera on

a smartphone to read the travel document, adding a greater level of certainty to the accuracy of the data provided.

In order to improve accuracy of API for travellers whose travel documents are not scanned at the airport or by a mobile device, steps may be needed to ensure the data being provided is accurate. A swipe of each traveller's document at the departure gate could be introduced to ensure accuracy, but this would add to the time taken to board an aircraft and would impact on the efficiency of airports and airlines.

Online check-in has improved efficiencies at the airport as the number of travellers needing to queue to see a check-in agent has reduced dramatically. This improvement in efficiency has led to a potential issue for border security which needs to be acknowledged and managed. In general, borders are easier to cross and safer as a result of knowing who is coming in advance of their arrival.

API and PNR allow border operations at airports to be streamlined, meaning more effort can be made securing borders away from airports. A few extra border guards and customs agents freed up at every international airport might just make a difference in the global fight against terrorism.

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

Registration Now Open

Register today and benefit from Early Bird delegate fees
For further details visit www.ciprna-expo.com/registration

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 more information visit www.ciprna-expo.com

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

To discuss exhibiting and sponsorship opportunities and your involvement contact:

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

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

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

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

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

Vishal Mehta
(India)
E: vishmeh@gmail.com
T: +91 99 999 85 425

Leading the debate for securing Amercia's critical infrastructure

Owned & Organised by:

Supporting Organisations:

Media Partners:

An Integrated Approach Used in Nuclear Security can be Adapted for Protecting Critical National Infrastructure

If a serious incident were to occur, either through accident or deliberate malicious action, the consequences can have national and international effects, as can be seen from the incidents at Fukushima Daiichi (2011), Chernobyl (1986) and Three Mile Island (1979).

Thus, to help prevent malicious threats against the industry there are international conventions, such as the Convention for the Physical Protection of Nuclear Material (CPPNM) and the United Nations (UN) International Convention for the Suppression of Acts of Nuclear Terrorism. Those conventions led to best relevant practice guidance published by the International Atomic Energy Agency (IAEA) in their Nuclear Security Series (NSS). Among the documents in the NSS are many that will be of value to all organisations that need to protect assets against threats.

The nuclear industry uses an approach to threat that articulates the Design Basis Threat (DBT); a national document developed by the State for dutyholders, those companies and organisations that own and operate nuclear facilities, need to design, operate and maintain their Physical Protection System (PPS) to counter threats. Specific documents provide advice and guidance on the development and maintenance of the DBT; and issues such as countering the Insider Threat, a challenging subject relevant to all organisations whatever their focus may be.

All security departments need to understand their assets that need to be protected, and for the nuclear industry that does not just mean the obvious, such as nuclear material (NM) and operational reactors; nuclear power plants or research reactors. It can also involve the systems, structures and components (SSC) that maintain the safety arrangements for the NM, other radioactive materials such as sources, and the computer based systems important to safety (CBSIS) and security (CBSISy). The cornerstone of every security plan is the identification of Vital Areas at nuclear facilities. This activity is the backbone that indicates the potential amount of material that could be subject to theft, and the potential significance of any unacceptable radiological

consequences (URC) through the release of material. It is at this point, where security specialists need their safety colleagues, and those in plant or facility operations, to help in determining the assets to be protected.

The nuclear industry, to prevent nuclear material and other radioactive materials, from becoming a hazard to the public or environment, have three main specialist groups working towards that overall protection strategy; safety, security and safeguards; the Triple S.

The aims for the individual specialisms are:

- Safety is aimed at protecting workers and the public from the harmful effects of radiation (or chemicals or other hazards);
- Security is aimed at preventing malicious acts that might harm a nuclear facility (sabotage) or result in the loss (theft) of nuclear materials; and
- Safeguards are aimed at preventing the diversion of nuclear materials from a civil nuclear programme to nuclear weapons purposes.

The 3Ss share the same overall objectives of protection and use similar principles to achieve protection; multiple barriers, defence in depth, decision analysis and consequence assessment. However, if they work predominantly in silos then compromises inevitably occur for operations and costs are inevitably higher than necessary.

However, as Safeguards is a uniquely nuclear consideration it will not be addressed further in this article.

The practical integration of Safety and Security to deliver enhanced outcomes

The National Nuclear Laboratory (NNL), a Government Owned Commercially Operated (GOCO) company in the United Kingdom that operates a number of unique national assets has employed a SINS (Safety Informed

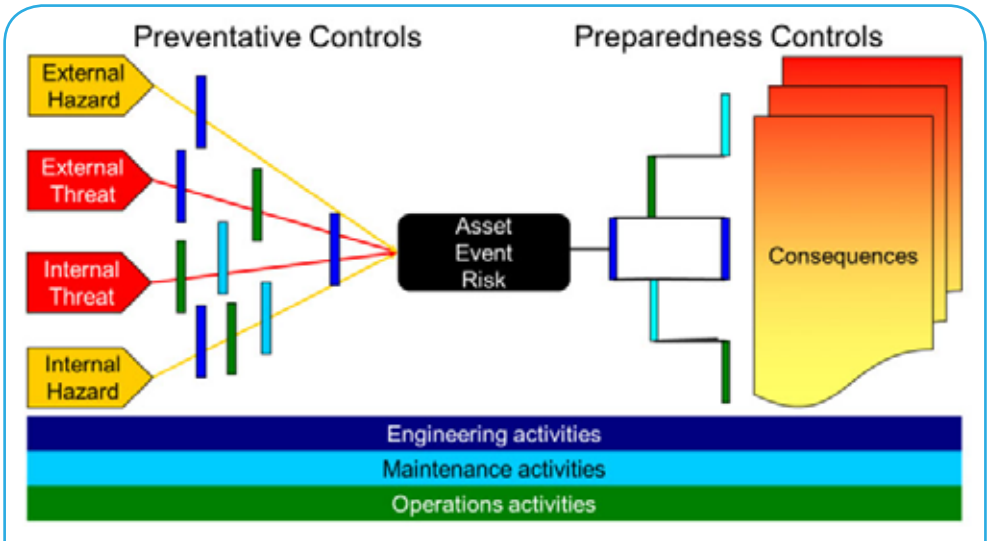


Figure 1: Preventative and Preparedness Controls as a Bowtie Diagram

Nuclear Security or Security Informed Nuclear Safety) approach to asset identification, security design and regulatory compliance.

Defence in Depth

Safety and Security both use the concept of defence in depth to minimise the likelihood that the failure of one aspect of their preventative arrangements will lead to the compromise of an asset; accident for safety and malicious action for security. This concept of defence in depth is shown in the bowtie diagram at Figure 1. Defence in depth can also be applied to the arrangements to mitigate the potential consequences of any failures; i.e. the emergency plans and counter-terrorism arrangements.

Security into Design

NNL are using an approach similar to that depicted in Figure 2 that identifies assets and potential radiological consequences, creates the design of the Physical Protection Systems (PPS) for the facility, and conducts the vulnerability assessment to determine whether the required security outcome is achieved. The system is iterative so that changes in inventory, arrangements, threats and vulnerabilities can be

adequately addressed to maintain or achieve the desired situation.

The expression Physical Protection Systems encompasses the entirety of physical and technical security equipment, procedures, personnel security, cyber security and information assurance, and guarding and armed response forces.

This approach brings together the best relevant practice promulgated by the UK's Centre for the Protection of National Infrastructure (CPNI) in the form of Operational Requirements (OR), and the Office for Nuclear Regulation (ONR) Security Assessment Principles (SyAPs). The SyAPs consider security outcomes against the functions of Delay, Detection, Assessment, Control of Access and Insider Mitigation, and the individual security components of the OR can be reasonably effectively mapped onto those functions.

Using the approach in Figure 2 NNL have been using their security and safety specialists in a SINS team to aid a customer in developing their concept design for a new capability, and to create Site Security Plans for their own facilities to meet new regulatory guidance and confirm adequacy of their arrangements.

The SINS approach has involved all specialists to work in a collegiate manner, share professional approaches to optimise outcomes and engage a learning attitude that has upskilled all those involved. It has also delivered a strong evidence base to underpin the claims, argument and evidence approach towards meeting outcomes based regulation.

Safety and Security Synergies

As previously mentioned nuclear security requires extensive safety input for the identification of Vital Areas. Safety assessments skills cover radiological consequence modelling, radiological hazard analysis, Probabilistic Safety Assessment (PSA), Serious Accident Assessment (SAA), internal and external hazards, and layout design all contribute to identifying potential Vital Areas. Many of the hazards requiring protection are unique due to the nature of the asset requiring protection, and based upon the material properties, but the principles of protection are equivalent to those for other sensitive assets.

The design basis accidents for safety and the design basis threats (DBT) for security approaches in both specialisms guide designers, practitioners and assessors to adequately consider those threats that may need to be countered.

Safety and security both use a graded approach.

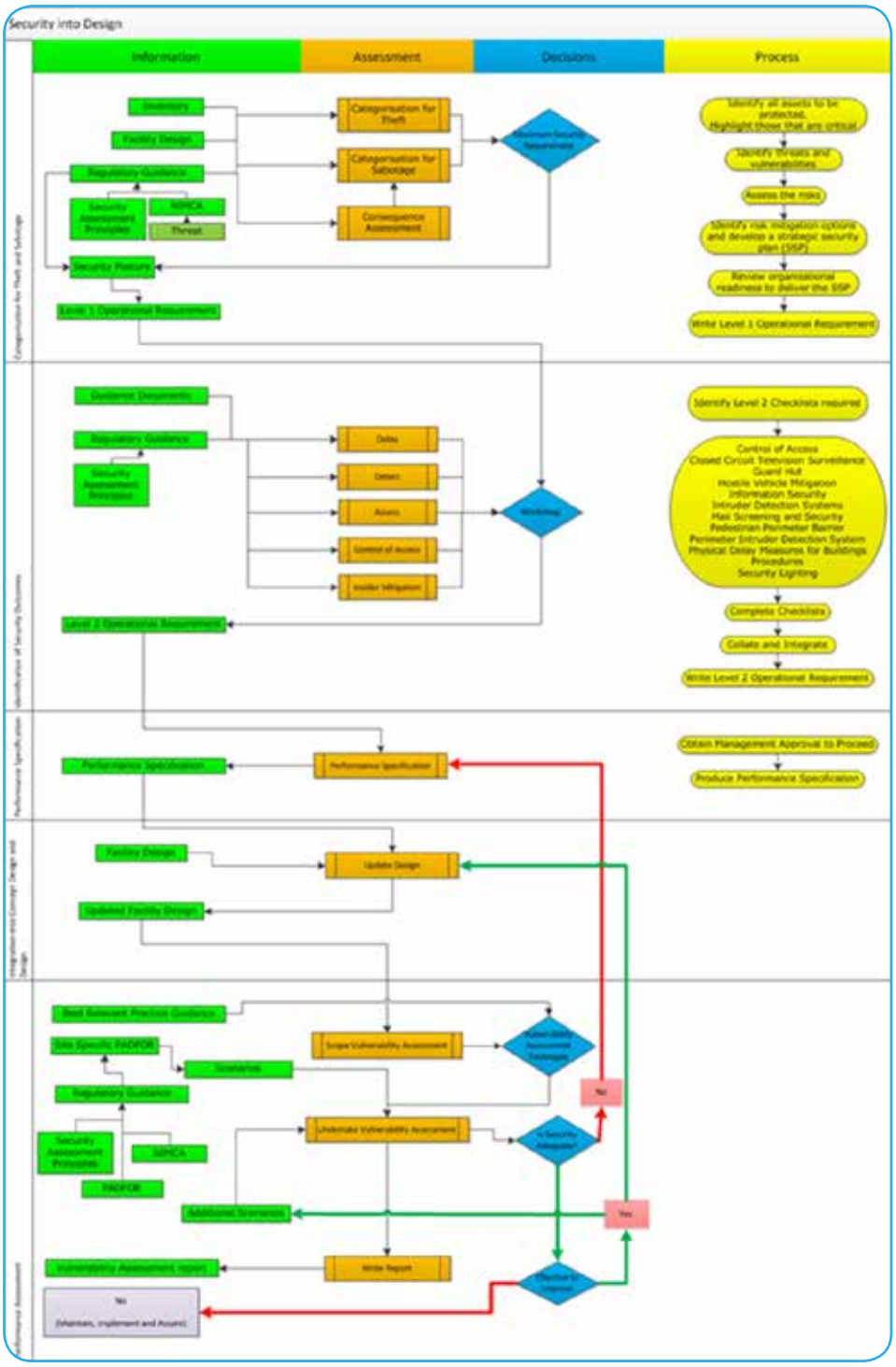


Figure 2: An Approach to Asset Identification, Security Design and Vulnerability Assessment

The relative importance of accident prevention and mitigation measures is expressed in terms of the adverse consequences for public and worker health. Likewise the relative importance of security measures is directed towards preventing and limiting what are considered high and low radiological consequence events.

Considerations on the speed of progress of an incident are important when viewed from the different perspectives, where for example security is trying to counter a malicious attack, and safety is countering an accident. This influences how Prevention, Response, Control and Management efforts are organised and structured. Those arrangements are depicted schematically in the Bowtie diagram (Figure 1) with the aim of minimising the impact on the plant, people, public and environment. These are all considerations that need to be addressed by Critical National Infrastructure (CNI) facilities and organisations

The UK adopts a risk-based approach, enabling operators to ascertain the appropriate arrangements commensurate with the risk. As such approaches and methods used in the minimisation of impact for radiological consequence through 'As Low As Reasonably Practicable' (ALARP) practices in safety are commensurate with those used by security through the use of risk management practices to manage potential vulnerabilities identified through PPS evaluation activities.

Safety and security in the nuclear industry both encourage and embrace Advisory Missions and inspections; from the World Association of Nuclear Operators (WANO), Integrated Regulatory Review Service (IRRS) and Operational Safety Review Team (OSART) for safety; and from the International Physical Protection Advisory Service (IPPAS) for security.

Safety and security both attempt to foster positive cultures that identify and report problems and issues. However the transparent and open communications of safety may conflict with the 'need to know' principles employed in security. Appropriate implementation of 'need to know' principle where consideration is given to what is 'needed to be known' can direct appropriate filtering and redaction so that appropriate interactions can occur without compromising security of materials or information. For example, consequence assessors do not need to know the

locations or means that material can be acquired by a perpetrator to undertake the assessment.

Thus, by fostering an approach that integrates both safety and security in a mutually supporting manner through peer-to-peer and other challenges of behaviours creates the opportunity for reinforcement of positive behaviours.

In summary, many of the principles and approaches used within nuclear security are directly transferable to other areas of the critical infrastructure, and the protection of high value assets.

Robert Rodger, Senior Technical Lead, National Nuclear Laboratory.

Jeremy Edwards, Technical Manager. Nuclear Security, CBRN and Resilience, National Nuclear Laboratory.

The Predator's View

Circa 1832, Prussian General and Military Theorist Carl Von Clausewitz noted : "War is not merely an act of policy but a true political instrument, a continuation of political intercourse carried on with other means." Long before Clausewitz and to this day, adversaries have sought and seek to identify, corrupt, disrupt, degrade or destroy capacities that enable their foes to inflict their will and objectives.

America's decades-long efforts to protect, and with the February 2013 publication of Presidential Policy Directive 21, ensure "Critical Infrastructure Security and Resilience," demands awareness, understanding and appreciation of "the predator's view ." Adversaries see America, Americans, and/or anything contributing to the nation's safety, security, quality of life and future, as legitimate targets. Given their inherent capacities to both empower and inflict consequences, this is especially true of America's interdependent critical infrastructures — cyber and physical.

The absence of understanding and appreciation of the predator's view has been evident throughout history. In 410 AD, the Goths laid siege to Rome and captured it after identifying aqueducts as a Single Point of Failure whose degradation would halt the flow of water into the city and thereby eliminate any resistance within it. In 1943, a Norwegian hydrogen plant producing "heavy water" was attacked and destroyed by Allied Saboteurs and a subsequent raid by 140 U.S. bombers. Not unlike Rome's aqueducts, the plant was a Single Point of Failure whose destruction (and the subsequent sinking of the Norsk, a ferry transporting the remaining inventory of heavy water) effectively terminated Nazi efforts to build an atomic bomb. Conversely, Japanese failure to neutralize critical infrastructures is evident in their December 7, 1941 attack upon Pearl Harbor. While Japan scored a stunning tactical victory along Battleship Row, its failure to attack maintenance and fuel storage facilities adjacent to it (then a Single Point of Failure for the Pacific Fleet) was a strategic blunder that greatly accelerated the demise of the Japanese Empire.

Fast forward to the Information Age. In the aftermath of Operation Desert Storm and America's and her Allies' stunning victory over Iraq's Army (then the world's fourth largest), the Chinese People's Liberation Army initiated a study that is captured in its 1998 publication, "Unrestricted Warfare." The study concluded that information was the key to the American and Allied victory and offered means to neutralize what could be termed "America's Nervous System." As a result, the Chinese (and any predator engaged in cyber probes and attacks) understand that it is no longer necessary to physically destroy a technology-reliant nation to inflict its will upon it.

They have discovered a more antiseptic and efficient approach: Attack interdependent and cyber-reliant critical infrastructures and produce consequences of potentially unprecedented scope, intensity

and duration and, in the process of doing so, degrade social cohesion — the heart of a nation's ability to defend itself. From The Predator's View, validating that approach is its recognition of a valuable contradiction: America's rapidly increasing reliance on the Internet and supporting telecommunications capacities is significantly outpacing its ability to assure their availability and security. The predator's conclusion: America is the most Internet-reliant nation on Earth and for whatever reason is creating the instrument of its demise, its own Achilles Heel — a Single Point of National Failure.

Consistent with this reality, Former FBI Director James Comey has repeatedly and very correctly warned: "Cyber is not a thing — it's a vector. " Despite popular perception that the Internet it has evolved into an "Internet of Things," the truth is it has become "The Internet of American Life." As evident from near daily press accounts, all manner of global cyber predators routinely and successfully probe, map and attack the information infrastructure that is "America's Nervous System." The nation therefore now finds itself at the crossroads of Internet reliance and availability.

Any continuity professional will warn that it is both illogical and irresponsible to rely on something over which you have limited or no control. While the term "lessons learned" is frequently used in America as a means of cognitively balancing catastrophic events, predators know the real metric of a lesson learned is a change in behavior and conditions at points of actual or potential impact. From The Predator's View, America has consistently produced only changes in rhetoric. Predators appreciate America's use of terms like "Cyber Pearl Harbor," "New Normal," and the "Internet of Things." They recognize that such characterizations understate reality and are useful in pacifying the masses and slowing efforts to eliminate vectors otherwise increasingly capable of inflicting human, physical, economic and social consequences of unprecedented scope, intensity, and duration.

There are numerous examples of predator success in walking their talk. Among them are:

1. China's aggressive behaviors in the Pacific and its version of the F-35, America's most advanced stealth strike fighter;

2. Russia's employment of Cyber Warfare in Georgia and the Ukraine;

3. Russian and/or Chinese attacks against State Department and White House networks; and

4. Secretary of State John Kerry's remarks: "It's very likely Russia and China are reading my e-mails. "

Through predators' eyes, great reliance enables great consequence. The Predators View is long and patient.

They perceive America as living in the moment rather than in the reality and continuity of time and history. While recognizing English is a very flexible language, predators also see in America's rhetoric a homogenization of otherwise incompatible terms. Specifically, its equation of iteration with innovation, process with progress, activity with accomplishment, and rhetoric with results. From the nation's habit of providing timely and accurate reporting of the effects of attacks on America's Nervous System (its information infrastructure), predators recognize our apparent tolerance for infrastructure degradation and failure, tendency to rationalize events and equate the absence of immediate consequence(s) with success in preventing them.

The Predator's View and the trajectory of infrastructure preparedness has not gone unrecognized. Over a decade ago, in the midst of the continuing consequences of a long-predicted failure of a critical infrastructure and single point of community failure in New Orleans, the Homeland Security Advisory Council's (HSAC's) review of Critical Infrastructure Protection programs resulted in its formally recommending that the Homeland Security Secretary make Critical Infrastructure Resilience (CIR) the national goal . Three years ago, that goal was captured in Presidential Policy Directive-21 "Critical Infrastructure Security and Resilience." While these documents very clearly set the requirement, progress in physically achieving CIR remains obscure at best. Operationally proven CIR mindsets, metrics, methodologies and technologies have been and remain immediately available for implementation. The decision to execute will herald and be the foundation of an advanced infrastructure and

national preparedness culture that is performance-based, comprehensive, nationally compatible, objectively measurable, achievable and sustainable. Given increasing predator exploitation of the "vector" the Internet has become, achieving and sustaining CIR is now the most fundamental and urgent of homeland and national security goals.

Among others, President Ronald Reagan captured the dangers of not eradicating dangers: "Status quo you know is Latin for the mess we are in ." Given the above and far more, the question remains: How does America clean-up ". . . the mess we are in?"

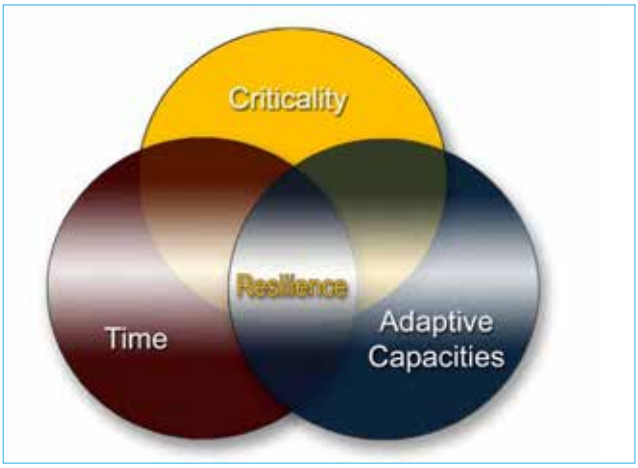
The good news is that despite the current and rapidly mounting dangers looming on its horizon, America has the experience (among others, the Year 2000 Transition), ingenuity and means to deal with existential threats to its cyber-reliant critical infrastructures. CIR is an advanced infrastructure preparedness condition that is symbiotic with existing critical infrastructure sector organization, protection and security programs. CIR, like anything built to last, is constructed and maintained from the ground up. In this case, from American communities, where all interdependent infrastructure operations naturally fuse and from where knowledgeable infrastructure performance requirements are set, single points of infrastructure failure are identified and eliminated, and (beyond information sharing) actionable, trust-building, question and answer-based information exchange originates.

With 50,000+ members deployed in 84 communities throughout the nation, InfraGard Chapters work in concert with local FBI Field Offices and constitute America's greatest resource for achieving and sustaining CIR — and by extension — national resilience. InfraGard members represent infrastructure service providers, businesses, local and state government agencies, academic institutions, emergency responders, faith-based organizations and state, local and federal law enforcement agencies - all of which support the continuity of infrastructure operations in all 16 interdependent infrastructure sectors.

InfraGard's Sector Chief Program and Special Interest Groups at the local and national levels form a network that provides proven experience and expertise in both sector and cross-sector issue identification and resolution, and in the institutionalization of continuous innovation and improvement in the protection, security and resilience of the nation's critical infrastructure(s).

Combined, the expertise and placement of InfraGard members throughout the nation advances the ability of the FBI and its federal partners to identify and address threats to America's critical infrastructure(s), and identify infrastructure performance shortfalls and Single Points of Failure throughout the nation. InfraGard is also a key source of the timely, accurate and actionable information required to attain and sustain the security and operational resilience of America's critical infrastructures — to include the creation of a Minimum Essential National Infrastructure that, true to its name, will (short of Global Armageddon) provide sufficient infrastructure capacities to sustain American life. In a nutshell, InfraGard meets the spirit, intent and letter of what Governor Tom Ridge, the first Department Homeland Security (DHS) Secretary, had in mind when he set the Department's mission culture, created and led DHS's execution of the following maxim: "When America's hometowns are secure, the homeland will be secure."

Turning to CIR execution, Einstein is quoted as saying: "If you can't explain it simply enough, you don't understand it well enough." Consistent with that truth, the objectively measurable and operationally proven CIR process is captured in the following Venn diagram:



CIR implementation requires entities ranging from individuals and businesses to communities, regions and the nation to:

1. Identify the cyber and physical infrastructure capacities that are critical

to their daily lives and operations;

2. Decide how long (time) any entity is willing to be without what is critical to it; and

3. Identify and/or create the adaptive capacities required to deliver critical infrastructure capacities within the time any entity is willing to be without them.

When implemented, CIR provides for the "predictable provision of essential infrastructure products and services and empowerment of essential functions© ." It is a proven, pragmatic, risk-based, performance-driven, nationally comprehensive and compatible, achievable and sustainable infrastructure operating and preparedness standard. Its achievement will leverage the power inherent in America's freedoms and its citizens' independence, innovative spirit and technological supremacy. The continuous application of resilience mindsets, improvement effected by always questioning the status quo, its metric (time), methodologies (illustration above), and innovations (e.g., cyber indications and warning); will:

1. Balance a national preparedness culture that is currently heavily focused on response and recovery; and

2. as General Russel Honoré, Task Force Katrina Commander, noted: will get America to ". . . the left side [prevention and continuity of operations] of the event horizon."

While time is the metric of resilience, it is no longer on America's side. The critical infrastructure reliance culture must be replaced with a critical infrastructure resilience culture that continuously:

1. Identifies and eliminates all single points of infrastructure failure;

2. Distorts "the predator's view";

3. Reduces infrastructure target values and the immediate and cascading consequences of attacks upon, or failures of, those targets regardless of cause;

4. Informs coherent investment in critical infrastructure (to include creation of a Minimum Essential National Infrastructure);

5. Creates an American Renaissance - a culture and resulting actions that enables continuous infrastructure innovation, investment and robust job creation to modernize and make resilient America's infrastructure foundations and all they empower; and

6. Builds national unity by enabling all Americans to work simultaneously in their best interests and ultimately in the best interests of all.

BOTTOM LINES: Sober recognition, understanding and appreciation of The Predator's View are the first steps in countering their objectives. What Americans take for granted as things common to our everyday lives, predators of all stripes from the "lone wolf" to nation-states and their allies, view as legitimate targets. The question remains whether CIR will be executed proactively and with precision or reactively and chaotically in the wake of yet another otherwise preventable tragedy.

America has the responsibility and ability to correct its increasingly infrastructure-enabled and consequence amplifying preparedness trajectory. In the process of doing so, America will disrupt the designs of global predators, reclaim control of its enablers, and build the foundation for a safer, stronger and more secure nation for present and future generations.

Time is the metric of resilience, but it is clearly no longer on America's side.

The Predator's View: The Imperative for Critical Infrastructure Resilience
By Jeff Gaynor, Colonel, U.S. Army (ret.) ,Former President, Chief Executive Officer and Director, Board of Directors, InfraGard National Members Alliance

Previously published in The Executive Journal of InfraGard San Diego (Volume 1, Issue 3). *Copyright © 2016 InfraGard San Diego Members Alliance. Reprinted with permission of InfraGard San Diego Members Alliance.*

In the Age of Uncertainty We Need More Cooperation and Coordination

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

As we all know - we live in an age of uncertainty – we are continually facing new and unforeseen threats to our security.

The ever-changing nature of those threats, whether natural through climate change, or man – made through terrorism activities, such as physical or cyber-attacks.

This means that to be able to act quickly and effectively we have to continually review and update policies, practices and technologies to meet these ever-growing demands.

Critical infrastructure must be secure and able to withstand and rapidly recover from all hazards.

Achieving this requires integration within the national preparedness systems across – Prevention – Protection – Mitigation - Response and Recovery.

It also requires sustainable Connectivity - Coordination - Cooperation and Communication between all those who are involved within the world of CIP.

As an association we continue do our best to facilitate this process in a number of important ways.

By co-hosting key events around the world, including:

- Critical Infrastructure Protection and Resilience Asia (www.cip-asia.com)
- Critical Infrastructure Protection and Resilience Europe (www.cipre-expo.com)
- Critical Infrastructure Protection and Resilience North America (www.ciprna-expo.com)

In addition to these events we also support other key events both Myself and our Eastern European Director, Robert Mikac were delighted to have recently taken part in the 3rd edition of the International Conference "CRITICAL INFRASTRUCTURE PROTECTION FORUM – CIP FORUM III 2018 - Council of the European Union Presidency 2019. Building Resilience in European Critical Infrastructure", which took place in Bucharest, at the Palace of the Parliament, between 24-25 of April, 2018.

The event was attended by more than 700 guests representing 125 institutions from 29 countries. The conference benefited from 71 speakers representing ministries, public authorities and private institutions, under the aegis of 10 universities and research institutes with expertise in the field.

We promote regional dialog by appointing 5 Regional Directors including our latest appointment Professor Matthew Warren, as Regional Director for Australasia.

We have also established a communication network with regular email Newsletters and enjoy the support of the World Security Report

Last year we launched our global members extranet **www.IACIPP.net**, a vital tool in supporting our community and facilitating the exchange of appropriate infrastructure related information and maximise networking opportunities.

The Association continues to develop and we have a number of activities we plan to deliver before Critical Infrastructure Protection and Resilience Europe in October this year, these include:

- Continuing to develop the range and scope of our Working Groups. In particular around transport - energy - telecomms – cyber.
- Producing a Digital Aide Memoir for CIP practitioners around the world.
- Delivering some bespoke educational programmes around some generic threats such as Terrorism and Cyber and also some more specific areas such as Physical Security
- And of course, we want to continue to grow our membership globally.

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

The IACIPP Poll

In the last issue we asked you the following question. Now see the answers...

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

1. Defense	0%
2. Nuclear	0%
3. Energy	13%
4. Transport	6%
5. Telecomms	6%
6. All of them	69%
7. None of them	0%

Visit www.cip-association.org to see the latest poll.

World's Biggest Marketplace Selling Internet Paralysing DDOS Attacks Taken Down

Webstresser.org sold Distributed Denial of Service attacks that could knock the internet offline for as little as EUR 15.00 a month

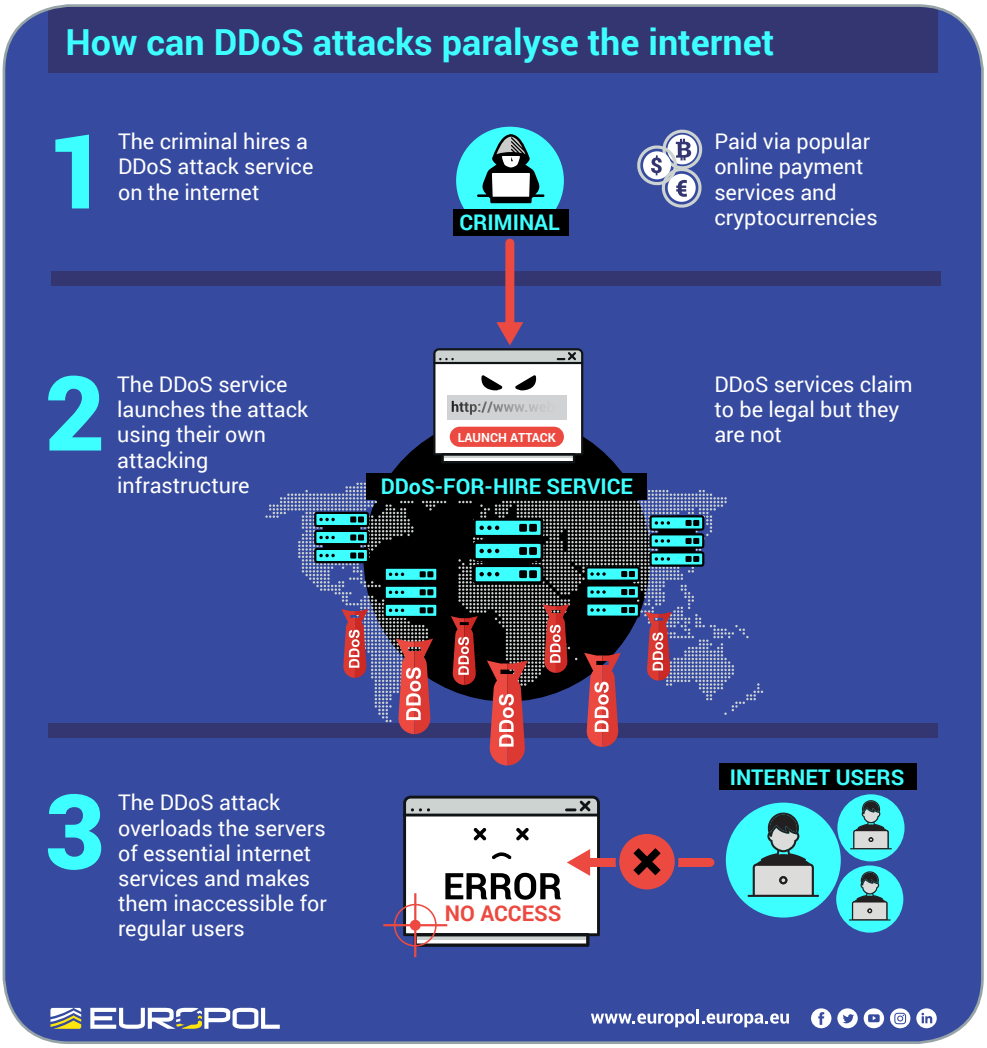
The administrators of the DDoS marketplace webstresser.org were arrested on 24 April 2018 as a result of Operation Power Off, a complex investigation led by the Dutch Police and the UK's National Crime Agency with the support of Europol and a dozen law enforcement agencies from around the world. The administrators were located in the United Kingdom, Croatia, Canada and Serbia. Further measures were taken against the top users of this marketplace in the Netherlands, Italy, Spain, Croatia, the United Kingdom, Australia, Canada and Hong Kong. The illegal service was shut down and its infrastructure seized in the Netherlands, the US and Germany.

Webstresser.org was considered the world's biggest marketplace to hire Distributed Denial of Service (DDoS) services, with over 136 000 registered users and 4 million attacks measured by April 2018. The orchestrated attacks targeted critical online services offered by banks, government institutions and police forces, as well as victims in the gaming industry.

Devastation for hire

In a DDoS attack enabled by such a service, the attacker remotely controls connected devices to direct a large amount of traffic at a website or an online platform. Whether this traffic eats up the website's bandwidth, overwhelms the server, or consumes other essential resources, the end result of an unmitigated DDoS attack is the same: the victim website is either slowed down past the point of usability, or it's knocked completely offline, depriving users from essential online services.

It used to be that in order to launch a DDoS attack, one had to be pretty well versed in internet technology. That is no longer the case. With webstresser.org, any registered user could pay a nominal fee using online payment systems or cryptocurrencies to rent out the use of stressers and booters. Fees on offer were as low as EUR 15.00 a month, thus allowing individuals with little to no technical knowledge to launch crippling DDoS attacks.



International law enforcement cyber sweep

International police cooperation was central to the success of this investigation initiated by the Dutch National High Tech Crime Unit and the UK National Crime Agency, as the administrators, users, critical infrastructure and victims were scattered across the world.

Europol's European Cybercrime Centre (EC3) and the Joint Cybercrime Action Taskforce (J-CAT) supported the investigation from the onset by facilitating the exchange of information between all partners. A command and coordination post was set up at Europol's headquarters in The Hague on the action day.

"We have a trend where the sophistication of certain professional hackers to provide resources is allowing individuals – and not just experienced ones – to conduct DDoS attacks and other kind of malicious activities online", said Steven Wilson, Head of Europol's European Cybercrime Centre (EC3). "It's a growing problem, and one we take very seriously. Criminals are very good at collaborating, victimising millions of users in a moment form anywhere in the world. We need to collaborate as good as them with our international partners to turn the table on these criminals and shut down their malicious cyberattacks."

"Stresser websites make powerful weapons in the hands of cybercriminals" said Jaap van Oss, Dutch Chairman of the Joint Cybercrime Action Taskforce (J-CAT). "International law enforcement will not tolerate these illegal services and will continue to pursue its admins and users. This joint operation is yet another successful example of the ongoing international effort against these destructive cyberattacks."

DDoS-ing is a crime

DDoS attacks are illegal. Many IT enthusiasts get involved in seemingly low-level fringe cybercrime activities, unaware of the consequences that such crimes carry. The penalties can be severe: if you conduct a DDoS attack, or make, supply or obtain stresser or booter services, you could receive a prison sentence, a fine or both.

The individuals that become involved in cybercrime often have a skill set that could be put to a positive use. Skills in coding, gaming, computer programming, cyber security or anything IT-related are in high demand and there are many careers and opportunities available to anyone with an interest in these areas.

Security Technology, Protocols and People in Sync through Training

Most of us admire the skill and ability of today's racecar teams. Some of us may have even entertained becoming part of one. However, without first understanding how an open wheel car works and how every person, part and track affects the ride, it would be impossible to get anywhere. The same holds true for inspection technology, security protocols and the personnel responsible for implementing the plan. Today's security plans include a wide variety of technology and techniques and require multiple levels of skill and knowledge for peak performance. Like a championship racecar team, each individual needs to know more than their part; and when they are all working in sync, the result is a winner.

Security has become paramount in today's infrastructure. Whether airports, stadiums, ports or border transit points, security plans include areas managed by security staff, technology or a combination of both. In addition, non-security staff need to aware of what look for and how to handle issues if they arise. All of this happens amidst the public while not showing them what's under the hood. It's a tall order for any security plan to contain.

As threats evolve, protocols change and technology becomes more powerful and sophisticated the most important component of a plan -- the people -- must remain well informed and consistently up to date.

Syncing up personnel and technology

When considering the different types of individuals employed in the security industry and how they are to use their assigned technology within the security plan, it becomes apparent that the more knowledge and experience they have the better they will perform. Training is the key to successful security programs. Training personnel to perform their duties, use their technology, understand the plan and interact with the public takes the right experience, the best message and the easiest delivery system.

Consider a volunteer at a world-class

event. It's possible this volunteer is going to be checking tickets with a barcode scanner before the security checkpoint at the entrance, directing fans to the nearest concession stand and operating the VIP section during the multi-day event. What does this person need to know about security? Ideally, training volunteers in general security techniques as well as their specific duties would be a requirement, but today also training volunteers on advanced security protocols and helping them understand how the technology works gives them the tools to interact with the public and provide important information in the event of an emergency.

At the parking lot or subway exit, the volunteer is the first interaction with the event. Fans at this point could be informed about security protocols, and since volunteers are trained they are able to pass on appropriate information. In addition, volunteers could explain what technology is used and why. This gives fans a high-level understanding of the security they are experiencing and an awareness of protocols to follow.

Another example where comprehensive personnel training increases success of a security program is at the border. At many entry points, multiple agencies are performing different duties. Different screening technology is available to assist personnel in discovering contraband or declaration errors. When all personnel are trained with at least a general knowledge of protocol at the entry point, there is less room for deviations and costly errors.

These two examples demonstrate how training, when combined with a comprehensive security protocol, can help:

- Overall efficiency and effectiveness of security operations
- Interaction and preparedness of the public
- Improved experience with security technology

Current conditions: Compartmentalized and confused

The public, although very aware of the kinds of security issues they may encounter today, expect that the agencies charged with providing security are well informed and will know what to do if a problem were to manifest. Part of that contract with the public is for all parts of a security plan to come together and work in sync to mitigate and respond to threat events. The only acceptable answer is for everyone to work together.

Knowledge is key: The benefit of comprehensive training

Security operations use many types of technology and situation changing protocols in their plans. Training various personnel who need some knowledge of the technology to those who require an expert level of proficiency takes a specialized approach. With online learning, coupled by in-person expertise, everyone from a volunteer to a technology systems operator can gain the level of training necessary to make security successful. Training designed by experts in process, protocol and engineering makes for varying levels of education for each role.

Bundling these levels under one roof, where the agency or company can manage all personnel assists with keeping staff up to date with their skills and allows new information to disseminate quickly.

Modern training: Key questions

Those responsible for implementing security protocols have in the past, focused on basic issues when purchasing training: time and costs. Now is the time to be asking how your training program can get beyond the basic and empower your personnel to obtain the right information to perform at their best.

By viewing training as a strategic contributor to a successful security plan, decision-makers should consider these key questions when making the most effective investment on training:

- How will proper security technology and protocol training increase our effectiveness?
- Is the training accessible for everyone in our hierarchical structure?
- Will my permanent personnel continually update their skills with refresher courses?

- Do experts using real-world scenarios develop the training?

This is a different way of approaching decisions about training course selection, and provides the opportunity to evolve personnel resources of many different security organizations. Ultimately, security directors should be seeking training solutions that enhance the knowledge and skills of their personnel; training has the potential, with the right vision, to be a critical component of the entire security operation and enhance your end user experience.

Author: Melissa Odegaard; Director, Marketing; S2 Global; www.screeningsolution.com

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.

Islamic State propaganda machine hit by law enforcement in coordinated takedown action

On 25 April 2018 law enforcement authorities of the European Union Member States, Canada and the USA launched a joint action against the so-called Islamic State (IS) propaganda machine in order to severely disrupt their propaganda flow. The takedown operation was coordinated by the European Union Internet Referral Unit (EU IRU) within the European Counter Terrorism Centre (ECTC) at the Europol headquarters.

Led by the Belgian Federal Prosecutor's Office and with the support of Eurojust, the operation involved authorities from Belgium, Bulgaria, Canada, France, the Netherlands, Romania, the United Kingdom and the USA in a coordinated effort to hinder IS's central capability to broadcast terrorist material for an undetermined period of time.

The case started at the end of 2015 when Europol informed all EU Member States about the rise of the Amaq News Agency and the technical resilience of the terrorist online infrastructure. Since then law enforcement agencies have, in a continuous joint effort, taken down the web assets of the media outlet.

In August 2016, thanks to contributions from EU Member States and non-EU countries, a first takedown was launched against Amaq's mobile application and web infrastructure. This action forced the propagandists to build a more complex and secure infrastructure to prevent further disruption from law enforcement. In June 2017 a second strike, led by the Spanish Guardia Civil and supported by Europol and the USA, targeted part of the news agency's web assets and infrastructure. The servers seized by the Guardia Civil allowed for the identification of radicalised individuals in more than 100 countries worldwide.

On 25-26 April 2018 a simultaneous multinational takedown, coordinated by Europol's EU IRU and with the support of Eurojust and the Belgian Federal Prosecutor, led to the seizure of digital evidence by law enforcement from Bulgaria (Cybercrime Department in General Directorate Combatting Organised Crime), France (SDAT-SDLC), Romania (Directorate for Countering Organised Criminality – Terrorism Investigation Unit with the support of the Romanian Intelligence Service), and the seizure of IS servers in the Netherlands (Dutch National Police – Internet Referral Unit together with the Belgian Federal Judicial Police – East-Flanders), Canada and the USA. Meanwhile, the United Kingdom (Counter Terrorism Internet Referral Unit) took the lead in the referral process of top-level domain registrars abused by IS.

With this takedown action, targeting major IS-branded media outlets like Amaq, but also al-Bayan radio, Halumu and Nashir news, IS's capability to broadcast and publicise terrorist material has been compromised.

Rob Wainwright, Executive Director of Europol, commented: 'With this ground-breaking operation we have punched a big hole in the capability of IS to spread propaganda online and radicalise young people in Europe. I applaud the determined and innovative work by Europol and its partners to target a major part of the international terrorist threat prevalent in Europe today.'

Main mouthpiece of IS

Initially giving the impression of an independent media outlet providing factual information on IS, Amaq was used in 2016 to claim the attacks in the Levant and all over the world, including the attacks in Paris, Brussels, Barcelona and Berlin, and more recently in Trèbes (France). Amaq News Agency is the main mouthpiece of IS. It was officially endorsed by the terrorist organisation in July 2017 and has since become the primary source of information regarding the remaining activities of IS worldwide.

Since 2015 Amaq News Agency has been launching its own software and has developed highly resilient online infrastructure hosting. As of December 2017 the entire range of IS propaganda is available in at least nine different languages, as well as a wide range of online services, such as mailed newsletters and add-on extensions for the most common browsers.

Law enforcement agencies involved expect that the data retrieved as a result of the takedown will help to identify the administrators behind IS media outlets and potentially radicalised individuals on European soil and beyond.

In the context of the EU Internet Forum, the EU IRU proactively monitors online propaganda activities of the listed jihadi terrorist organisations in the EU on a daily basis, including related websites, servers and applications disseminating IS propaganda.

Commissioner Julian King said: 'This shows that by working together we can stamp out the poisonous propaganda Da'esh has used to fuel many of the recent terror attacks in Europe. For too long the internet has been open to terrorists and those who seek to do us harm: those days are coming to an end thanks to this type of coordinated global work.'

Project Stadia brings together experts on sports event security

With the safety and security of major events relying on effectively integrating people, technology and processes, Project Stadia has brought together experts from law enforcement, FIFA, venue operators, sporting clubs and the private security sector to shape solutions for this security challenge.

A core component of INTERPOL Project Stadia is to create a Centre of Excellence to help INTERPOL member countries in planning and executing policing and security preparations for major sporting events.

To achieve this, Project Stadia is mandated to organize expert group meetings on the key themes of physical security, legislation and cybersecurity.

These meetings bring together global experts from law enforcement, event organizing committees, government, the private sector, academia and civil society to explore state-of-the-art research and analysis and develop independent recommendations for planning and executing security arrangements for major international sporting events.

Col. Mohammed Majid Al-Sulaiti, Director of the Security Department of Qatar's Supreme Committee for Delivery & Legacy, said: "In our bid to host the FIFA World Cup we told the world to expect amazing. To deliver on this promise, in partnership with INTERPOL, we have brought together experts from all over the world along with Qatari law enforcement officers to enable the transfer of knowledge, experience and share good practices to prepare us for 2022."

The main objective of the 3rd Stadia Sports Safety and Security Expert Group meeting (23 25 April) was to shape best practices in key areas such as cooperation and communications with public security, skills and training, accreditation procedures, and command and coordination.

John Beattie, Stadium and facilities Director at Arsenal Football Club, said: "The expert group meeting on sports safety and security organized by INTERPOL's Project Stadia brought together a number of experts who provide relevant knowledge and skills. The resulting questions and discussions will assist with security preparations in the running of the 2022 World Cup."

INTERPOL and Banco do Brasil S/A sign cooperation agreement against cybercrime

The INTERPOL National Central Bureau (NCB) in Brasilia and Banco do Brasil S/A have signed an agreement for cooperation and information sharing to tackle cybercrime.

This public-private partnership, which came into effect 7 May 2018, aims to establish a systematic exchange of data related to cyber threats so as to enhance cyber security activities undertaken by INTERPOL and its 192 member countries.

As part of the agreement, Banco do Brasil S/A will second a representative to INTERPOL's Global Complex for Innovation (IGCI) in Singapore to work alongside specialists from other technology and financial companies, as well as with INTERPOL officers on secondment from member countries.

During the agreement ceremony at NCB Brasilia, the President of Banco do Brasil S/A, Mr. Paulo Rogério Caffarelli, applauded the agreement, emphasizing how the bank already works with the Brazilian Justice and Federal Police. The signing of the agreement will now trigger the development of information technology solutions and strategic tools to prevent and fight cybercrime.

The General-Director of the Brazilian Federal Police, Mr. Rogério Galloro – who is also a Delegate for the Americas on INTERPOL's Executive Committee – highlighted the importance of expanding and intensifying cooperation with Banco do Brasil S/A in the fight against cybercrime and in the development of new security technologies. Mr. Galloro pointed out that the agreement is an important step for Brazil towards expanding its activities on the international scene.

BT Joins Forces with EUROPOL to Build Safer Cyber Space

BT has signed a Memorandum of Understanding (MoU) with Europol to share knowledge about major cyber threats and attacks, as the two organisations reinforce their efforts to create a safer cyber space for citizens, businesses and governments.

The agreement, which was signed at Europol's Headquarters in The Hague in the Netherlands, provides a framework for BT and Europol to exchange threat intelligence data as well as information relating to cyber security trends, technical expertise and industry best practice.

Steven Wilson, Head of Business, European Cybercrime Centre (EC3), said: "The signing of this Memorandum of Understanding between Europol and BT will improve our capabilities and increase our effectiveness in preventing, prosecuting and disrupting cybercrime. Working co-operation of this type between Europol and industry is the most effective way in which we can hope to secure cyberspace for European citizens and businesses. I am confident that the high level of expertise that BT bring will result in a significant benefit to our Europe wide investigations."

Kevin Brown, VP, BT Security Threat Intelligence, said: "As one of the world's largest cyber security businesses, we at BT have long held the view that co-ordinated, cross border collaboration is key to stemming the global cyber-crime epidemic. "We're working with other law enforcement agencies in a similar vein to better share cyber security intelligence, expertise and best practice to help them expose and take action against the organised gangs of cyber criminals lurking in the dark corners of the web. The signing of today's accord with Europol sees BT take another significant step forward in making the internet a safer place for consumers, businesses and public sector bodies in the UK, Europe and beyond."

BT is committed to sharing its threat intelligence data with industry partners and law enforcement agencies such as Europol in a secure and trusted way, as a means of better protecting UK and global customers from the rapidly expanding cyber-crime industry. Earlier this year, it became the first telecommunications provider in the world to start sharing information about malicious software and websites on a large scale with other ISPs via a free online portal – the Malware Information Sharing Platform (MISP). Since the platform was launched, BT's worldwide team of more than 2,500 cyber security experts have so far helped to identify and shared the details of more than 200,000 malicious domains. The recipients of BT's threat intelligence data have then able to take the appropriate course of action to protect their customers and stakeholders against the specific threats identified.

Cybercrime Prevention: A Unified Message Towards Online Criminals

EU Member States, Europol Third Parties and EU Agencies join forces to strengthen the current cooperation model in the area of prevention and awareness as a way to contribute to the reduction of cybercrime.

Under the coordination of Europol's European Cybercrime Centre (EC3), law enforcement representatives from 29 countries1 gathered with delegates from the EU Agency for Network and Information Security (ENISA), the EU Agency for Law Enforcement Training (CEPOL) and the EU Crime Prevention Network (EUCPN) in the fourth Cybercrime Prevention and Awareness Forum to assess the status and further implementation of the current EU communication strategy model. Initiated in 2015, the model aims to align the cybercrime prevention and awareness efforts among the EU Member States and to increase the effectiveness of the educational materials produced.

Initiatives such as No More Ransom, Stop Child Abuse – Trace an Object, Say No to child sexual coercion and extortion and the European Money Mule Action, among others, were presented as best practices of what can be achieved through optimization of human and financial resources, both at a national and an EU level.

The EC3 organises the Cybercrime prevention Forum with the aim to facilitate the cohesion of activities and campaigns, the sharing of existing materials, the development of new ideas and the exchange of best practices. Ultimately, its purpose is to enable a pan-European dialogue among all law enforcement entities in the area of prevention and awareness, thus strengthening the EU's fight against cybercrime.

Pre-screening visa-exempt travellers for increased security when travelling to Europe

Third country nationals exempt from visa requirements will have to get an authorisation before travelling to the EU, under new rules approved on Wednesday by the Civil Liberties Committee.

MEPs backed, with 45 votes to 10, the informal deal reached with EU ministers establishing a new European Travel and Authorisation System (ETIAS).

The system, which should be operational in 2021, will allow for advanced checks on visa-free travellers and those considered to pose a risk in terms of security, irregular migration or high epidemic risk will be denied access.

Non-EU nationals who do not need a visa to enter the Schengen area will have to fill in an electronic form prior to their intended travel with their personal data (including name, date and place of birth, sex and nationality),

travel document information (validity, country of issue), home address and contact information, and the European country of first intended entry.

A dedicated public website and an application for mobile devices will be set up, managed by eu-LISA (the EU Agency for the operational management of large-scale IT systems in the area of freedom, security and justice).

The travel authorisation will cost 7 euros (Parliament negotiators managed to waive the fee for travellers under 18 and over 70 years of age), and it will be valid for three years, or until the travel document expires.

The applicant will also need to inform authorities of any convictions for serious criminal offenses (such as terrorism, sexual exploitation of children, trafficking in human beings or drugs, murder and rape), about stays in specific war or conflict zones and of any prior administrative decisions requiring them to leave a country, all over the last ten years.

In the case of terrorist offences, the period will extend to the previous twenty years, and additional clarification on the date and country of the conviction will be needed.

MEPs succeeded in removing all health-related questions from the application. They also restricted the level of detail required on occupation (to job group) and education (just primary, secondary, higher or none) related information.

The application will automatically be checked against all relevant databases, including the new ETIAS' watch list (which, fed by Europol, will include suspects of terrorism or other serious crimes), the Schengen Information System, the Entry/Exit System, as well as other Europol and Interpol databases to verify, among other issues, whether the travel document used has been reported lost or stolen and whether the person is wanted for arrest.

If there are no hits, the travel authorization will be issued automatically (that is expected to be the case for the vast majority of applications). In case of one or several hits, or a positive reply to any of the questions on criminal records, trips to conflict areas and orders to leave a country, the data will be manually checked and the security, migration or epidemic risk individually assessed. The applicant may be requested to provide additional information, and in exceptional circumstances may be invited for an interview.

Travellers should get a reply, or a request for additional information, within 96 hours from the moment of lodging the application. Thanks to amendments introduced by Parliament, they will be able to check the status of the application, via the webpage and mobile application.

Kinga Gál (EPP, HU), Parliament's rapporteur, said: "I consider the ETIAS extremely important for the security of EU citizens as there is no freedom without security. Our aim was to create a system which contributes to a more secure Europe preventing terrorism, illegal immigration and epidemic risks, but which won't put an excessive burden on visa exempt citizens visiting the EU."

The draft legislation will now be put to a vote by plenary, scheduled in July. Once formally adopted by the Council of Ministers, it will be published in the Official Journal. The aim is for it to be operational in 2021.

There are currently more than 60 countries and territories whose nationals can travel visa-free to the EU. The Commission expects a significant increase in the number of visa-exempt travellers crossing the Schengen borders in the coming years, from 30 million in 2014 to 39 million in 2020.

Disasters could cost Asia-Pacific region $160 billion per year by 2030, UN warns

Economic losses to disasters in Asia and the Pacific could exceed $160 billion annually by 2030, the United Nations development arm in the region warned on Tuesday, urging greater innovation in disaster risk financing.

The need is all the more pressing given that only eight per cent of region's losses are insured, said the UN Economic and Social Commission for Asia and the Pacific (ESCAP).

"The time for establishing solutions to these complex emerging challenges is now," underlined Shamshad Akhtar, the Executive Secretary of ESCAP, speaking at an event on financing for disaster risk reduction in Asia-Pacific at the UN Headquarters, in New York.

The low insurance coverage has persisted in the region even though it has suffered nearly $1.3 trillion in losses over the last 50 years.

The result is that individuals, businesses and Governments are left to bear the staggering costs of natural calamities. And with extreme weather events increasing as the region's cities become more crowded, the gap could widen.

"Business as usual is unsustainable […] policy makers and financial strategists in both the public and private sectors have to work together," said the head of ESCAP.

In her remarks, Ms. Akhtar outlined the opportunities offered by recent innovations such as catastrophe risk modelling, parametric insurance, a mix of traditional and global financial reinsurance, and concessional insurance.

She also highlighted the role ESCAP – which spans a geographic region from Turkey in the west to the tiny Pacific island of Kiribati in the east, and from Russia in the north to New Zealand in the south – could play.

"The provision of a regional platform for building capacity as well as mutual trust among countries is the key to successful sovereign risk pooling [and] ESCAP, whose primary mandate is regional cooperation, is well suited for this role," said Ms. Akhtar.

Speaking alongside Ms. Akhtar, Mami Mizutori, Head of the UN Office for Disaster Risk Reduction (UNISDR), highlighted the importance of both disaster risk financing and resources to reduce disaster risk to ensure resilient and sustainable development.

"At present, we need both […] Let's face it: when natural hazards hit, without these mechanisms, we cannot cope with the aftermath," she said.

Ms. Mizutori, who is also the Special Representative of the UN Secretary-General for Disaster Risk Reduction, also highlighted the importance national strategies to strengthen resilience and mitigate natural hazard risks, a call made in the Sendai Framework for Disaster Risk Reduction.

NEMOSYS-XRTM selected for high-end defence applications

EXAVISION has been selected by French integrators to provide NEMOSYS-XRTM for military camps protection in Africa and military airbase surveillance and Counter-UAV projects in France.

NEMOSYS-XR™ is a modular range of optronic solutions integrated on a 2-axis Pan&Tilt, that comes with a Full HD color camera, a Made in France cooled (Band II MWIR) thermal camera, and complementary options (GPS, DMC, LRF …) allowing long range observation and surveillance for day and night purposes. NEMOSYS-XR™ has been developed and designed to provide customers with robust, easy to use and performing solution for critical infrastructure surveillance.

NEMOSYS-XR™ solution is the result of EXAVISION experience in designing video supervision systems (linked to radar detection and non-lethal effectors) dedicated to sensitive area protection as borders and coastal surveillance, military camps protection, ports and airports, petrochemical and nuclear industries.

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

NATO wins the world's largest live-fire cyber exercise

NATO has won the world's largest live-fire cyber exercise, Locked Shields 2018. After an intense competition from 23 to 26 April, NATO's "Blue team" of 30 cyber defenders – led by the NATO Communications and Information (NCI) Agency – took the top prize in Tallinn, Estonia. French and Czech teams placed second and third, respectively. In total more than 1,000 experts from nearly 30 nations participated this year.

"I could not be more proud of the success of our cyber-team that once again demonstrated the expertise of NATO's technology agency. They are hard-working, dedicated and ready 24/7 to defend NATO

networks," said Kevin J. Scheid, General Manager of the NCI Agency.

"This year's exercise was even more realistic and certainly tougher than ever before and we are incredibly proud of our NATO cyber defenders," said Ian West, Cyber Security Chief at the NCI Agency. The drill challenged the participants to respond in countering high-intensity attacks on a fictitious country's IT systems and critical infrastructure networks.

"Success in Locked Shields is not just about defending your own networks – it is also about collaborating closely with the other defending teams," explained Ian West. The teams had to maintain complex IT systems while reporting incidents, managing crises and making strategic decisions, as well as solving digital forensics tasks, and dealing with other challenges. Altogether the exercise involved 4,000 virtualized systems and more than 2,500 attacks.

Cyber defence is part of NATO's core task of collective defence. In July 2016, Allies recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea. The NATO Communications and Information Agency acquires, deploys and defends communications systems for NATO's political decision-makers and commands.

UN-backed programme logs record high cocaine seizures at seaports in Latin America and the Caribbean

UN-trained law enforcement units have intercepted huge shipments of illegal drugs being trafficked through seaports this year, including 2.8 tons of cocaine at Brazil's Port Santos, the largest such seizure in the port's history

The joint customs and police Port Control Units, work at some of the world's busiest ports and are trained to combat smuggling of drugs, precursor chemicals, as well as merchandise breaching intellectual property rights and protected wildlife.

Recently, the Unit in Ecuador has seized two contaminated containers with over a tonne of cocaine. Similarly, the Unit in the Port of Callao in Brazil, interdicted a container with 1.5 tons of cocaine hidden inside.

These units are at the heart of a joint programme launched in 2003 by the UN Office on Drugs and Crime (UNODC) and the World Customs Organization.

The aim is to train customs and law enforcement officials in Latin America and the Caribbean, and elsewhere, to detect and disrupt the flow traffic of illicit goods, while facilitating legitimate trade and raising State revenues.

Every year, more than 720 million containers move around the globe by sea, transporting 90 per cent of the world,s cargo. Most carry licit goods, but some are being used to smuggle drugs, weapons, and other illicit goods.

"The Container Control Programme has become one of the most effective and result-oriented programmes worldwide," said Tofik Murshudlu, UNODC's Chief of the Implementation Support Section.

The Programme also helps Member States build capacities and expertise to identify and seize suspicious container shipments of drugs, firearms, precursors, counterfeit medicines, wildlife species, smuggled goods and many others, he added.

According to the UNODC, 18 operations have netted more than 8.9 tons of drugs. In addition, 18 containers have been detained due to intellectual property rights violations.

So far, the Programme is operational in 14 countries in Latin America and the Caribbean, providing site visits, technical assessments, trainings, and other support to create long-term enforcement structures in select seaports. It is also operational in Burkina Faso, Cabo Verde, Ghana, Pakistan, Senegal, Togo and Turkmenistan.

FLIR Launches Radar and Thermal Products for Border Patrol with the ability to detect both drones and land-based objects

FLIR Systems has announced the availability of three products for use by global militaries and government agencies including border patrol agents. These products include two FLIR Ranger® mid-range panel radars, one with airborne drone and ground target detection, and the Recon® V UltraLite thermal monocular. The products, unveiled at the Special Operations Forces Industry Conference (SOFIC) 2018 in Tampa, Florida, are part of FLIR's Soldier Solutions family and demonstrate the company's commitment to deliver the most advanced equipment

to armed services personnel.

The FLIR Ranger R8SS-3D and R8SS radars, part of FLIR Ranger family of radars, offer mid-range detection capability for both fixed-based installation and forward-deployed operations personnel. The R8SS-3D detects both land and air objects, such as micro-drones, and differentiates birds from drones. The Ranger R8SS-3D reports the altitude and location of small drones at ranges of 2 miles and can also detect vehicles and people walking or crawling. Both the R8SS-3D and the R8SS, the latter of which offers land detection only, can detect over 500 threats and their exact locations simultaneously, and work within an existing data network. The R8SS series mount to either a vehicle, surveillance tower, or tripod, and allows for full 360-degree surveillance, ensuring that threats within surveillance range are detected.

Barrett HF on surveillance boats in remote Chilean region

Barrett Communications have recently supplied High Frequency (HF) radio communications equipment for surveillance boats which operate in the remote and environmentally challenging Aysen región in the South of Chile.

The Aysen región in Chile, is not only remote but also very complicated with lake systems, islands, mountains, rivers and extreme climatic conditions. The Barrett authorised dealer in this region, Skytel Telecommunicaciones are present in this area in many organisations that are critical to the community. These organisations include health care services, the aerodromes, the agricultural and livestock service, the national emergencies bureau and the uniformed police.

The HF stations are used in offices, service vehicles, ambulances and also in surveillance and border patrol boats.

The mobile installation kit for the Barrett 2050 HF Transceiver was installed inside the port console and the 2050's detachable front panel along with the external speaker and PTT were installed onto the port console, as requested by the client. From the Barrett 2050 transceiver, a control cable was installed and channeled below the cabin's deck to a crew member seat, where the 4011 tuner was installed in available space under the seat. From there a cable went through one of the cabin walls to reach the HF antenna installed on the port side of the boat using a specially designed mast and a fixing plate."

The HF mobile station was tested under hard and real conditions and was able to establish good quality communications to the nearest port, the closest town, other stations within the same region, and the main station 1,700km away.

Mr José San Martín from Skytel Telecommunicaciones commented "We have designed and installed a complete HF mobile station on the surveillance boats, and the crew can maintain communications over the HF network throughout Chile."

Transportation Security Administration Selects Unisys to Secure, Operate, Maintain and Protect Screening Equipment in U.S. Airports

Unisys Corporation announced it has been selected by the Transportation Security Administration (TSA) to leverage an integrated package of Unisys Stealth® software and application services in developing, implementing and maintaining a suite of mission-critical applications that connect, protect and integrate the agency's security screening equipment deployed at more than 400 U.S. airports.

The work will be performed under the single-award Domain Awareness Integrated Network (DOMAIN) Support Services blanket purchase agreement (BPA) within TSA's Security Technology Integrated Program (STIP). A joint effort by TSA's Passenger Screening Program and Electronic Baggage Screening Program, the Unisys implementation provides a secure and scalable platform to integrate data from passenger and baggage screening equipment for real-time threat awareness and risk assessment.

The BPA has a ceiling value of $250 million over five years and covers a one-year base period followed by four option years. Under the BPA, Unisys will provide full lifecycle application development and operational support services to connect and integrate data from up to 14,000 TSA security equipment devices.

The solution includes Stealth™ microsegmentation software to deliver a powerful deployment model allowing TSA to securely connect and manage all airport screening equipment on the agency's global network. These screening devices perform duties such as scanning baggage and personnel to ensure the safety of travelers entering and leaving U.S. airports.

The Stealth security products deliver adaptive protection through the application of microsegmentation technology across extended enterprises, securing users, data, applications and systems from cyber threats. Through the creation of secure Communities of Interest, authorized users and Internet of Things devices like TSA's screening equipment engage in encrypted Stealth-enabled segments, cloaked from external attackers and protected from insider threats.

New security innovation protected thousands at the recent London Marathon

The annual London Marathon became the latest event to receive the highest levels of protection from potential vehicle attacks.

With over 35,000 runners on the start line on 22 April 2018, and thousands more spectators gathered to cheer on racers, an innovative roadblock system was deployed to safeguard against a possible vehicle attack.

Surface Guard, which was developed by ATG Access, the world's leading designer of road blocker, bollard and vehicle barrier systems, was installed on each side of Parliament Square to protect the people at the event.

The system was deployed extremely quickly, with the team able to install the system at each end of the square in just one hour, keeping road closures, prior to and during the event, to a minimum.

The Surface Guard being deployed at the London Marathon by StadiumTM

Once the event finished, the solution was removed just as quickly, so that the roads and bridge could be reopened an hour after the marathon finished. As the system does not need anchoring to the ground, no damage was caused to the road or pavements when the system was removed.

The Surface Guard has been specifically designed in response to the surge of vehicle ramming attacks that have taken place across Europe and has been tested in accordance with the IWA 14 crash test standard. It is capable of withstanding an attack from a 7,200kg lorry travelling at 32 kph, and its lightweight modular design makes it quick to install, transport and easy to store.

The solution has been designed to complement existing street furniture and blend into the background, making it ideal for use at the event as it did not create unnecessary distress to the public. It was manned throughout the day and saw huge crowds of people walking through the system, as well as pedestrians with prams, wheelchair users and cyclists also able to pass through the barrier with ease.

Glenn Cooper, CEO of ATG Access, said: "The need for increased security at temporary events has been heightened after the recent surge in vehicle attacks across Europe and further afield. It is now more crucial than ever that people feel secure and protected when visiting public events, but solutions used must cause minimal disruption to daily life to prevent creating a 'fortress mentality'.

"Our innovative Surface Guard System was deployed to protect thousands of people at one of the country's largest and most popular sporting events. We were able to deploy and secure the whole square extremely quickly, and because of the flexible configuration and modular shape of Surface Guard, it meant that obstacles weren't an issue to manoeuvre around.

"Surface Guard is still a new innovation for the security market in comparison to traditional concrete blockades and national barrier asset steel barricades. We firmly believe that this solution will prevent further vehicle attacks, and will make safeguarding the public at temporary events easier and more robust for organisers."

Since the launch of Surface Guard, just eight months ago, it has already been deployed to protect numerous high profile events, including the official reopening of Motcomb Street in London, the popular Lord Mayor's show in London and multiple Premier League football stadiums and now the London Marathon.

360 Vision Technology launches UK designed & manufactured INVICTUS Hybrid Ultra-Low-Light HD PTZ camera

360 Vision Technology has recently launched Invictus, a new range of cost-effective, high-performance, ruggedised PTZ cameras – aimed at the competitive midrange CCTV camera sector.

Bridging the divide between analogue and IP systems, and coupled to attractive pricing, Invictus cameras have been designed to deliver a highly competitive all-in-one PTZ camera package, aiming to provide a viable alternative to low-cost options.

Packed with high-end functionality, performance and proven reliability, Invictus Dual Hybrid functionality offers enables installation within existing analogue systems, or stunning full 1080P HD video streaming and IP control – without the need for camera hardware changes.

Invictus achieves incredible ultra low-light colour/mono imaging performance via the choice of either the latest 1/2.8" Sony StarVis, or 1/1.9" Sony Exmor R (Ultra) best-in-class HD camera modules, with a choice of 20:1 or 30:1 zoom. And providing unobstructed scene imaging, Invictus views 360 degrees pan and 160 degrees tilt, alleviating the viewing limitations associated with PTZ dome cameras.

For flexibility of control, Invictus is compatible with a wide-range of data protocols and VMS offerings, and features industry leading ONVIF 2.4 Profile S integration. Watching over intelligent illumination and Night Setting Presets during periods of inactivity, an advanced Low Power mode reduces power consumption by up to 50%, to control illumination and power consumption for use within low power consumption sensitive applications.

Enhancing 24-hour operation, the new Invictus range is the only ruggedised all-in-one PTZ camera to offer both IR and White-light high-intensity illuminators with an industry-leading 200m illumination. Further supporting optimum imaging, Invictus cameras employ the same proven flat viewing window and wiper system as used in Predator. Unlike with dome cameras, this design allows the wiper blades constant, even and uninterrupted contact with the window surface, keeping them clear for 100% effective scene surveillance.

Available with on-board recording options up to 256GB, Invictus also draws on the field-proven 360 Vision high-end 'Predator' camera range for its construction from high grade, hardened aluminium and stainless steel – ensuring a rugged, durable and compact camera.

An upright mounting design and full 360-degree continuous pan and the ability to tilt above the horizon, assure operators an unobstructed view of targets above the camera's horizontal installation height.

HENSOLDT has unveiled its Xpeller counter-UAV system for the first time in a compact and deployable version called "Xpeller Rapid"

The new configuration combines a radar system, a camera, radio detectors and jammers. The system can either be integrated into a vehicle or can be used in a transport container for rapid deployment. Thanks to sensor fusion, which is effected via a smart control software application, all UAV-relevant signals are detected with high precision and extremely short reaction times are ensured.

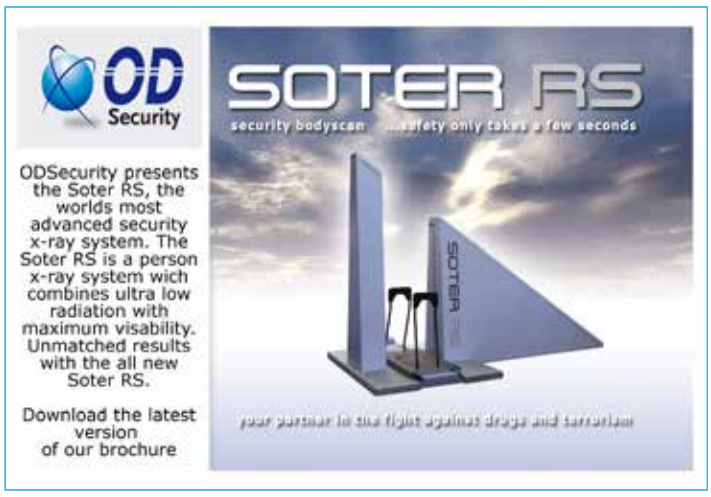
The modular Xpeller product family includes various sensors such as radar systems, cameras and radio frequency detectors as well as direction finders and jammers. Xpeller uses sensors to detect and identify a drone and assess its threat potential at ranges from a few hundred metres up to several kilometres. Based on real-time analyses of the control signals, a jammer then interrupts the link between drone and pilot or interferes with its navigation. The modular Xpeller system concept allows customised solutions to be created by combining individual devices from the product family depending on customer requirements and the local conditions. This way, the customer can select from a set of components and countermeasures. HENSOLDT also supports the development of individual security concepts offering consultancy and weak point analysis..

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.

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.



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

une 2018

5-7
InfoSecurity Europe
London, UK
www.infosecurityeurope.com

11-12
Transport Security & Safety Expo
Washington DC, USA
www.transportsecurityworld.com/events/tssx

11-15
EUROSATORY 2018
Paris, France
www.eurosatory.com

19-21
IFSEC International 2018
London, UK
www.ifsec.events/international

25-27
Security Document World.
London, UK
www.sdwexpo.com

July 2018

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

25-26
Latin America Security Congress
Santiago, Chile
www.isc2latamcongress.com

25-27
Australian Security Industry Association Exhibition & Conference
Melbourne, Australia
www.asial.com.au/events/category/security-conference-exhibition

August 2018

16-18
Secutech Vietnam
Ho Chi Minh City, Vietnam
www.secutechvietnam.com

29-31
Asia Risk & Resilience Conference
Singapore
www.arrconference.com

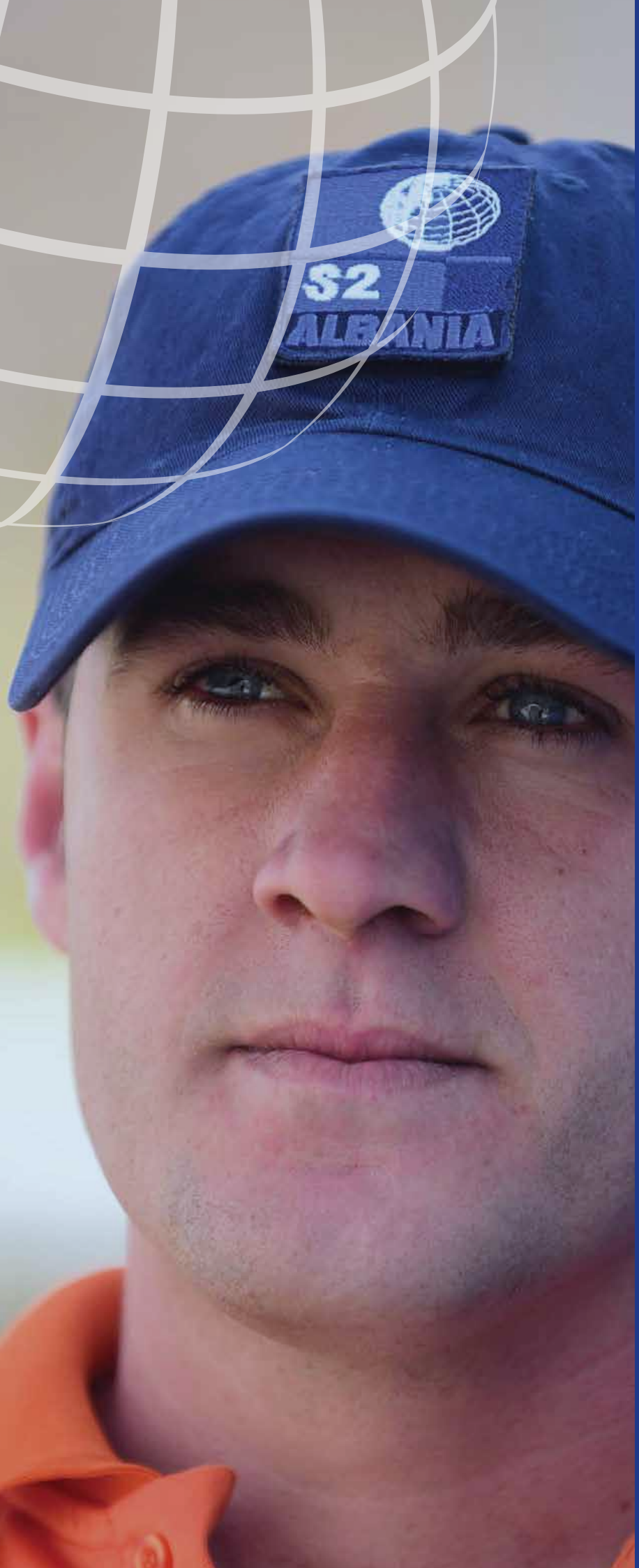
September 2018

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

December 2018

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

WorldSecurity-index.com
The Homeland Defense and Security Database



S2 GLOBAL
An OSI Systems Company

Highly Trained People are a Critical Requirement for Effective Screening Operations

Security initiatives are better served when the people whom are responsible for the processes are highly trained.

S2 Global provides security training for governments and entities looking to maximize the potential of their personnel.

For more information contact
Gary Heffner, Director of Training
gheffner@screeningsolution.com
+1 954-779-7102

www.screeningsolution.com

BORDER SECURITY REPORT

VOLUME 10
MAY / JUNE 2018

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

COVER STORY

ICAO RELEASES FIRST TRAVELLER IDENTIFICATION PROGRAMME (TRIP) GUIDE

SPECIAL REPORT

Transforming Passenger Processing p.21

AGENCY NEWS

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

SHORT REPORT

UN Migration Agency, DR Congo Government Enhance Ebola Screenings at Border-crossings p.11

INDUSTRY NEWS

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

CONTACTS

Editorial:
Tony Kingham
E: tony.kingham@knmmedia.com

Contributing Editorial:
Neil Walker
E: neilw@torchmarketing.co.uk

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

Subscriptions:
Tony Kingham
E: tony.kingham@knmmedia.com

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

Copyright of KNM Media and Torch Marketing.

Inter-agency and international co-operation on the border

I'm pleased to report in this issue that the IOM, the UN Migration Agency, and the World Customs Organization (WCO) have signed a Memorandum of Understanding (MoU) to boost co-operation in coordinated/integrated border management.

At our own conference World Border Security Congress in Madrid last March, the calls for inter-agency and international co-operation was once again a recurring theme, as it will no doubt be in Casablanca next year, so it nice to have something positive to report.

But of course, whilst this is a welcome step in the right direction of inter-agency and international co-operation, it is only that…..a step. Because as important as these two organisations are, they are just two among hundreds of agencies working at borders worldwide, and their remit is limited.

Border police, border guards, immigration officers, coastguards and in some places the military all have a role at the border. And the mix of these national agencies and jurisdictions also varies from country to country. Add international agencies like Interpol, Europol, Frontex, Aseanapol and more, the complexity of border co-operation becomes obvious.

So, in practical terms what can be done. Well our suggestion is to start with very modest ambitions and build from there.

Start with something tangible. Something like a password protected network, similar to a social media platform like LinkedIn, but for border agencies personnel only. It should be free to users and joined on a purely voluntary basis. From there, just like social media, users can build relationships with other users and agencies and start sharing experiences and useful stuff like best practice documents.

Over time, as the number of users grows, and trust grows, it can metamorphize into something altogether more ambitious.

Maybe this MoU is the first step, but the key is to get something started!

We even offered to do it ourselves as part of World Border Security Congress. We have the platform and we even started work, but without funding the project was halted. So, if there is an organisation out there that wants to help do something practical now to promote border co-operation, drop us a line!

Tony Kingham
Editor

READ THE FULL VERSION

The digital version of Border Security Report contains all the additional articles and news listed in the contents page below. The full digital version is available for download at
www.world-border-congress.com/BSR

CONTENTS

BORDER SECURITY REPORT

» p.5

» p.8

» p.18

» p.17

5 ICAO TRIP GUIDE RELEASED

ICAO is releasing the very first version of the ICAO Traveller Identification Programme (TRIP) Guide

8 AGENCY REPORTS

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

12 ATAK SITUATIONAL AWARENESS ARRIVES AT THE BORDER

US CBP leads the way in combining USSOCOM software and consumer communications hardware to greatly increase agent safety and effectiveness.

18 AGENCY NEWS

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

23 TRANSFORMING PASSENGER PROCESSING

SITA report outlines how biometrics in identity management will transform passenger processing.

25 WORLD BORDER SECURITY CONGRESS

A review of the international border security community in Madrid, Spain on 20th-22nd March 2018.

28 INDUSTRY NEWS

Latest news, views and innovations from the industry.

IOM, World Customs Organization to Boost Cooperation Towards Effective, Efficient and Responsible Border Management

On 8 May 2018, IOM, the UN Migration Agency, and the World Customs Organization (WCO), an intergovernmental organization based in Brussels, Belgium, signed a Memorandum of Understanding (MoU) to boost cooperation on issues of mutual interest, in particular, those related to effective, efficient and responsible border management.

This MoU offers the necessary framework for intensified cooperation between the two organizations. It opens increased joint programming opportunities notably in the field of coordinated/integrated border management, as well as in the field of border management and development and trade.

The MoU brings together two agencies with different but complementary mandates: While IOM focuses in its work on the well-being of migrants and the management of border crossings by persons, WCO's work is concerned with the management of the crossing of borders by goods and passengers.

The Memorandum was signed by William Lacy Swing, IOM Director General and Dr. Kunio Mikuriya, WCO Secretary General.

"We see in our member states around the world great interest in the cooperation topics covered in the MoU, especially in Africa, where the relationship between border management and development and trade has become a programming focus for many states, Regional Economic Communities (RECs) and the African Union (AU). IOM is already active in this field, for instance by supporting African states to introduce One Stop Border Posts (OSBPs)," said Ambassador Swing.

The intensified cooperation between IOM and WCO strengthens the support the two organizations can give to Member States to further improve and modernize their border management, facilitate regular border crossings and exchange of goods and services across borders, support development, and better protect migrants.

At the signing, Dr. Kunio Mikuriya stressed that "WCO encourages Customs administrations to adopt a coordinated approach with the various border agencies for greater efficiency over managing trade and travel flows, while maintaining a balance with compliance requirements. Coordinated border management is high on the Customs agenda and WCO has developed in this regard tools and instruments to support its implementation by Members, while involving national and international stakeholders."

The agreement will enhance the collaboration between IOM and WCO through coordinated activities and elimination of unnecessary duplication, increased consultations, exchanges of information and documents for an effective cooperation and liaison between both Organizations' Secretariats or Regional Offices and Country missions.

The MoU encourages both organizations, within their respective complementary mandates, to support their Member States to strengthen international, and intra-state cooperation between their national border agencies, and exchange of information in thematic areas such as: i) border management; ii) sharing of best practices in coordinated border management policies, regulatory frameworks and administrative and institutional structures; iii) capacity building efforts; iv) responsible data collection and information exchange with a focus on risk analysis and risk management; and v) joint research.

INTERNATIONAL ORGANIZATION FOR MIGRATION
IOM·OIM
THE UNITED NATIONS MIGRATION AGENCY

WORLD CUSTOMS ORGANIZATION
ORGANISATION MONDIALE DES DOUANES

ICAO TRAVELLER IDENTIFICATION PROGRAMME (TRIP) GUIDE RELEASED

ICAO is releasing the very first version of the ICAO Traveller Identification Programme (TRIP) Guide on Border Control Management (BCM) to help States optimize their use of the available tools, systems, and applications.

In their traveller border control arrangements, States seek to maximise the economic, social and political benefits of travel while at the same time identifying and mitigating risks and threats. The central concept of the Guide is that BCM is most effective when the iterative process of identification of travellers and risk assessment is repeated as new

information becomes available at each phase of the traveller journey: Pre-Departure, Pre-Arrival, Entry, Stay and Exit.

The TRIP Strategy is a framework bringing together elements of identification management to uniquely identify travellers in order to enhance border security and facilitation. The ICAO TRIP Guide on BCM is a product of the TRIP Strategy and thus focuses on the border controls applied to travellers. The regulatory framework of the Guide is found more prominently in the Annex 9 – Facilitation and in Doc 9303, Machine Readable Travel Documents.

The Guide is intended for reference by States. It includes 13 technical topics describing and categorizing the Inspection Systems and Tools and Interoperable Applications that are used at specific or multiple phases of the traveller journey and each contribute, to different degrees, to the identification of travellers and/or to traveller risk assessment.

Inspection Systems and Tools	Interoperable Applications
A. Visas and Electronic Travel Systems	H. Advance Passenger Information and Interactive Advance Passenger Information
B. Document Readers	I. Passenger Name Record
C. Biographic Identity Verification	J. Public Key Infrastructure and the ICAO Public Key Directory
D. Biometric Identity Verification	K. eMRTD Biometric Identity Verification
E. National Watchlists	L. INTERPOL's Stolen and Lost Travel Documents Database
F. Entry and Departure Databases	M. International Watchlists
G. Automated Border Controls	

Traveller identification and risk assessment is repeated throughout the traveller journey as additional information becomes available to the receiving/ destination State

While States can be expected to have extensive knowledge of their own citizens and residents, they rely on foreign data and information about the identity and nationality of the citizens and residents of other States. Therefore, the Standards and Recommended Practices (SARPs) and technical specifications published by ICAO play a critical role in ensuring that travel documents issued by States contain standardised traveller identity information in a standardised machine readable format and that the identity information can be communicated in a standardised, interoperable way.

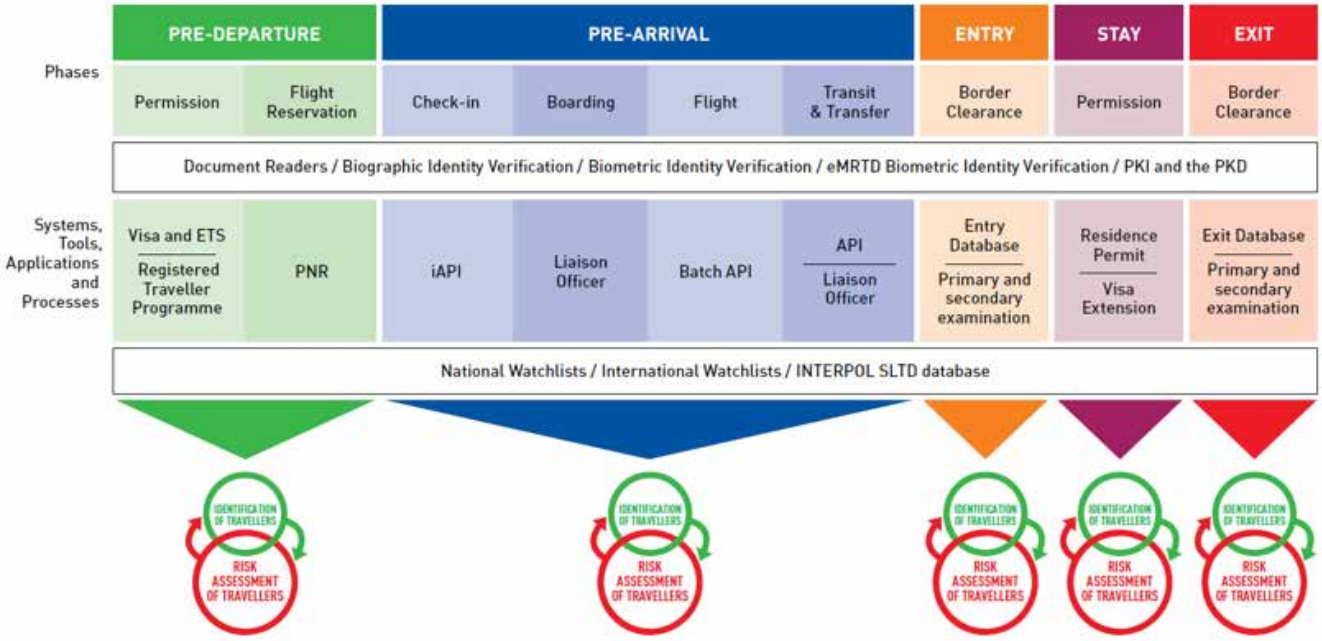
The Guide further discusses contributions made by other United Nations (UN) agencies and international organisations to BCM. The Consolidated UN Security Council Sanctions List and INTERPOL Red Notices identify potential travellers of security and law enforcement concern to States. Checks against INTERPOL's Stolen and Lost Travel Documents database are essential prior to relying on travel documents as evidence of identity.

When applied in conjunction with its companion document, the Assessment Tool, the Guide can improve the traveller identification and risk assessment practice of States to achieve better security and facilitation outcomes in BCM.

The ICAO TRIP Guide on BCM is available at www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

To ask questions or communicate with the Facilitation Section, States are invited to write to: FAL@icao.int.

ICAO extends heartfelt thanks to individuals and organizations that have contributed to develop the content of the Guide: European Border and Coast Guard Agency (FRONTEX), ICAO Implementation and Capacity Building Working Group (ICBWG), ICAO New Technologies Working Group (NTWG), International Criminal Police Organization (INTERPOL), International Organization for Migration (IOM), Joint Regional Communication



Centre (JRCC) of the Caribbean Community (CARICOM) Implementing Agency for Crime and Security (IMPACS), Organisation for Eastern Caribbean States (OECS), United Nations Counter-Terrorism Committee Executive Directorate (CTED), United Nations High Commissioner for Refugees (UNHCR) and United Nations Office on Drugs and Crime (UNODC).

WCO supports CITES national ivory action plans

The WCO participated in the recent CITES National Ivory Action Plan (NIAP) Meeting held in Maputo, Mozambique.

On this occasion, as one of the five intergovernmental member organizations making up the International Consortium on Combatting Illegal Wildlife Crime (ICCWC), the WCO (i) delivered a presentation on the role of Customs Risk Management in support of Illegal Wildlife Trade (IWT) enforcement operations and NIAPs; (ii) facilitated a session, in support of INTERPOL, relating to criminal prosecutions; and (iii) led the discussions by a working group dealing with cross-border and international cooperation issues.

CITES NIAPs are practical tools under the CITES Convention, used by a number of its Member states to strengthen their controls on the ivory trade and markets, and to help them combat the illegal trade in ivory. These NIAPs are developed in compliance with recommendations made by the CITES Standing Committee. Each Plan outlines the urgent measures that a CITES Party commits to delivering – including legislative, enforcement and public awareness actions – along with specified implementation time-frames and milestones.

While the Plans follow a common structure of actions with time-frames and milestones, each NIAP is unique. A Plan should identify the actions that are of highest priority for a particular Party to help combat the illegal ivory trade, depending upon the Party's own circumstances including its capacity-building needs, available resources, and the scale and nature of the illegal trade, and whether the Party is a source, transit or destination country for illegally acquired ivory.

8 Arrested for Smuggling Migrants to Germany in Lorries

With the support of Europol's European Migrant Smuggling Centre (EMSC), three individuals suspected of facilitating large-scale irregular migrant smuggling to Germany have been arrested in Romania, Serbia and the United Kingdom on European arrest warrants in a covert strike on 8 May.

These arrests coincided with the arrests of 5 suspects in Serbia in a parallel investigation following several months of joint operational work between the countries involved, coordinated by Europol, to identify the key facilitators in the Western-Balkan region.

International police cooperation was central to the success of this investigation, initiated by the Munich regional office of the German Bundespolizei, as it soon became clear that the facilitators were using several identities and rapidly changing their place of residence to evade justice. For example, one of the suspects located in Serbia was arrested on the basis of Romanian forensic data on a German arrest warrant. The United Kingdom also arrested a suspect using a different identity when crossing from France to the United Kingdom. With the help of Europol, which allowed for the timely sharing of information cross-border, the involved countries were able to identify the suspects, and subsequently arrest the criminals sending lorries with hundreds of migrants to Germany.

Toll Fraud - How Criminal Network Made Fortune Through Fraudulent Use of Counterfeit Fuel and Credit Cards

24 suspects have been arrested in Spain by the Spanish National Police and the Guardia Civil in an international operation involving Spain and France and supported by Europol. The organised crime group was specialised in using counterfeiting fuel and credit/debit cards to avoid paying toll fees and in selling these cards to truck drivers and hauling companies.

Over the course of the three months of action of operation ANDREA, fuel card companies and one card scheme reported approximately 30 000 fraudulent transactions linked to counterfeit cards used to cross toll barriers in Spain and France. Law enforcement agencies then initiated investigations, on the basis of the information obtained, to identify the license plates of the involved vehicles, of which more than 600 were located in Spain only.

The investigation initiated by Spain allowed the identification of the criminal group operating mainly in the Spanish region of Catalonia, although the cards were also used on French highways. As a result of the cooperation between Europol, the Fuel Industry Card Fraud Intelligence Bureau (FICFIB), the Spanish authorities and the French Gendarmerie, 24 people were arrested and 11 fraud cards factories were dismantled.

Successful Counter-Terrorism Operation in Tenerife

The Spanish National Police has arrested three men of Moroccan nationality in San Isidro, Tenerife suspected of recruiting and financing terrorism. The three arrestees, respectively 27, 35 and 37 years old, were facilitating the trip to Syria of a jihadist in order to join the terrorist group Al Nusra. Al Nusra is a Salafist jihadist organisation fighting in the Syrian Civil War, with the aim of establishing an Islamic state in the country.

The alleged jihadist, a 35 year-old Moroccan national, was recruited and radicalised by the three arrestees, and eventually left for Syria in 2013. In 2015 the man returned to Tenerife, with severe battlefield injuries.

EUROPOL

People smugglers identified during INTERPOL border security operation

Suspected people smugglers were identified during an INTERPOL-led border security operation in South Asia.

Operation Mandala took place at five international airports and one land border point in Bangladesh, Bhutan, Myanmar, Nepal and Sri Lanka. Nearly 500,000 individuals were screened against INTERPOL's nominal and Stolen Lost Travel Document (SLTD) databases during the operation.

This resulted in multiple positive 'hits', including individuals subject to INTERPOL Red and Blue Notices and several travel documents registered in the SLTD database.

Among the hits were two individuals suspected of involvement in human trafficking and people smuggling activities in the region, and a Sri Lankan national who was the subject of a Red Notice from the UAE for misappropriation of funds.

"The operation has helped enhance the efficiency of immigration officers in Bangladesh in screening travel documents and following up on potential hits," said Mahbubur Rahman, Deputy Inspector General for Operations and Head of the National Central Bureau in Dhaka.

"We appreciate the support of INTERPOL in securing our country's borders and will be extending this application to additional border points in the future," he added.

Operation Mandala was held as part of INTERPOL's Project Relay, a Canadian-funded initiative to enhance migrant smuggling capabilities in South Asia through training, improving systems and providing technical equipment..

Tackling human trafficking focus of INTERPOL training for Central Asia

An INTERPOL training course targeting human trafficking and migrant smuggling across Central Asia has concluded in the Uzbek capital.

The five-day event brought together law enforcement experts from 14 Central Asian countries to learn the latest investigative skills required to coordinate transnational responses to the region's trafficking and smuggling challenge.

With illegal migration into Central Asia becoming an increasingly serious security threat in the region, improving the exchange of police information and boosting the use of tailored INTERPOL capabilities was central to the training programme.

Protecting cultural heritage across the Americas

Over the past decade, law enforcement agencies worldwide have seen a marked increase in the illicit trafficking of cultural objects.

With this in mind, some 100 international experts from 11 countries across the Americas have gathered to devise a common strategy against the organized crime groups which are constantly looking to increase profits from this lucrative trade.

The three-day (17 – 19 April) Americas Conference on Illicit Trafficking in Stolen Cultural Property, organized by INTERPOL in close collaboration with Argentina's Federal Police and Ministry of Security, aimed to boost the exchange of information and best practice in the region.

The event highlighted the need for increased cooperation between law enforcement agencies and international organizations and featured presentations from UNESCO, ICOM and the United Nations Security Council (UNSC) Monitoring Team linked to resolutions concerning ISIL, Al-Qaida and the Taliban.

Specialized anti-trafficking training course for regional branches of police in Uzbekistan held in Urgench with OSCE support

The first in a series of training courses on anti-trafficking for investigators and operative agents of Uzbekistan police forces was held in Urgench.

The course, organized by the OSCE Project Co-ordinator in Uzbekistan, brought together 25 participants from Khorezm, Bukhara and Navoiy regions, and the autonomous Republic of Karakalpakstan.

The training's objective was to increase knowledge and develop police skills and attitudes to identify victims of human trafficking and labour exploitation and refer them to the appropriate assistance.

Management of Contemporary Security Systems focus of OSCE seminar in Podgorica

The OSCE Mission to Montenegro and the Police Academy of Montenegro held a three-day seminar on the management of contemporary security systems, police leadership qualities, in Podgorica.

The Contemporary Security Management course is designed to provide relevant training on modern-day practices to run a security department efficiently and effectively. It addresses vital themes such as leadership in management, employee relations, risk management, terrorism, information security, access control, investigations, substance abuse, workplace violence, and emergency management..

Combating destruction of cultural heritage and trafficking in cultural property in Central Asian Region

Practical measures to combat illicit cross-border trafficking in cultural property in the Central Asian Region was the focus of a five-day regional workshop in Tashkent.

Organized by the Border Security and Management Unit of the OSCE Transnational Threats Department, with the support of Italy, which is chairing the OSCE in 2018, and the OSCE Project Co-ordinator in Uzbekistan, the workshop was attended by 18 participants from relevant law enforcement services and ministries of culture of all five Central Asian participating States.

"In recent years we have experienced a dramatic upsurge in the destruction and degradation of archaeological sites and in trafficking of cultural property in the OSCE area and beyond," said Deputy Permanent Representative of Italy to the OSCE, Luca Fratini. "It has become evident that this kind of trafficking is deeply linked to transnational organized crime and corruption networks and the financing of terrorism. Combating the destruction of cultural heritage and trafficking in cultural property is a priority of Italy which is currently chairing the OSCE"

OSCE

Organization for Security and Co-operation in Europe

UN Migration Agency, DR Congo Government Enhance Ebola Screenings at Border-crossings

IOM is supporting the deployment of teams of epidemiologists and medical staff from the Ministry of Health and the National Programme of Hygiene at Borders (PNHF) in Kinshasa to 16 points of entry along the Democratic Republic of the Congo's (DRC) borders. This deployment is part of an effort to prevent and control the outbreak of Ebola in the DRC, supporting the World Health Organization (WHO).

The DRC Ministry of Health, which is leading the response, announced an outbreak in the Equateur Province on 8 May. In recent days, Ebola cases have been confirmed in larger urban areas, making the risk of the disease spreading further even greater, due to heavier density of population and higher population mobility.

The essential deployment of these border health officials was made possible through USD 75,000 reallocation of funds from the Government of Japan and a release of internal emergency funds totalling USD 100,000. Border health officials will set up infection prevention and control measures at priority border crossings, travel routes and congregation points..

Over 700 Ghanaian Migrants Return Home with IOM Assistance

IOM in partnership with the Government of Ghana and the Airport Authorities, facilitated the return home of 148 Ghanaians via charter from Libya. The group, which included four women and two children, arrived at Kotoka International Airport in Accra in what was the fourth charter flight organized by IOM through the EU-IOM Joint Initiative for Migrant Protection and Reintegration.

So far since June 2017, a total of 706 (661 men, 45 women) Ghanaians stranded in Libya have been assisted to return home voluntarily. The majority (70 per cent) of the returnees are being returned from various detention centres in Libya, while the rest are from the cities.

Support Belize Develop New Migration Policy

The Government of Belize and IOM, the UN Migration Agency, jointly held the launch of a National Migration and Development Policy for Belize this week (16/05).

The development of the national policy will be led by the Government of Belize through a Steering Committee chaired by the Department of Immigration and Nationality Services. In developing the policy, the Government of Belize requested technical assistance from IOM in 2016; a steering committee was formulated in 2017 to work on drafting the policy framework and to ensure that the policy is aligned with the Government's development strategy and national vision.

The latest data indicate that emigrants as a percentage of the Belizean population stand at 15 per cent, with the United States as the primary destination; while immigrants represent 15.3 per cent of the total population in the country, coming mainly from Central America.

INTERNATIONAL ORGANIZATION FOR MIGRATION
IOM·OIM
THE UNITED NATIONS MIGRATION AGENCY

BORDER SECURITY REPORT

ATAK SITUATIONAL AWARENESS ARRIVES AT THE BORDER

US CBP leads the way in combining USSOCOM software and consumer communications hardware to greatly increase agent safety and effectiveness in austere environments
Keywords: ATAK, Android Tactical Assault Kit, goTenna, situational awareness.

Border security is a dangerous law enforcement mission. Frequently executed in remote and austere environments, border agents have to contend with rough terrain, extreme remoteness from external support, and the very real risk of life threatening situations.

In these environments agents must depend on the support and operational intelligence provided by their team on the ground, however the very nature of where they are operating makes this very difficult due to the lack of effective communications systems. Tasked with protecting vast expanses of land that are more often than not completely devoid of any traditional communications networks, establishing communications across agents is of utmost importance.

In the ongoing challenge to increase border agent security and operational effectiveness in the field, the US Customs and Border Protection Agency (CBP) has turned to a toolkit directly sourced from Special Operations community – the Android Tactical Assault Kit (ATAK). First fielded in 2010 during operations in Afghanistan and Iraq, USSOCOM's ATAK platform has become the de facto situational awareness and

command/control battlespace management tool for not only SOF operators, but conventional military, and now civilian law enforcement as well.

Although the name and pedigree may make the system sound like a tool solely suited for war, the ATAK platform is actually much less scary and aggressive than it may appear when looking at its name (likely why the civilian version is more often called the Android Team Awareness Kit). ATAK can perhaps be best described as a combination of Google Maps with What'sApp.

Now this is definitely a simplification of the capabilities within ATAK, but roughly speaking this is accurate. The ATAK system is an Android application which displays map data and, more importantly, allows its users to communicate critical situational awareness data in a live, dynamic, and user friendly interface over that map data.

Although the diversity of tools within ATAK are way too numerous to list out, at its core the platform is used to communicate 3 simple, but critical, types of information to its users:

First and foremost, there is blue force tracking. ATAK displays all users on its map allowing teams to have rapid visual confirmation of their position and the position of their teammates. In the rough and vast expanses covered by border security agents, the ability to know one's location as well as the location of their team is of utmost importance – not unlike a SOF team assaulting a target in a military operation.

Secondly, ATAK allows its users to quickly create markers and waypoints and other points of interest for their entire team. This could be something as simple as a rally point to help gather a team after a dispersed operation, or something more critical like marking a possible hostile actor in a hidden position. Once again, although SOF teams might use this tool for marking snipers and IEDs, something border agents hopefully do not have to encounter on a regular basis, at its core, the utility function is the same. Perhaps a border team uses the tool to mark hidden groups of people or rally or observation points, but the use case is functionally the same.

Finally ATAK is also used to communicate commands back and forth via a straightforward chat messaging tool which helps coordinate actions around the geospatial markers that team members are creating for their squads.

Although this may sound like an incredibly simple set of features, things we take for granted almost every day with our Google Maps and What'sApp, ATAK is a game changer for these field operators for a few reasons.

Firstly, it offers significantly more advanced map data, marker accuracy, and other tools that are necessary when the task at hand isn't finding your friend on a street corner, but possibly coordinating actions which could result in life or death consequences. It is difficult to describe the gamut of features in ATAK that make it so much more than the commercial tools we see every day, but its quick uptake across the US DoD, NATO partners, FBI, Secret Service, CBP and many more attest to its criticality.

However what is perhaps the clearest differentiator of ATAK (aside from its commercial availability, ease of use, and stability) is that unlike the Google and other commercial tools, it is capable of operating in completely disconnected environments. Although ATAK does have a server-based system, it is also natively integrated with the latest off-grid communications tools that allow tactical operators to continue to use these situational awareness features in places where they would traditionally expect to be completely disconnected – remote and hostile locations - exactly where border agents need to operate.

But as valuable as this ability to

operate off-grid and without a server is, it is also one of the most difficult capabilities to practically field.

Simply put, although ATAK can work off-line with radios, the reality is that traditional tactical radios are astronomically expensive. Costing on average over $15,000 per unit, a digital tactical radio link, until recently, has remained a capability only accessible to the most well funded of tier-1 SOF teams. CBP and many others knew and trusted the capability of ATAK, but they simply couldn't afford the kind of investment needed to meaningfully equip their agents in a way where they could trust and rely on the system. Although some tests had been run using ATAK on regular cellular connection, the reality was that the remote and austere nature of border operations necessitated an answer to the off-grid problem before ATAK or any other such platform could ever be realistically operationally integrated.

This all changed recently however with the introduction of a new player in the tactical radio space, goTenna. A small Brooklyn-based startup that originally focused on the recreational hiking and skiing market, goTenna started creating miniaturized radios for consumers to pair with their smartphones to allow them to text and track each other's locations offline while doing off-grid sports.

What made goTenna radios unique was that they did not attempt to provide broadband data communications like other legacy systems. Instead, they focused solely on providing short-form burst data transmissions, sufficient for locations, markers, shapes, and text – but no more, no less. What goTenna got in return for its conservative approach to features was the creation of a family of radio systems that can be best described as very practical and accessible. A humble set of descriptors, but extremely meaningful.

Although conservative in features, these radios provided the core of what was needed – situational awareness - and provided it at a radically lower size, weight, power, and cost than anything else around - $499 to give it a number.

These practical advantages quickly caught the eye of DARPA and SOCOM who realized that the small bursts of data supported by the little consumer radio systems could successfully support the core functions within the ATAK platform. It couldn't support everything feature within ATAK, but it supported the most important components of personnel tracking, map marking, and text. This led to a quick integration between the goTenna radios and ATAK which soon saw the systems deployed with SOF teams in combat in locations as extensive as Iraq, Afghanistan, Niger, and more – primarily as a tool to enable local partner forces to interoperate with coalition forces who could not provide them with their restricted and expensive radio systems.

As unique as SOF operations might be in their fine details, taking a macro perspective shows that their requirements are little different than that of a border security team, or even a crew of wildland firefighters. Everyone needs to know where they are, where their team is, the dangers/objectives, and issue commands to address those objectives. Its pretty simple, but its what is needed.

What has resulted from this similarity in mission requirements is that SOCOM software, consumer smartphones, and a radio system originally designed for hiking have suddenly come together to

create a practically accessible and operationally relevant situational awareness and command/control system which can be had for just a few hundred dollars per agent – not tens of thousands.

This is a game changer, and many outside of the military have taken notice.

Seeing an opportunity to really move the needle in operational capabilities, in late 2017 CBP purchased roughly 1200 goTenna radios for a price tag that didn't break $1MM. CBP was able to follow the lead of SOCOM's foreign operations to equip over a 20th of its border force for a cost that barely registered a blip on its budget.

CBP's creative efforts at enhancing agent situational awareness in austere environments have drawn the attention and support of its parent agency in the US, the Department of Homeland Security (DHS), which kicked off an APEX operational evaluation program specifically designed to officially review the power of the ATAK platform, and its supporting systems, for broader deployment across the breadth of US security forces.

As smartphones, goTenna, and ATAK are all EAR99 non-controlled systems – this is a capability architecture which any border security agency around the world should carefully look into.

East African Customs will work together to enhance border control through PGS

Under the auspices of the WCO/JICA (Japan International Cooperation Agency) Joint Project, to support trade facilitation and border control in Africa, a Sub- Regional Awareness Raising Seminar on Programme Global Shield (PGS) in East Africa was held in Nairobi, Kenya, from 15 to 17 May 2018. This is the first activity of the enhanced border control component of the new Trade Facilitation and Border Control project launched by the 5 Revenue Authorities in East Africa.

Programme Global Shield is a multilateral WCO initiative, which aims at building the capacity of customs administrations to counter the illicit trafficking and diversion of chemicals and other components used by terrorists to manufacture improvised explosive devices (IEDs). The Seminar aimed at raising awareness amongst East African Customs of the threat posed by IEDs and demonstrating ways how customs can contribute to mitigating the threat. It also provided a platform for participants from East Africa to share their experiences, exchange and discuss best practices.

Twenty (20) Customs officials from Burundi, Kenya, Rwanda, Tanzania, and Uganda in addition to five (5) observers from Kenya Revenue Authority participated in this seminar. Each Customs administration shared its country presentation that included their efforts in strengthening customs control at the borders, the level of cooperation between Customs and other law enforcement agencies, and how they deal with explosive precursor chemicals and other components used to manufacture IEDs.

During the seminar, the WCO experts provided updates on the WCO Security Project's initiatives and shared information about Customs role in border security, technology deployment, and operational activities. The Joint Improvised-Threat Defeat Organization's briefing set the scene in relation to the global harm and regional perspective of IED use; while Japan Customs expert explained how advanced technologies can help Customs to efficiently identify chemicals.

Visit of President of AMERIPOL to EUROPOL

The President of AMERIPOL, carried out a visit of knowledge and coordination with the Executive Director of EUROPOL, Rob Wainwright. Also participating in the visit was the Director of Horizontal Operational Services, Mrs. Julia VIEDMA and the Security Analyst and Head of Corporate Institutional Affairs of the European Union (G21) Ms. María ESPEGEL BETEGON.

In his current role as President of the Community of Police of America, at the hearing, the President spoke about the need to have a greater participation and proactive impact of the members of the American Organization, in the fields related to the exchange of information, training programs existing and sponsored by the European Union, the possibility of opening new field offices of the European Agency in different police forces of our continent.

Government of Ecuador Awarded by Commissioner General

The Government of the President of the Republic of Ecuador, Lenín Moreno Garcés, awarded the Badge of Police Merit award to the Commissioner General of the Federal Police, Manelich Castilla Craviotto, as a recognition of his effort to promote coordination to prevent transnational crimes between authorities of the American continent.

Ambassador Arizaga Schmegel highlighted the exchange of information between authorities of different nations, to prevent and deal with global crimes such as human trafficking, drug trafficking or cybercrime; along with the formation of high-level commanders among the police of the continent, achievements reached by the Commissioner General of the Federal Police, during his tenure as President of the Community of Police of America (AMERIPOL).

Gendarmeria Nacional Argentina Seize Total of 389 Kilos of Cocaine

Through a judicial investigation, a criminal organization was formed, made up of citizens of Russian nationality and naturalized Russians from Argentina, who collected and then transported cocaine hydrochloride in diplomatic pouches to Russia. From the field tasks and the analysis of the information, a controlled delivery of the narcotic substance was achieved, which was replaced by flour, destined for Moscow. Through international collaboration with the federal service of a fluid exchange of information achieving Russian security, the gendarmerie investigators maintained the detention of six (6) citizens of Russian nationality.

ASEANAPOL Receives working visit from delegates from the Ministry of Public Security (MPS) of China

The ASEANAPOL Secretariat received a working visit from delegates from the Ministry of Public Security (MPS) of China led by Guoli Jiang, the Deputy Director General of Criminal Investigation Department of MPS and his two officers. They were warmly welcomed by the Executive Director (ED) of ASEANAPOL Secretariat, Police Colonel Kenechanh Phommachack, Directors and staffs.

Soon after the ED gave his welcoming remarks, Guoli Jiang expressed that MPS of China regards ASEANAPOL a crucial counterpart in the region to combat transnational crime. He then conveyed his presentation on "Organised Transnational Telecom Fraudulent Crimes" which had clocked 610,000 cases filed in 2016 and incur RMB 17 billion loss in China itself.

In his presentation, Guoli shared the current crime situation and trends; modus operandi of the crime; their success stories in Europe and ASEAN; problem and difficulties faced by the operation team; and later their proposal for further collaboration.

After much discussion between the MPS delegates and ASEANAPOL Secretariat, both parties agreed to the need for collaboration to fight against such transnational crime in order to keep both region safe. The MPS of China will submit their proposal of "Joint Operation and Mutual Legal Assistance in Combating Organised Transnational Telecom and Internet Fraudulent Crimes" to the secretariat for detailed discussion.

INTERPOL Capacity Building and Training Directorate

A delegation of officers from the Interpol Capacity Building and Training Directorates, based in Interpol Global Complex of Innovation (IGCI), made a courtesy call to the ASEANAPOL Secretariat office. Executive Director, Police Colonel Kenechanh Phommachack together with the staff warmly recieved the delegation.

During the meeting the delegate from Interpol Capacity Building and Training Directorates shared briefly on their respective roles and functions which mainly focus on capacity building, databases collection and operational activities that are on project basis. The delegate had also shared that they had understood through their visiting around the region that there was a keen interest in the forensic development as such they offered their assistance in helping ASEANAPOL Forensic Science Network (APFSN) committee in their development on area such as the Disaster Victim Indentification (DVI) and Crime Scene Investigation (CSI). Executive Director, Police Colonel Kenechanh Phommachack extended the appreciation for the support from Interpol delegate and he hopes for the success on this cooperation in the future to come.

AGENCY NEWS AND UPDATES

Migrants must be 'repelled at border' if refugee centers plan fails

Germany must start turning potential asylum seekers back at its borders if a new refugee centers initiative championed by federal authorities fails to work as planned, the Bavarian Interior Ministry head said.

"Uncontrolled immigration has already fundamentally changed not only the political architecture but also the security situation in Germany in 2015. That should not happen again," Markus Soeder, the Bavarian interior minister and a member of the Christian Social Union (CSU), told the Bild daily.

If the new initiative – which is aimed at the creation of large refugee centers to house all potential asylum seekers while their applications are being processed – ultimately fails, Soeder believes Germany must resort to more drastic measures.

Migrants Transferred In Bosnia After Hours-Long Standoff

Buses carrying 270 refugees and migrants from Sarajevo reached an asylum center in southern Bosnia-Herzegovina after an hours-long standoff between regional and national authorities in the multiethnic Balkan state.

More than 4,000 migrants have entered Bosnia this year after traffickers opened a route through Greece to Western Europe via Albania, Montenegro, Bosnia, and Croatia.

The migrants had been staying in an improvised camp in a park in Sarajevo, but authorities ordered them to be moved to a refugee center in Salakovac, near Mostar, some 100 kilometers south of the Bosnian capital.

Hundreds of migrants, mainly from Syria, Iraq, Afghanistan, Turkey, and North Africa, had camped in the park for nearly two months.

Guarding EU external border is cornerstone of migration policy

Guarding the external borders of the European Union is the cornerstone of migration policy and Frontex plays a key role in that, Estonian President Kersti Kaljulaid said on Friday when visiting the European Border and Coast Guard Agency (Frontex) in Greece.

"Estonia values highly the work of Frontex in boosting the security of the EU's external border and we have sent our people and equipment to help with that," Kaljulaid said.

Considering the size of its population, Estonia is the biggest contributor to Frontex with officials of the Police and Border Guard Board (PPA) as well as border guarding equipment, but the country is always open to consider doing more.

Border guards detain Russian over 'information war' on Poland

Border guards have detained a woman suspected of helping wage a Russian "information war" against Poland and who has a ban on entering the country, according to a report.

The woman, who is a citizen of Russia and Cyprus, is to be expelled from Poland, public broadcaster Polish Radio's IAR news agency reported on Friday.

The woman, named only as "Anastazja Z", worked to consolidate pro-Russian groups in Poland in order to challenge Polish government policy on historical issues and "replace it with a Russian narrative," according to IAR.

Colombia and Ecuador Increase Counter-terrorism Operations along Border

The killing of three journalists from the Ecuadorean daily newspaper El Comercio on April 13, 2018 at the Colombian border spurred authorities from both countries to take combined measures to strengthen security and guarantee the safety of the area. Dissident members of the Revolutionary Armed Forces of Colombia (FARC, in Spanish), whose leader goes by the alias Guacho, kidnapped the journalists three weeks earlier in Mataje parish, in the Ecuadorean province of Esmeraldas.

The countries' ministers of defense and military high command held a special meeting of the Binational Border Commission on April 17th in Quito, Ecuador. The meeting was called under the cooperation mechanism known as 3+2, which provides grounds for meetings between the two nations' Foreign Relations, Defense, and Interior ministries.

The authorities agreed to an increase in military and police operations, with 24-hour operations in Esmeraldas province and in Tumaco, Colombia.

Far-right groups, counter-protesters rally over asylum seekers at Canada-U.S. border

So far this year, more than 7,600 asylum seekers have crossed into Canada at unofficial ports of entry, the vast majority of them at Roxham Road, which is a short drive from Lacolle.

Officials expect that number to jump in the coming months — outstripping the nearly 20,000 who crossed last year in Quebec — and are putting resources in place to accommodate the influx.

The RCMP recently erected a semi-permanent structure at Roxham Road, where they process and screen asylum seekers. The Quebec government is also pressuring Ottawa to send more of the claimants elsewhere after they are processed.

With Focus On Mexican Border, Greater Security Threat Could Be From Canada

Competing versions of what constitutes a safe southern border with Mexico are at the center of a debate echoing from Mexico City to Washington, D.C. — and especially in the four border states of California, Arizona, New Mexico and Texas. And citing national security, President Donald Trump recently signed an order to deploy the National Guard on the southern border, adding to an already substantial presence of personnel and technology there.

However, some argue that when it comes to the potential for terrorism, the security focus should be applied equally to the Canada-U.S. border.

There are about 16,000 border patrol agents on the Mexican border. There are about 2,000 agents on the

Canadian border, which is twice as long as Mexico's. The U.S. Attorney for the District of Vermont, Christina Nolan, says she's concerned about the northern border..

Eight Israeli Bedouin Arrested for Drug Smuggling Over Egypt Border

Eight Israeli Bedouin have been arrested — and some are being charged with espionage —for allegedly vandalizing security cameras along the Egyptian border last month in a drug smuggling operation, police and the Shin Bet security service announced.

An Israel Defense Forces tank driver, Sgt. Eliyahu Drori, was killed in April in an attempt to catch the suspects now under arrest. While pursuing them near the Egyptian border, his tank rolled down a ravine, causing a shell inside the vehicle to ignite. Three other soldiers were injured in the incident.

The eight suspects, residents of the Bedouin community of Bir Hadaj in the northern Negev, were charged in Be'er Sheva District Court; some of them, with espionage.

Three arrested on charges of smuggling arms, drugs from Pakistan

In a joint operation, the Border Security Force, the intelligence unit of Rajasthan

police and the Sriganganagar police arrested three people from Punjab'sTarantaran district for their alleged involvement in smuggling in the border area.

The accused have been identified as Jasvindra Singh alias Sonu, Jagraj Singh alias Billa and Ratanbeer Singh alias Ratan. The joint team also recovered two sophisticated pistols and two cartridges.

SP Harendra Mahavar said the team was working on some input and following the leads the arrests were made.

Myanmar orders Rohingya to leave tense border zone

Myanmar security forces have resumed loudspeaker broadcasts near its border with Bangladesh ordering Rohingya Muslims to immediately leave a strip of no-man's land between the two countries.

Around 6,000 refugees from the persecuted minority have been camping on the narrow stretch of land since fleeing a brutal military crackdown in Myanmar's west last August.

The majority of the nearly 700,000 Rohingya who escaped the violence settled in huge camps in Bangladesh but a smaller number insisted on staying put in the buffer zone between the borders.

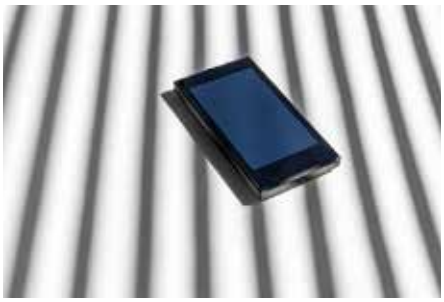
Myanmar had agreed in February to stop using loudspeakers to order the stranded Muslims to leave the area immediately and cross into Bangladesh.

Pakistan Rangers make truce with BSF after facing heavy retaliation

Pakistani Rangers were forced to broker peace after Border Security Forces pounded their bunkers and other installations across the International Border (IB) in retaliation to prolonged shelling in Jammu and Kashmir to push infiltration of militants. The unprovoked firing was also to undermine the central government suspending operations to reach out to people of Jammu and Kashmir during the ongoing Ramzan.

A senior BSF officer, aware of developments in Kashmir, told ET that two Rangers and 6 civilians were reported by the Pakistani media to have died due to our targeted heavy fire and 26 were injured. The Rangers called up the BSF unit in Jammu Saturday and urged our troops to stop firing, said sources in the paramilitary force.

Border Police find 6 phones in smuggler's body intended for jail



Israeli Border Police officers arrested an Arab attempting to cross the security fence in the Jerusalem area for the second time. Only minutes before he was jailed in Ofer Prison six cell phones were removed from his body that were allegedly intended to be smuggled to security prisoners.

Last Tuesday evening, a Nitzan Brigade forward observer spotted a suspect climbing the security fence in the a-Ram area as he tried to cross into Israel illegally. A team of Border Police officers directed to the site located the suspect who was arrested and transferred for interrogation, after which he was released and returned to Judea and Samaria.

Last night the observer again identified the suspect trying to pass over the security fence in an attempt to infiltrate into Israel illegally, and once again a Border Police team was able to locate and arrest the suspect.

National Guard & Border Patrol Team Up to Uncover Hidden Meth

U.S. Border Patrol (USBP) agents in San Diego Sector arrested a 31-year-old woman on Interstate 15 for transporting 51 bundles of methamphetamine inside her vehicle.

She was turned over to Riverside County law enforcement and now faces narcotic smuggling charges.

The woman's vehicle was seized and transported to a secure facility. The vehicle underwent a routine secondary search to ensure there was no additional contraband inside the vehicle. As a part of the secondary search, and with the aid of a recently assigned National Guardsman, Border Patrol agents conducted a thorough visual and physical inspection. During the search of the vehicle, a National Guardsman located 11 additional bundles of suspected contraband that was deeply concealed within the door panels of the vehicle. Border Patrol agents took custody of the bundles, it was field tested and was positively validated as methamphetamine.

The bundles added more than 13 pounds of methamphetamine to the seizure, which now totaled over 68 pounds with an estimated value of $206,000. The National Guardsmen are not assigned to do immigration tasks, will not have direct contact with illegal aliens, nor will they carry weapons.

Study of Indonesia-PNG Border Security

The field of international relations and security studies is among the most dynamic and challenging aspects of politics. Relationship between states depend on various factors such as politics, economic cooperation and socio-cultural partnerships. Despite the growing interdependency between states through the means of bilateral, multilateral or regionalism, security issues have remained to play a vital role in determining their level of cooperation and coexistence. This qualitative research entitled: Indonesia-PNG Border security, underlines Indonesia and PNG's foreign policy while addressing the impacts of Papuan separatism on the 750km border. The relationship of Indonesia and PNG has remained cordial and robust over the years, however the existence of the Papuan conflict has often threatened to destabilize mutual understandings between the parties.

The findings specify that the issue of Papuan separatism is one the sensitive and complicated political and cultural problems of the modern era. The sensitivity that lies behind the Papuan separatism issue has often caused difficulties to Indonesia and PNG policy makers. Border policies are designed to obtain the state objectives; however, cultural aspects have always benefited the third party (OPM) in their existence along the border. Subsequently, the Papuan autonomy has allowed for the acknowledgment of Papuan's cultural rights. Moreover, the Papuan separatism has managed to gain support from many external parties. The growing participation of external parties have triggered internal security concern. This study indicates that the Papuan separatism issue will

remain to influence Indonesia-PNG border security in the years to come. The designing of border policies should focus and encourage more on building trust as means of overcoming misunderstanding. More cooperation between all relative authorities such as the CIQS is vital to maintain a good and favorable a relationship.

Thai troops seize record meth haul on Myanmar border

Thai soldiers have seized a massive haul of methamphetamine in Chiang Rai Province in northern Thailand smuggled through the Thai-Myanmar border.

An official from the border task force confirmed that the drug haul was seized late Friday while the soldiers were inspecting vehicles at a checkpoint on the road between Doi Luang and Wiang Chiang Rung districts in Chiang Rai.

The official said the suspect tried to drive away after seeing Thai troopers manning a checkpoint but the vehicle fell into a ditch.

“The ditch was only 350 metres from the checkpoint. A total 7.8 million methamphetamine pills and 50 kilos of ‘ice’ or crystal methamphetamine have been seized,” he said.

During a news conference in Chiang Rai a day later, Thai military officials said the soldiers found 39 fertilizer sacks containing 7.8 million methamphetamine pills and 50 kilos of ‘ice’ or crystal methamphetamine inside the vehicle.

Man allegedly involved in shooting tasered by Border Patrol

Border Patrol agents responded to a call for assistance from the police department to help find someone involved in an apparent shooting.

Agents say they were able to find the vehicle in question and attempted to conduct a traffic stop.

The driver then stopped in the middle of the road, got out of the car and began to approach the agents.

Border Patrol says the suspect ignored agent’s commands and resisted being taken into custody. After a struggle, agents used a taser on the man.

Police, border cops hunt Commonwealth Games overstayers

State police forces will work with Border Force officials to try and track 50 people believed to be in hiding after overstaying their Commonwealth Games visas.

Border Force officers have teamed up with state police to hunt 50 people in hiding after overstaying visas they were given to attend the Commonwealth Games.

Home Affairs Minister Peter Dutton says officers have launched an operation to find the athletes and officials who disappeared after the Gold Coast event last month.

About 250 people who came for the event remain in Australia.

Border force officials defend dawn raid on Sri Lankan asylum seekers

Australian Border Force officials have defended taking a Sri Lankan family from their central Queensland home and placing them in immigration detention 1,800km away.

Tamils Priya and Nadesalingam and their two Australian-born children were swept up in a dawn raid of their Biloela home in early March. The couple are in detention in Melbourne with their two girls, three-year-old Kopika and baby Tharunicaa, as they await a decision on whether they will be deported.

The ABF commissioner, Michael Outram, was quizzed about the case during a Senate estimates hearing in Canberra.

TRANSFORMING PASSENGER PROCESSING

SITA report outlines how biometrics in identity management will transform passenger processing.

Biometric technology is emerging as the top solution for airlines and airports to automate identity checks amid rising passenger numbers. This is according to Biometrics for Better Travel: An ID Management Revolution, a report published today by SITA. It outlines how using biometrics to check passenger's identity will power faster and more secure self-service processes at airports as passenger numbers are set to almost double to 7.8 billion by 2036.

Airlines and airports are already investing in various forms of biometric technology and SITA's report explores innovative ID management programs that are transforming the travel experience today. In the future, these will be more commonplace worldwide as 63% of airports and 43% of airlines plan to invest in biometric ID management solutions in the next three years.

Sean Farrell, Director, Strategy & Innovation, SITA, said: "Across the world, airlines are required to check that passengers are who they say they are and that they have the right travel documents. This is a fundamental

element of securing the travel process which cannot be eliminated. With passenger numbers set to double by 2036, airlines and airports need to be able to move passengers through these checks as securely and quickly as possible. Efficient identity management is essential for better security while at the same time improving the passenger experience. Biometrics is the technology that can deliver this."

The good news for airlines, airports and the various government agencies involved in passenger identity management, is that passengers are happy to use biometrics. This technology is becoming increasingly commonplace in people's lives. For example, by 2020 more than 75% of smartphones will have fingerprint sensors. This user acceptance can be seen among passengers too. SITA reports that the majority of passengers would definitely use biometrics on their next flight.

Farrell adds: "Passengers are ready and want to use biometrics. The easiest way for airlines and airports to make this happen is to use technology that integrates easily with their existing infrastructure – kiosks, bag drop, automated boarding gates. Moving to single token identity management where passengers can simply use their biometric, such as their face, at every checkpoint on their journey will speed passengers securely through the airport."

SITA's report outlines how airlines and airports must have a global consensus on how to securely resolve passenger identity issues as an integral part of the next generation of self-service systems. All industry stakeholders have a role to play to harness technologies that can make the processes better, faster and more secure. The air transport industry must collaborate across all stakeholders and across the globe with governments to ensure scalability and interoperability across borders.

Biometrics for Better Travel: An ID Management Revolution combines SITA's global research with commentary and cases studies from airports, airlines and global entities that are exploring and adopting biometric technology to transform the passenger experience. Those featured include Brisbane Airport, British Airways, JetBlue and Orlando International Airport along with industry perspectives from the International Airline Travel Association (IATA).

For further details of SITA's full report - Biometrics for Better Travel: An ID Management Revolution see www.sita.aero/id

THE MOST ENGAGING DISCUSSIONS IN BORDER MANAGEMENT

EVENT REVIEW

World Border Security Congress

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

Over 230 delegates from 52 countries participated in the 2018 World Border Security Congress which took place in Madrid, Spain on 20th to 22nd March 2018, for 3 days of great discussions, meetings, workshops and networking for the global border security experts.

The international border security community gathered to discuss the challenges from mass refugee movements across Europe, illegal economic migrants from Africa and Asia, threats from terrorist organisations and movement and return of foreign fighters.

Supported by the **Spanish Ministry of Interior, National Police and Guardia Civil**, support was 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, demonstrating the World Border Security Congress remains the premier multi-jurisdictional global platform where the border protection policy-makers, management and practitioners together with security industry professionals, convene to discuss the international challenges faced in protecting borders.

Many exciting, interesting and informative presentations were given from all parts of the world, giving a truly global perspective on the international challenges being faced.

The delegation enjoyed two great site visits:

- Madrid Barajas International Airport, courtesy of the Spanish National Police; and

- EUROSUR Maritime Coordination Centre, courtesy of the Spnaish Guardia Civil

both giving an insight into the developments, latest technologies and operations that help secure the airports of Spain and the Mediterranean Sea.

Conference Chairman Closing Notes on World Border Security Congress – Madrid 20th-22nd March 2018

An excellent conference which was described by a senior border specialist of one of the 52 nations that were represented as, “a timely and important event focusing on the most challenging issues facing border management internationally”

The welcome session set the scene for the 3-day congress with an initial opening address from the Chairman, John Donlon QPM followed by inputs from the International Organisation for Migration, the Organisation for Security and Co-operation in Europe and the President of the European association of Airport and Seaport Police.

The keynote speakers on day one articulated the importance of Border Management activity internationally and the significant challenges, which Governments, Policy Makers and Law Enforcement Agencies face with increasing pressures in a difficult economic climate.

The task for the event was to explore the major issues that were common to so many nations and seek to share experiences and continue to develop border management resolutions and solutions.

With a global audience from 52 nations and nearly 250 participants the conference was delighted to have received some excellent presentations from a broad range of distinguished and experienced border related experts. Alongside this, and importantly, there were some exceptional discussions and debates teasing out some of the more demanding areas of concern and addressing them from a range of perspectives, both from government and commercial positions.

The congress was very fortunate to have significant support from the Ministry of Interior in Madrid, the Spanish National Police and the Guardia Civil. The event was also most fortunate to have the support of, and speakers from, a wide range of international security organisations who have a focus on and around border management operations. Organisations such as:

OSCE Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

AFRICAN UNION

International Association of CIP Professionals

NS&RC

• Organisation for Security and Cooperation in Europe (OSCE)
• International Organisation for Migration (IOM)
• United Nations Office for Counter Terrorism
• European Association of Airport and Seaport Police (EAASP)
• UK Border Force
• EU Border Assistance Mission in Libya (EUBAM-Libya)
• EUROPOL
• AFRIPOL
• African Union

This was a truly global conference seeking to address global border issues and challenges and one which highlighted the need for continued efforts in developing, national, regional and international; Coordination, Cooperation and Communication.

There was, this year, a great deal of focus on migration pressures and the need for nations borders to be; Ordered – Structured and Safe to assist the enormous amount of migrant movement at a time when the displacement of people is even greater now than any time since the second world war.

As predicted, terrorism continued to be topic of special interest with a number of speakers presenting on the significant challenges that we all face globally and are likely to face for many years to come.

At last year's congress we heard a lot about Drug Smuggling and the international initiatives in place to tackle the issues, but not so much this year. However, we heard a lot more about Human Trafficking, a growing trend which is truly a global concern, with some particularly good references demonstrating how easy it is to miss something if you are not looking for it.

Modern Day Slavery was also a topic of considerable discussion and some figures that were quoted, in terms of the amount of people in slavery, estimated to be 45.8 million really drove home the extent of the issue.

There was some surprise that there was not more focus on Cyber activity and its potential implications for border management information systems but no surprise at all that there was a continuing theme on Information Sharing. Again this year there were some very positive comments from Europol on the progress that has been made in this area over the last 12 months.

A number of presenters spoke of the continuing need for cooperation and coordination and a quote that was used on more than one occasion captured the way forward: "Alone we can only do so much, but together we can do so much more".

The Chair of the congress closed at the end of day 3, thanking the participants for their active participation across a wide range of discussions and linked the fact that all who attended were seeking new ways through new challenges and treating those challenges as opportunities to do things better in the future.

The **2019 World Border Security Congress** will take place in Casablanca, Morocco on 19th-21st March 2019, co-hosted by the Moroccan Ministry of Interior and Directorate General for Migration and Border Surveillance.

Further details can be viewed at **www.world-border-congress.com**.

Silver Sponsor: S2 GLOBAL
Welcome Reception Sponsor: Isdefe
Networking Reception Sponsor: SITA Create success. Together
Lanyard Sponsor: Cellebrite
Sponsor: IATA
Media Partners: BORDER SECURITY REPORT, WORLD SECURITY REPORT, World Security-index.com

Gemalto's Biometric Authentication Technology Aims to Revolutionize Automated Border Control in Colombia

Gemalto and INCOMELEC SAS, a Colombian partner, are transforming the immigration and border crossing in Colombia through biometric iris verification implemented by Migración Colombia, the country's border control agency.

This innovative solution was launched in February with a pilot program at Bogota's El Dorado International Airport. The Automated Border Control (ABC), known locally as "BIOMIG", is benefiting both citizens and border officials. Gemalto's ABC speeds identity authentication and significantly reduces bottlenecks in the immigration process while maintaining strong security control for each traveler.

A growing majority of airport arrivals in Bogota – up to 60% - are Colombian citizens re-entering the country. This often results in long immigration queues, congested waiting areas and travel weary citizens. "BIOMIG" mitigates these challenges while complying with Colombia's stringent border control security requirements.

The solution integrates a highly intuitive iris recognition terminal that allows swift long range iris capture from 35 to 45 centimeters away. This eliminates physical contact with the terminal and improves comfort and ease of use. To use the service, Colombian citizens aged 12 and older only need to visit one of 30 BIOMIG enrollment stations at the airport as they exit the country. In less than one minute, their unique iris scan is securely registered with Colombia's Border Management System (BMS). When re-entering the country, previously enrolled citizens simply enter their national ID number on a touchscreen integrated with an automated door barrier by INCOMELEC, SAS. After a quick glance at the iris reader terminal, identity is validated via a secure digital process and the automatic doors swing open.

VSD System Selected for Middle Eastern Military Border & Maritime Security Programme

Cambridge Pixel's Video Security Display (VSD) system has been selected as part of a military mobile protection programme in the Middle East, integrating multiple sensors (radar and cameras) to provide comprehensive and effective monitoring for a border and maritime security application.

The project involves the supply of forty systems through Cambridge Pixel's Middle Eastern partner - Defense Integrated Solutions Security Systems (DISS). Each system is equipped with multiple sensor interface hardware and the VSD application software for deployment on a mobile platform.

David Johnson, CEO, Cambridge Pixel, said, "We are delighted that our Video Security Display software has been selected for this border and maritime security programme. The software has been designed to address a wide variety of security and monitoring requirements and will provide the end user with a highly flexible and powerful solution."

Blighter Surveillance Systems secure first sale into India for its Blighter B400 series E-scan micro Doppler ground surveillance radars

Blighter Surveillance Systems, a British designer and manufacturer of electronic-scanning (E-scan) radars and surveillance solutions, has secured its first sale into India for its Blighter B400 series E-scan micro Doppler ground surveillance radars.

The contract was awarded by system integrator Tata Power Company Limited (Strategic Engineering Division) following Blighter's success at a radar/sensor trial organised by India's border management organisation in Gwalior in November/ December 2016. The Blighter radars will be deployed by Tata Power during 2018 as part of the Indian Government's Comprehensive Integrated Border Management System (CIBMS).

Crossmatch Receives FBI Certifications for Mobile NOMAD 60 Wireless Fingerprint Reader

Crossmatch, has announced its mobile NOMAD 60 Wireless Reader received the FBI Appendix F and Mobile Identifcation FAP 60 certifications.

Representing the latest in fingerprinting technology,

NOMAD readers utilize a capacitive thin-film transistor sensor for superior outdoor and bright ambient light performance and are not impacted by tattooed or stained fingers. The FAP 60 format facilitates rapid fingerprint collection of non-cooperative subjects and those with large hands, yet stores easily in your pocket.

"The NOMAD 60 Wireless Reader delivers true mobility wrapped with the thoughtful design and reliability that are Crossmatch hallmarks," noted John Hinmon, vice president of marketing. "We offer complete flexibility and mobility during in-field identification and verification applications. Law enforcement, border control and military users are not encumbered by power and communication cords, light sensitivity or hard to use smaller platen formats – those hassles don't exist with NOMAD."

DERMALOG: Market leader for biometric border control "Made in Germany"

More travellers, shorter check-in times and increasing cost pressure – in times of globalization, cross-border traffic is challenging authorities. The biometrics innovation leader DERMALOG offers efficient and secure solutions to these challenges.

DERMALOG Identification Systems GmbH, based in Hamburg, offers state-of-the-art biometric recognition systems to make airport checks and other border controls more secure and more efficient. Biometrics can make an important contribution to significantly speeding up and simplifying passenger handling, for example, by facial or fingerprint recognition.

Twelve states, including Singapore, Malaysia, Maldives, Cambodia, Algeria and Brunei, are already relying on DERMALOG's solutions to monitor their national borders. The company's fingerprint scanners are also in use at German airports and at border crossings in Switzerland and the Netherlands. This makes DERMALOG Europe's leading provider of border control systems.

The core of the DERMALOG solution is a so-called Automated Biometric Identification System (ABIS). The multimodal system cannot only match fingerprints but also additional biometric features such as facial or iris patterns. This makes DERMALOG ABIS much more reliable than solutions that only check one identifier.

Especially for border control at airports, DERMALOG has developed the DERMALOG Self Registration Kiosk and the DERMALOG Gate. Equipped with latest camera and scanner technology, travelers can be checked fully automated. The portfolio is complemented by video surveillance systems with integrated face recognition. If monitoring from the airspace is required, the DERMALOG technology can also be integrated in drones.

A Border Technology Story

In 2015, three students a Bethnal Green Academy with known terrorists connections flew without issue from London to Syria to marry ISIS fighters.

Had the screening process taken into account their online history or Scotland Yard's records, their terrorist plot would have ended in the airport.

Two of these "Jihadi Brides" are still unaccounted for.

While healthy border protection is critical in a global economy, the technology in use at many points of entry is in serious need of an update.

Areas with heavy traffic need a robust identity verification process that checks against more than just a list of names. Online history and police report data provide insight into an individual's profile—and are essential information to modern border screening.

Areas with poor infrastructure or frequent power outages need a mobile, infrastructure-independent screening solution to ensure security and maintaining processing flow.

With 20 years of experience applying AI to human language, Basis Technology is developing a comprehensive, two pronged solution for these modern border security issues.

For high volume points of entry, Basis Technology is developing a modern screening solution that aggregates and checks against everything from Facebook data to police interviews to ensure authorities can follow up on suspicious characters and clear innocent travelers with confidence. Basis Technology has also developed a mobile screening device that can operate entirely independently of power or internet connection, providing authorities with the flexibility needed to deal with less-than-ideal border security situations.

A Unique Solution for Effective Border Control

Situation: Border crossings have been increasing in virtually every country year over year. The US handled nearly 400 Million travelers in 2017, while the UK processed over 300 Million people and Australia process over 40 Million people. To add to the complexity, most countries support hundreds of ports of entry, including air, sea and land.

The typical border enforcement agent has minutes to determine if the person they are admitting into their country is a bad actor, and often it is based on the stamps in their passport and whether they act or look suspicious.

Now imagine a new process: One where you can scan their mobile phone within minutes and based on their digital footprint, determine whether that person(s) should be speaking to an investigative agent. Based on content stored in their phone, Cellbrite can scan images, video, contacts, geo-locations, email, text and application data to help border agents determine if a person has a suspicious digital footprint – all within minutes. The same data analysis is made available to the investigative agent so they can ask formative questions to rapidly determine the threat level.

Teledyne ICM release new range of extra slim and light portable X-ray scanner

Teledyne ICM have released a new range of extra slim and light portable X-ray scanners for the security market. Building on the success of its predecessor the FLATSCAN range, the all-new FLATSCAN XS is a direct response to the evolving portable X-ray market.

Experts in many fields such as EOD, customs and law enforcement agencies are constantly requiring lighter, more compact and ever more mobile X-ray solutions. With the increasing use of EOD robots and the constant weight of 80-lb (36-kg) bomb suits, extra-light equipment is a godsend for many operators.

This new digital panel comes in two distinct sizes. The FLATSCAN30 XS enjoys a detection area of 30 in (76 cm) across, enabling scanning of large objects in one single shot, while the FLATSCAN15 XS is a reduced panel of 15 in (38 cm) - perfectly fit for Teledyne ICM's new backpack solution. Flat panel, generator, and tablet can easily fit into one single backpack, enabling the end user to carry this carbon-based detection equipment with ease and comfort.

Combined with Teledyne ICM's unique constant potential X-ray sources CP120B - CP160B and their reduced focal spot, the new FLATSCAN XS scanners deliver sharp, clear and detailed images of any object at high speed.

In a crowded airport, or at a busy checkpoint, FLATSCAN XS scanners answer the needs of many X-ray professional around the world.

ADVERTISING SALES

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

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

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

Isaac Shalev
(Israel)
E: isaac@itex.co.il
T: +972 (3) 6882929

World Border Security Congress

19th-21st March 2019

Casablanca, Morocco

www.world-border-congress.com

Building Trust and Co-operation through Discussion and Dialogue

Ministere de l'Interieur
&
Directeur de la Migration at de la Surveillance des Frontieres

Call for Papers

Abstract Submittal Deadline - 31st July 2018

Submit your abstract online at www.world-border-congress.com

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

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

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

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

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

We look forward to welcoming you to Casablanca, Morocco on 19th-21st March 2019 for the next gathering of border and migration management professionals.

www.world-border-congress.com

for the international border management and security industry

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

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

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

Sam Baird
(Germany, Austria, Switzerland & Israel)
E: sam@whitehillmedia.com

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

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

Vishal Mehta
(India)
E: vishmeh@gmail.com
T: +91 99 999 85 425

Supported by:

Media Partners: