INCORPORATING BORDER SECURITY REPORT

WORLD SECURITY REPORT

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

JANUARY / FEBRUARY 2019
www.worldsecurity-index.com

WHY FACIAL RECOGNITION ON BODY-WORN CAMERAS WILL NOW TRANSFORM FRONTLINE POLICING

critical infrastructure PROTECTION AND RESILIENCE AMERICAS

May 7th-9th, 2019

Tampa, Florida, USA

A Homeland Security Event

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 Open

Register today and benefit from Early Bird delegate fees

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

SPECIAL DEAL FOR GOVERNMENT AND OWNER/OPERATORS

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.

We must be prepared!

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

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

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

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

Leading the debate for securing Amercia's critical infrastructure

Confirmed speakers include:

- ***Keynote Speaker:*** Brian Harrell, Assistant Secretary for Infrastructure Protection, US Department of Homeland Security (DHS)
- ***Keynote Speaker:*** Commissioner Gladys Brown, Chair, Committee on Critical Infrastructure, National Association of Regulatory Utility Commissioners, Pennsylvania Public Utility Commission
- Chauncia Willis, Emergency Coordinator, City of Tampa
- Jean W. Duncan, P.E., Director. City of Tampa Transportation and. Stormwater Services Department
- Stephanie Jenkins, Cyber Security Analyst Sporting and Critical Infrastructure, Argonne National Laboratory
- Nathaniel Evans, Cyber Operations Analysis and Research Lead, Argonne National Laboratory
- Michael Cotton, National Telecommunications and Information Administration (NTIA), Institute for Telecommunication Science (ITS)
- Jose Sanchez, Deputy Director of Research and Development and Deputy Chief Scientist, US Army Corps of Engineers H
- Deborah Kobza, President, International Association of Certified ISAOs (IACI)
- Jessica Yuzwa, Project Administrator, Franklin County Office of Homeland Security and Regional Communications

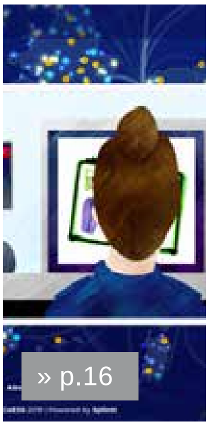
For speaker line-up visit www.ciprna-expo.com

Supporting Organisations:

Media Partners:

CONTENTS

WORLD SECURITY REPORT



ANTI-DRONE SYSTEMS COME OF AGE

For years now, those of us in the security business have been talking about drones; the capabilities they offer and the threats that they pose.

Industry was quick to see the threat and opportunity and a whole new anti-drone industry has developed at a speed that I've not seen in 25 years in the business. But, adoption of these systems was slow.

This is understandable for a number of reasons. Firstly, until December 2018, major incidents that seriously disrupted airport operations were yet to have happened. And actual drone attacks by terrorists were something that only happened in Middle East war zones. The second key factor is that most airports and critical infrastructure sites are in the hands of the private sector, which means decisions relating to major expenditure have to be justified by a clear business case. And last, what technology is the right technology?

Well, the Gatwick and Heathrow incidents have changed all that.

Gatwick's December drone incident disrupted the airport for 33 hours and cost airlines an estimated £50 million ($64.5 million).

The cost and disruption changed the dynamics from a cost justification process to a clear business imperative, resulting in the immediate installation of an anti-drone system.

It would now be a brave or foolhardy airport operator that did not now find the funds and take urgent steps to make their airport secure from drone threats. Indeed, airlines will insist on it.

With 17,678 commercial airports around the world, that's without the tens of thousands of critical infrastructure sites that are also at risk, the anti-drone business really has come of age.

But, for operators the question of 'what technology' to adopt still remains. Many systems have gone for RF disruption or takeover and others propose drone capture as the safest solution. Some even favour birds of prey.

But there are other questions that also need to be answered. Will these systems cope with low level attacks through cluttered environments like neighbouring streets, swarm attacks or pre-programmed autonomous attacks?

Because, what is certain is, terrorists and would-be terrorists are watching and asking themselves the same questions.

Tony Kingham
Editor

READ THE FULL VERSION

The full version of World Security Report is available as a digital download at www.torchmarketing.co.uk/WSR

www.worldsecurity-index.com

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

Assistant Editor:
Neil Walker
E: neilw@torchmarketing.co.uk

Features Editor:
Karen Kingham
E: karen.kingham@knmmedia.com

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

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

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

G4S Global Forecast 2019

As 2019 gets underway, G4S Risk Consulting has produced a guide for businesses seeking to identify and anticipate the myriad of challenges posed by political and operating environments.

The use of technology by hostile actors, citizens, politicians and businesses, each pushing agendas, will risk impacting on reputation, revenue and safety. This gives a platform for persistent issues such as income inequality and cultural conflict to dominate public discourse and be responded to quicker than ever.

Consequently, 2019 will likely see a rise in citizenship – people proactively involved in their national discourse determining the type of future they want – taking to the streets if they feel it will further their cause. In some cases this will bear the emergence of fringe parties but also force governments to listen to competing visions.

At a strategic level, countries are more willing to cite national security as justification for pursuing protectionist policies in trade and diplomacy – notably the US and China. However, much depends on the ability of leaders to convince both competing political stakeholders and a demanding population, that the means justify the end, beyond the short- to medium-term.

Agile corporations will move to adapt to geopolitical changes, placing operations and people where they can continue business as usual and restructure their global supply chains accordingly.

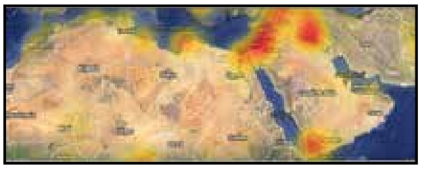
Global Outlook

Shifts in global governance over the past two years have resulted in a leadership vacuum that has seen China, Russia, Iran and Saudi Arabia attempt to capitalise on US withdrawal or disinterest from regions. The post-WWII order appears to be fragile - traditional alliances are waning, treaties are broken, while international groupings such as the G-20 have been rendered impotent by rising nationalism, slowly losing relevance as a talking shop.

With a noticeable decline in international cooperation, domestic priorities are coming to the fore. Populist rhetorics are driving politics in North America and Europe, where EU parliamentary elections could return gains that restrict the EU's legislative process and further nationalist agendas. In the Middle East, governments in Saudi Arabia and the UAE are increasingly assertive both at home and abroad, while Asia, Africa and Central America are experiencing increasing demands for accountability of leaders and an end to corruption.

Competing aims between the US, China and Russia are manifesting in competition in cyberspace, technology, notably artificial intelligence, and arms. Tensions between the US and China are likely across political, security and economic fronts amid a trade war that is gradually opening into a battle for strategic dominance, undermining global growth and security.

Middle East & North Africa



• Clandestine insurgent cells in northern Iraq and south-western Syria have reverted to an asymmetric strategy based on rural extortion and isolated attacks on security forces, as they seek to survive and rebuild.

• The humanitarian situation in Yemen will plausibly deteriorate if the ceasefire breaks down and the Emirati-led offensive resumes against Hodeidah port, on which aid supplies depend.

Improvement Trends

The murder of a journalist by a suspected Saudi government assassination squad in Istanbul has caused deep damage to the reputation of Saudi Arabia's de facto ruler, Crown Prince Mohammed bin Salman. The resulting outcry has alerted international public opinion to the catastrophic humanitarian impact of Yemen's civil war and the Saudi-UAE coalition's role in it, with active US military support. This pressure has created a rift in the US between Congress, which has taken a bipartisan vote towards curtailing the US military role, and the Trump administration, for whom a key driver is supporting the war to continue selling advanced weapons systems to its Gulf allies.

Public pressure has forced the US to put its weight behind a UN-brokered ceasefire deal. The most likely scenario for material change in the course of the conflict is a combination of cutbacks in US military support for the Saudi-led coalition, combined with successful implementation of the UN taking a role in the administration of the strategic port city of Hodeidah. If diplomatic options fail and the UAE decides fighting should resume, the UN projects a worst-case scenario of 15 million Yemenis starving. Fighting has reached the outskirts of Yemen's Hodeidah port, on which food supplies depend.

The worst-case scenario is a catastrophic man-made famine, assessed as plausible in the coming six months, with Houthi forces, who are backed by Iranian military hardware, utilising images of starvation to garner international support. More than 1.3 million Yemeni children have suffered acute malnutrition since March 2015. The best-case scenario is for clashes to slow, particularly in the event of further intervention by the US Congress.

Deterioration Trends

Declarations of victory in the war against Islamic State (IS) have long been premature. The insurgents have reverted to a familiar asymmetric strategy based on rural extortion rackets to finance and coerce populations in an area of operation that stretches from remote south-eastern Syria to Iraq's Diyala province. Although the group has largely lost its capability to direct terrorist attacks overseas, it is still resilient as a clandestine armed movement, despite the loss of territorial control, reverting to the tactics of 2006-2014, prior to entering the Syrian civil war and the later capture of northern Iraq.

Its focus now is to continue attacks against Iraqi security forces and paramilitaries, aiming to provoke reprisals that drive a wedge between them and alienated Sunni communities, which have been decimated by the alleged endemic use of torture and rampant abuses by Iraqi security forces and paramilitaries. Iraq's biggest challenge lies in how to build capability in its de-centralised security sector, in a time of fragile political consensus behind the new government.

Business-As-Usual Trends

The appointment of a government in Iraq has forestalled the risk of an immediate slide into post-war chaos. Prime Minister Adil Abdul Mahdi's technocratic government has only tenuous support from a fractious parliamentary coalition of populists and Iranian proxies. In the national assembly's fluid and personalised system, it will highly likely prove impossible to tackle structural corruption and other governance failures, despite the best intentions of Mahdi and some of his colleagues.

The best-case scenario is that Iraq avoids being dragged into the proxy warfare between Iran and the US, giving it a chance to cement military gains against Islamic State (IS) via meaningful reconstruction investment in practical infrastructure such as electricity provision, coinciding with a non-sectarian reconciliation process that includes alienated Sunnis, Kurds and other minorities. Delay over the appointment of the new defence and interior ministers does not give cause for optimism, indicating progress is likely to be slow and easily reversible.

Sub-Saharan Africa

- Insurgent groups' asymmetric strategies means they will remain highly resilient to military strategies in the absence of socio-political processes addressing grievances
- A close race between two heavyweights in Nigeria's presidential election will likely go down to the wire.

Improvement Trends - For further analysis, see Gulf Investment in the Horn of Africa Parts I, II, and III.

Ethiopian Prime Minister Abiy Ahmed's continued drive to enact wide-ranging reforms has enabled the reconciliation between Eritrea and Ethiopia, while also improving relations between Eritrea and Djibouti, and between Ethiopia and Somalia, allowing for cautious optimism. As China and Gulf countries, particularly the UAE and Qatar, invest in major infrastructure projects, Horn countries are finding common economic interests.

Although this may not be enough to overcome parochial rivalries, infrastructure investments will give investors scope to assist with mediation, if required. Reconciliation has led to the lifting of UN sanctions on Eritrea. This is unlikely to result in any immediate lift in the reclusive pariah regime's policies such as forced indefinite conscription, but some economic liberalisation and inward investment may help improve domestic living conditions.

Deterioration Trends

Insurgencies in the Sahel, Somalia, Mozambique, DR Congo, and Cameroon are likely to deteriorate further. Financial and logistical difficulties are hindering the G5-Sahel Joint Force's mobilisation in Mali and its neighbours. Meanwhile, the French Barkhane operation's targeting of insurgent leaders is likely to fragment the militant alliance, Jama'at Nusrat al-Islam wal-Muslimin (JNIM), creating a power vacuum that will see rivals dispute the leadership. Insurgent attacks will continue to target the Operational Coordination Mechanism (MOC) to undermine local peace initiatives.

Al-Shabaab is likely to further ramp up its activities in the Galmudug region of Somalia, which has prompted a series of US drone strikes that are highly unlikely in isolation to curtail the group's asymmetric capabilities and manipulation of clan politics. Meanwhile, emerging evidence of Somali insurgents training Mozambique's Ansar al-Sunna militants comes as extremist networks take advantage of unemployment to recruit in disenfranchised communities in Cabo Delgado. Mass arrests and detentions and targeting of mosques will provide further ground for radicalisation.

In the DR Congo, the surprise victory of opposition leader Felix Tshisekedi has prompted fears of a backdoor deal between the candidate and President Joseph Kabila as observers deployed by the Catholic Church estimate that another opposition leader, Martin Fayulu, won by a large margin. Graver still is the delay of the presidential vote in Fayulu strongholds in four constituencies of North Kivu and Mai Ndombe provinces. The decision disenfranchises 1.3 million voters in a region that sees the response to an Ebola outbreak stumble in the wake of widespread anti-government militia violence.

The expected result in Cameroon's presidential poll in October will see re-elected President Paul Biya maintain a repressive stance against separatist groups in Anglophone regions, driving further incidents of kidnapping and violence as well as resentment among Anglophone populations. Biya's advanced age will focus attention on his successor.

Business-as-Usual Trends

In February's presidential election, incumbent Nigerian President Muhammadu Buhari will contest a close race with opposition candidate Atiku Abubakar. Atiku will bring a more energetic approach to campaigning alongside his deep pockets, while Buhari will take advantage of his strong northern support base and incumbent control over the security services. In Nigeria's exceptional chaos and complexity, the race is likely to be too close to call until the official result is announced. Clashes over disputed results in some localities will be highly likely, particularly Plateau, Kaduna, Rivers and Akwa Ibom. The winning contender may seek to assert his position by cracking down on Boko Haram and its offshoot Islamic State in West Africa (ISWA) in the Lake Chad region following an increased pace of attacks against military targets, which partly seeks to destabilise the polls.

Europe & Russia

• The European Union will struggle to reverse the trend towards fragmentation propelled by authoritarian populists, nationalist sentiments and its own internal contradictions.

• The form taken by UK's exit from the union in March will signal the path ahead: ugly compromise or potential catastrophe.

Improvement Trends

The retirement of EU Commission President Jean-Claude Juncker and the choice of his successor will be the political focus in Brussels in 2019. If the controversial "spitzenkandidat" process returns, it will give the commission's presidency to the party with the most seats in the European Parliament: either the centre-right European People's Party (EPP) or, less likely, the centre-left Party of European Socialists and Democrats (PES). Manfred Weber, the EPP candidate and clear favourite, has struck a traditionalist tone, helping him secure the backing of Hungary's prime minister, Viktor Orban, whose posture stands between authoritarian Euroscepticism and the Franco-German mainstream. Weber may be able to incentivise Orban to adopt a course more in line with European liberal democracy.

In Russia, President Vladimir Putin's government has adopted a defensive strategy in the face of a challenging economic outlook. Protests against pension reforms have indicated popular frustration at stagnant living standards. The technocrat behind Russia's strong economy in the 2000s, former finance minister Alexei Kudrin, has returned to Putin's cabinet, albeit to a minor post. His warnings that US sanctions will lead to decelerating growth have contributed to Putin's budget for 2019-2021 focusing on raising living standards via spending boosts in health, education and infrastructure.

Deterioration Trends

It is highly likely that UK Prime Minister Theresa May will be unable to pass her Brexit deal through parliament. Eurosceptics in the ruling Conservative party are supported by the party members who would have the final choice over the party's next leader, but blocked by two thirds of the parliamentary party. They are aligning behind a no-deal outcome as means to pursue an ideological agenda of deregulation, privatisation and public spending cuts. This outcome would mean economic and social turmoil. This is not fearmongering; planning for these circumstances is already underway in both government and industry.

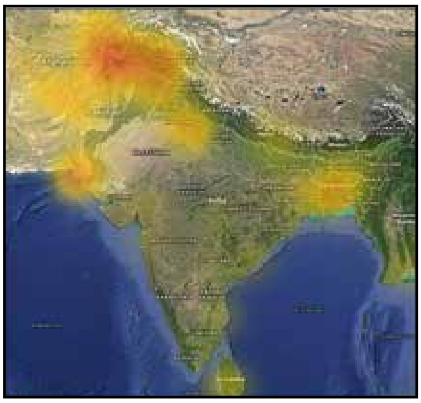
However, it would almost certainly be impossible to achieve this outcome via a parliamentary majority vote, and the Eurosceptics have no immediate-term path to power. A no-deal could only occur through the government deliberately allowing the Article 50 process to run its course, counter to the wishes of the legislature, leading to a chaotic, unmanaged Brexit.

Other plausible scenarios include another election, a delay to the Article 50 process and/or a second referendum if the election proves inconclusive. Parliament may take control over the process and force the government to adopt what is known as a "Norway plus" model, meaning continued customs union and single market membership, as well as continued free movement and budget contributions and no influence over rule-making. On balance, no deal appears marginally the more likely outcome, but the permutations are numerous.

Business-As-Usual Trends

Juncker's successor will face the task of stemming the drift towards authoritarian populists, most of all in Italy but also in the centre and east. The greatest threat is Italy's atypical government – simply put, a populist coalition of neo-anarchists and post-fascists – which has a popular mandate to fight EU fiscal rules, as Italian GDP has not grown since Italy joined the Euro. If markets take fright and Italian debt levels become unsustainable, it will create a crisis on a scale vastly larger than Greece. French President Macron's drive to set up a pan-European bank deposit insurance scheme, protecting the banking sector against spiralling sovereign borrowing costs, has stalled in the face of German conservatism, backed by Dutch-led fiscal hawks. No structural reforms are likely until Germany has a chancellor with a new mandate in 2021, particularly with Macron in such a weakened position following the gilet-jaunes (yellow vests) unrest.

South Asia



- New governments and returning administrations will raise both prospects for thriving democracy and fears of increasing autocracy over the coming year.
- Regional security priorities will continue to centre on the conflict in Afghanistan, which is highly unlikely to be resolved through a peace deal in 2019.

Improvement Trends

The removal of autocratic President Abdulla Yameen in September 2018's general election will herald a flourishing of democracy in the Maldives. The new government, led by Ibrahim Mohamed Solih, faces an uphill battle in addressing the corruption and nepotism that became entrenched under the Yameen premiership, as well as the country's swelling debt to China. Concerns around human rights legislation and will continue to unnerve prospective investors. Despite this, Solih's efforts to root out corruption and re-engage with the international community bode well for a more permissive operating environment.

Deterioration Trends

The security environment in Afghanistan will highly likely deteriorate further as a resilient Taliban insurgency makes battlefield gains and peace efforts continue to falter. The US will maintain its "fighting and talking" strategy, seeking to deny the Taliban militarily while pressuring Pakistan to force Taliban hardliners into joining negotiations.

A NATO drawdown, a Taliban precondition for peace talks, remains unlikely in 2019, with the Afghan army unable to provide security by itself. Presidential elections, scheduled for July 2019, are likely to go ahead, despite logistical and security concerns. The Taliban will almost certainly disrupt proceedings, resulting in an uptick in violence ahead of the vote.

The victory of the Awami League (AL) in December's national elections has served to accelerate Bangladesh's democratic backslide. The AL's win, precipitated by alleged repression targeting opposition parties, journalists and civil society groups, will further cement Bangladesh's status as a one-party state. A restrictive environment for dissent will intensify opposition grievances, which will in turn threaten to drive individuals further towards extremism, increasing the likelihood of sporadic terrorist violence in 2019.

Business-as-Usual Trends

In Pakistan, continued Chinese and Middle Eastern investment will provide a short-term solution to the country's economic woes; however, Islamabad's escalating balance of payments crisis, coupled with plummeting reserves, will likely force new Prime Minister Imran Khan to agree an IMF bailout package. The dangers for Khan are vast: increasing religious fanaticism, poverty, endemic corruption and an export market far smaller than that of India and Bangladesh. Khan will almost certainly defer to Pakistan's powerful military on foreign policy matters, with the military remaining obsessed with framing government policy in terms of national security.

The government's austerity programme will fuel unemployment, forcing Khan to rely on China creating more jobs for locals on the China-Pakistan Economic Corridor (CPEC) project. However, CPEC also brings its own inherent risks, with Baloch separatists targeting personnel and infrastructure and the enormity of the project threatening to double Pakistan's external debt. For more on the security risks facing Chinese developers in Pakistan, please see The China-Pakistan Economic Corridor: the Security Challenges.

As a result, Khan faces a deteriorating relationship with the US over a perceived lack of progress in countering violent extremism. The US will pursue high-pressure tactics to change Pakistani behaviour, likely revoking Pakistan's non-NATO major ally status, building on the suspension of military funding and restricted defence sales. Nevertheless, Pakistan under Khan will highly likely remain an enabling environment for violent extremists despites efforts by the armed forces to crack down on the Islamists they do not control in late 2018.

Asia Pacific

- Strong growth outlook for Asia Pacific with the prospect of improved economic cooperation
- Pressure growing on Myanmar

over possible crimes committed against the Rohingya

Improvement Trends

The economic outlook for the Asia Pacific region remains strong, duelling Asia Pacific free trade agreements, the Regional Comprehensive Economic Partnership (RCEP) and the Trans-Pacific Partnership (TPP) likely to see future progress. The RCEP has made significant diplomatic progress and Thailand is expected to champion the deal as chair of the ASEAN in 2019.

The TPP has been unexpectedly resurrected after President Donald Trump withdrew from the agreement. The revised pact, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) passed a major milestone when it was ratified by Australia in October 2018, triggering the beginning of implementation. Over time, the successful implementation of the CPTPP will support trade, investment and growth.

Deterioration Trends

Security concerns in Malaysia revolve around cross-border kidnappings, smuggling activities and unresolved sovereignty issues in the country's eastern Sabah state. Militants from the southern Philippines have reportedly resumed kidnap-for-ransom operations after a nearly two-year hiatus, raising the threat of abduction for vessels, particularly those traversing the waters off Sabah's east coast. Islamic State (IS)-affiliated terrorist networks, including Jamaah Ansharut Daulah (JAD), continue to pose a threat in Indonesia. Dozens of convicted terrorists are due to complete their prison sentences in 2019, including IS-linked individuals with connections to Syria, prompting concern that they may re-join existing networks to stage attacks.

Pressure is growing to hold Myanmar accountable for possible crimes committed against the Rohingya, and public deliberations on this issue will continue to negatively impact the country's investment climate in 2019. The UN has called for Myanmar military leaders to be prosecuted for genocide and other crimes against the Rohingya, and the International Criminal Court has indicated it could exercise jurisdiction to investigate alleged crimes against humanity.

Business-As-Usual Trends

The South China Sea will remain a regional flashpoint, although there has been a notable effort by the US and China to maintain communication channels, including via face-to-face meetings between senior military leaders. The US and Chinese navies have had close encounters at sea, and more incidents are likely in 2019. There has also been an increase in military drills by a number of navies in the region. US positioning will continue to fuel tensions which have so far manifested in a tit-for-tat trade war. The US has announced that it will partner with Australia to develop a naval base in Papua New Guinea in a strategic commitment aimed at countering Chinese influence.

The One Belt, One Road initiative will continue to provide abundant opportunities for China's economic growth and global strategic influence in 2019. Under the 'Digital Silk Road' element of the initiative - encompassing a global expansion of digital communications infrastructure - China will likely seek to commission and bring online numerous new satellites rivalling the US-owned GPS system. Chinese largesse will not, however, benefit all partners in One Belt One Road, with grants, loans and investments leaving several recipients, including Laos, Cambodia, Myanmar and Indonesia, at risk of becoming more deeply embroiled in debt traps they are highly likely unable to escape.

While violence in Thailand's southern region has declined in recent years, the stagnating conflict between Pattani-Malay separatists and the government will continue throughout 2019. The insurgent National Revolutionary Front (BRN), which controls most fighters in the region, rejects negotiations initiated by the Mara Pattani insurgent umbrella group. While plausible, there are no indications that the BRN will engage in direct talks with the Thai government, which is unlikely to devote significant resources to any peace talks against the backdrop of the ongoing royal transition and in the context of a looming election.

North & Central America

- Trade is the principle focus for the US, as it attempts to pass the USMCA agreement and navigate trade tensions with China.

- Poor socio-economic conditions will drive more Central American citizens towards Mexico and the

US, adding to social pressures over immigration issues.

Improvement Trends

The successor to NAFTA, the US-Mexico-Canada Agreement (USMCA) is likely to be approved by Congress by Q2. That all three countries have reached an agreement means the Democrats are unlikely to derail the deal due to the lack of a viable alternative. Global investors are likely to choose the US over other countries given current economic strength. However, benefits to corporations from tax cuts in 2018 are likely to fade, with growth forecast to revert back to its longer-term pace of near 2 percent.

Although corruption in the Northern Triangle of Honduras, Guatemala and El Salvador is endemic, mounting public discontent with elite corruption and moves by the courts and human rights ombudsman to hold leaders to account are gathering momentum among grassroots campaigners. Senior political figures such as Guatemala President Jimmy Morales, linked to electoral funding corruption, may plausibly be held to account, despite his campaign against the ombudsman.

Deterioration Trends

Differences between the US and China on trade will continue to ratchet upwards in 2019, with intermittent attempts to find a negotiated de-escalation likely to fail. Instead, tariffs already imposed on each other by the US and China are likely to remain in place as a grand agreement looks out of reach. This will be driven by US concerns over technology transfer and intellectual property protection, with further scrutiny on exports to China, triggering retaliatory Chinese action in turn.

The combination of instability, poverty, gang violence, corruption and weak governance in Central America will continue to drive groups of asylum seekers north towards Mexico and the US. Though many are unlikely to be granted legal asylum in the US, many families appear to have reached a tipping point nonetheless. A swelling number of young parents are prepared to risk dangerous journeys in order escape gang recruitment at home in Honduras, El Salvador and Nicaragua, where anti-government protesters continue to demand President Daniel Ortega's resignation.

Business-As-Usual Trends

Newly sworn-in Mexican President Andres Manuel Lopez Obrador, known as AMLO, faces the task of balancing the populist anti-establishment platform that won him the election with the pragmatism demanded by financial markets. Though AMLO has taken a more market-friendly approach to policy than his campaign rhetoric suggested, investors opposed to his agenda have alleged erratic policy formation, notably in his public consultation on the highly likely cancelled Mexico City airport project.

Relations with the US may be subject to greater strain, most of all on immigration and security, with AMLO unlikely to be as acquiescent to Washington as his predecessors, but also struggling for new ideas. The US government will press the Mexican government to maintain its policy of arresting and deporting migrants detained in southern Mexico, as the Trump administration conflates the issue of drugs and immigration for political purposes. Continued increases in coca production in Colombia and Peru will create swelling supply, resulting in cheaper and higher-quality cocaine in rich countries such as the US. In turn, conflict over supply routes will drive further gang violence and resulting displacement as the drugs are trafficked north.

In Canada, focus will turn to October's federal election where the Justin Trudeau's Liberals appear well placed to repeat their 2015 election victory, particularly if a split in the conservative leadership prevails. Voter concerns are highly likely to focus on immigration and a controversial carbon tax, potentially bringing populism into the fore for the first time with polls indicating that the Federal Conservatives hold a majority among males and non-university educated Canadians.

South America

- Continuing deterioration of the situation in Venezuela will place further political and economic pressure on neighbouring states.

- The spread of transnational organised crime will remain a persistent threat across much of the continent.

Improvement Trends

Transnational crime syndicates, such as the Brazilian Red Command (CV), are highly likely to continue to expand their presence in Paraguay. Despite this, recent successes of large-scale, Interpol-led operations in countering violence and trafficking suggests an evolution in the capability of law enforcement authorities to tackle and minimise organised crime.

Paraguay's improvements in tackling organised crime are, however, likely to be a regional anomaly. With organised criminal groups developing at a rate faster than regional law enforcement's coping capabilities, 2019 will see a strengthening, rather than contraction of gang-related crime.

With the exception of Venezuela, and to some extent Argentina, the region will experience slow, but consistent, economic growth. 2019 will continue a three-year upwards trend of approximately 2.7 percent growth, bolstered by pro-investment policies in Colombia, an alternative NAFTA agreement for Mexico, economic reform in Brazil, and mining industry growth in Chile and Peru.

Deterioration Trends

In Argentina, continued economic contraction and standby loan negotiations with the International Monetary Fund (IMF) will negatively impact President Mauricio Macri's popularity in the run-up to October elections. IMF-mandated cuts to public spending alongside impacts of recession mean public discontent is increasingly likely.

Presidential and Congressional elections in October will be Bolivia's greatest potential flashpoint. Declining support for President Evo Morales, compounded by frustration over term limits, will bolster opposition movements. These factors make a contested election result likely, with increased risk of street protests from both sides of the political spectrum. Unrest will cause widespread transport disruptions, potentially leading to sporadic outbreaks of violence.

In Colombia, as negotiations with the National Liberation Army (ELN) continue to falter, instances of violence against security forces and private entities within the energy sector will increase. This violence will predominantly be concentrated in the oil-producing regions of Norte de Santander, Putumayo, and Arauca. Despite President Ivan Duque's promises to tackle drug cultivation, failure to successfully implement crop substitution programmes means coca cultivation, cocaine production, and drug trafficking will remain significant issues.

The persistent economic crisis in Venezuela will continue to shape the country's short and long-term future. Inflation is likely to reach 10,000,000 percent, coinciding with a catastrophic fall in GDP and oil production. The focus of most Venezuelans on basic survival is impeding the development of a domestic opposition movement. Although most Venezuelans support a military coup, the persecution of Nicolas Maduro's opponents has forestalled this to date. The most probable outcome is further deterioration of the economic, political, and humanitarian situation, resulting in continued outflows of refugees.

Business-As-Usual Trends

Chile will remain comparatively stable, with limited examples of the instabilities present elsewhere in the region. As fiscal recovery following structural reforms continues, and the country sees some decrease in inequality, the likelihood of significant economic or political dissatisfaction remains low. There will be few instances of international organised crime groups operating to the same extent as in other South American nations.

A full PDF of the report can be downloaded at https://g4sriskconsulting.campgn3.com/Global-Forecast-2019?vsmaid=1245&vcid=20017

Why Facial Recognition on Body-Worn Cameras Will Now Transform Frontline Policing

Facial recognition might be transforming the security of our airports, workplaces and homes, but in law enforcement, where one might expect to find the most fervent take-up of this new and powerful technology, it has not been smooth sailing. Accusations of inaccuracy, unlawfulness, bias and ineffectiveness have become the norm. But the real issue is 'deployability': the AI engines powering facial recognition solutions need to be trained for the real world. And, more importantly, the wrappers around the usage and systemizing of the technology need to be properly architected.

Facial recognition was initially designed for identity assurance and access control, to operate in controlled conditions and to confirm that a person is who they claim to be. Now cameras scan crowds, comparing every passing face to a watch list. This is of itself is plagued with difficulty. But when there is a match, what happens next? How can systems account for data quality, environmental conditions and scoring thresholds? How can users shift the focus from technology to outcomes?

With mass adoption now on the way, there might just be enough traction to resolve these challenges. Police forces are actively testing facial recognition, working out use cases. There is still much work to be done, but the answer to that 'deployability' challenge could be, literally, right in front of them.

Moving Forwards

Recent news that the FBI has been testing Amazon's facial recognition was met with predictable levels of consternation from a privacy lobby that has decided facial recognition in law enforcement is bad. Period. As it happens, the example cited by the FBI for where the technology could have been used was just about the least contentious one imaginable: sifting thousands of hours of recorded video for sightings of Vegas shooter, Stephen Paddock. "We had agents and analysts, eight per shift, working 24/7 for three weeks going through the footage," FBI Deputy Assistant Director Christine Halvorsen told an

AWS conference in November.

Although many law enforcement agencies make use of facial recognition to analyse recorded video footage, saving time and effort, it is much harder to use in real-time, in the real world. The mathematics of checking every passer-by in a crowded public space against even small watch lists pushes facial recognition to its limits. Only the very best systems can cope. Consequently, there is still remarkably little live facial recognition used in mainstream policing. But that is about to change.

One force testing the options for real-time facial recognition is the Metropolitan Police in London. Commissioner Cressida Dick said last year that facial recognition "is getting better and better and better by the minute… I think the public would expect us to be thinking about how we can use this technology and seeing whether it is effective and efficient for us." But, in December, when the Met Police parked a surveillance van in the city's Soho area with a nest of roof-mounted cameras to check Christmas crowds against a watch list of wanted criminals, it prompted a stark response from privacy campaigners. The director of Big Brother Watch called it "a terrible waste of police time and public money" and said that "it is well overdue that police drop this dangerous and lawless technology."

Recognizing the controversial aspects to the technology, the Met Police has made clear its keenness to engage. Ivan Balhatchet, the Met's strategic lead for live facial recognition, said in a statement in December that "we continue to engage with many different stakeholders, some who actively challenge our use of this technology; in order to show transparency and continue constructive debate, we have invited individuals and groups with varying views on our use of facial recognition technology to this deployment."

Going Mobile

In contrast to facial recognition, bodycams have already seen mass adoption. These body-worn video devices now accessorize police uniforms worldwide, providing evidence management, officer safety and public reassurance. Bodycams record footage for offloading into physical or cloud-based storage systems. Some bodycams also live stream video back to control rooms. Others link to weapon holsters to automatically trigger video recording. As mobile devices evolve, the newer models of bodycams which are based on smartphone platforms are set to become more powerful. This means the two technologies will converge. Facial recognition on bodycams is an obvious next step. Empowering officers with watch lists of wanted criminals, persons of interest, missing children, vulnerable adults… The list goes on.

And it has already started.

In December, whilst London debated its green van, a different test of facial recognition was taking place in another 'world city' many thousands of miles away. This test didn't generate headlines. It was unpublicized. Its details undisclosed. But it is much more illustrative of how facial recognition will be deployed in frontline policing. As with London, the test took to city streets with a watch list of around two-thousand people. But this test focused on 'stop and search', with facial recognition on bodycams, rather than CCTV or surveillance vans. The test involved a small number of officers wearing devices that worked in real-time from the same watch list. Within the first few hours, two arrests were made following successful facial recognition matches from those bodycams. The suspects are now being prosecuted.

Those arrests were made by a city police force that is focused on tackling gang violence as well as serious and organized crime. At a federal level in the same country, facial recognition on bodycams is being trialled in airports as part of an ongoing process to enhance security at the highest profile locations. The nature of live, networked facial recognition is that

CRITICAL INFRASTRUCTURE PROTECTION FORUM

BUCHAREST, ROMANIA
MARCH 25TH - 29TH, 2019
4TH EDITION

EMEREGING TECHNOLOGIES TRANSFORMING CRITICAL INFRASTRUCTURE

New geopolitical and geostrategic asymmetric threats make it possible to destabilize global, regional, European and / or state security. In the context of migration and numerous terrorist attacks and the opening of conflict zones at its borders, Europe is forced to re-calibrate its Member States' security and union policies to overcome unprecedented dynamics of security-related conflicts and its stability. Thus, the protection of critical infrastructure becomes important and absolutely necessary for the achievement of the safety of the European citizen.

The Forth Edition of the CRITICAL INFRASTRUCTURE PROTECTION FORUM – CIP FORUM - EMERGENT TECHNOLOGIES TRANSFORMING CRITICAL INFRASTRUCTURES - aims to promote the use of emerging technologies in critical infrastructure protection transformation.

Conference Topics
A multitude range of topics have been announced for the fourth edition of the conference, including discussion regarding subjects considered pillars for 2019, such as: ***Cybersecurity*** (It was a transition year for cyber security professionals and attackers alike. The total number of violations has fallen since 2017, but attackers change tactics: once servers and workstations have priority, threats are now directed directly to mobile applications); Smart cities (smart city spending is estimated to reach $ 80 billion this year and will grow to $ 135 billion 2021, according to a new report by International Data Corporation (IDC); ***Artificial Intelligence*** (Labour productivity growth is expected to account more than 55% of contributions to the GNI by the Artificial Intelligence between 2017 and 2030); ***Blockchain*** (In the 2018 PwC analysis of 600 executives from 15 territories, 84% say their organizations have at least one involvement in blockchain technology. Everyone talks about blockchain, and nobody wants to be left behind).

Join us in Bucharest, Romania, between March 25th-29th, 2019

www.cip-forum.ro

the same endpoints can link to multiple watch lists: immigration, crime, counter-terrorism and national security. And the nature of such a system means that results are also networked live, but only to those authorized to view such information. An immigration issue might be flagged to local officers, whereas a counter-terrorism match would alert elsewhere.

The clear difference between facial recognition on bodycams as opposed to surveillance vehicles or CCTV is the human interaction involved. An officer is engaging with members of the public, with potential persons of interest. There are clear benefits to this, including ensuring that someone on the frontline is making an active decision before any arrest or intervention is made. Facial recognition should be seen as a valuable tool to assist officers, not a decision-making system in itself. This is especially true with stop and search.

Stop and search is of itself controversial. Such powers go to the heart of policing by consent, raising questions about profiling and bias and justification. Despite the criticism, it can be immensely effective, taking weapons from the street and arresting those in possession. Identity confirmation is a key part of the tactic. As is targeting those to be stopped. Bodycams with facial recognition ensure identities are captured and checked accurately, all in accordance with legislation and policy. Known offenders, persons of interest – whether identified or not, vulnerable minors and adults, all can be identified as such. As an aid to intelligence-led frontline policing it offers serious benefits. The arrests referenced above were only made possible by such methods. In this instance, it resulted in a process to deploy the bodycams across the city. The results were incontestable.

Setting Boundaries

The use of facial recognition on bodycams also offers a defence against accusations of racial bias. Policies can be set to prevent officers searching those not identified by facial recognition, even when stopped. Where the accusation is made that stop and search over-polices low-level crime in specific communities, facial recognition on bodycams offers a balance. It is this kind of safeguarding that will help prompt broader adoption.

Facial recognition on bodycams will also provide secondary verification for matches from surveillance vehicles and CCTV cameras. Following an initial match, an officer on foot approaches the person and runs a second check from a bodycam, running from the exact same watch list. Only if there is also a match is anything taken further. In of itself, this is a very material safeguard against so-called false positives. It also provides a person to person interaction before any final decision on an arrest is made.

Edge Artificial Intelligence At Work

It is this systemizing of facial recognition that we will see next. The linkage of multiple cameras to the same watch lists, and to each other. Shifting processing to mobile devices opens up the broader benefits of edge-intelligence. AI on mobile devices that can link to each other as well as to a central hub. The ability to run from multiple, segmented, and synchronized watch lists. All live and in real time.

As surveillance systems running networked facial recognition across multiple endpoints of different types become more commonplace, we will see it running across the combination of CCTV feeds, overt and covert vehicles as well as rapidly deployable cameras and mobile devices. There is already testing at transport hubs and sports stadiums, where security and surveillance is stressed at particular times of the day and week, and the need for flexibility is paramount. Testing for border security is even further advanced, where facial recognition is already used in immigration systems, and more advanced systems are relatively straightforward given the controlled environment and compliant footfall.

In discussing advances in surveillance, senior officers will emphasize time and again that "policing is live and real-time". As soon as point surveillance solutions shift to networked systems, the quality and resilience of connectivity becomes critical. Whilst the performance of a facial recognition system is important, there is serious frustration with some early adopters where their watch lists are standalone and linked to specific camera deployments, and their results are not shared beyond the immediate location. As we see the acceleration of IoT devices for security and law enforcement, this will be resolved.

With live connectivity, if there is an incident, as the intelligence picture changes, all cameras – including bodycams – are continually updated. The secondary benefit of this is the potential to use edge-intelligent bodycams to provide an initial match, essentially narrowing down the haystack, with the match then sent to a central cloud-based system using the same AI engine, or a different AI engine, or even multiple AI engines, to provide a much more accurate filter before any 'match' is presented to an operator. All of that would happen in one or two seconds.

The results would be near 100% perfect.

This Is the Year

This should be the year when facial recognition shakes the accusations of inherent bias and inaccuracy. It should be the year when there is an acknowledgment that not all facial recognition technologies are the same. Different tools should be acquired for different purposes. And the sterile assessment of such engines in controlled conditions should give way to actual customer references and proof of outcomes.

The first generation of bodycams in operation today has focused on recording video for evidence management systems. Now, Bodycam 2.0 will shift the focus to live video streaming, facial recognition and on-device Edge-AI. This next generation of IoT bodycams will join the billions of other IoT devices that will be deployed on 4G and 5G networks over the coming years. Designed to be networked, to share data, to split processing from edge to centre, these devices will evolve away from 'just in case' video recording towards an essential policing tool. Ultimately, convergence will see the types of bodycam in use today morph into ruggedized, large-screen smartphones that will combine a capture and streaming capability with edge AI analytics and rich data presentation to the frontline officer. The era of the single-purpose record-only camera is coming to an end.

For facial recognition, the debate and controversy in 2019 should be around the completely unregulated uses of the capability for marketing and commercial security. AI in silicon embedded in cheap IP cameras, accessible to all. I have written before about the concerns we should have at the thought of commercial enterprises, schools, universities, maybe even neighbourhood watch schemes compiling their own watch lists of persons of interest based on captured or opensource databases. The use of this technology in law enforcement will cease to be quite so polarizing.

And so, as far as policing is concerned, 2019 will be marked as a turning point for facial recognition. Tests will morph into deployments. Deployments will yield results. The arguments will be won. The majority of the public, ultimately, will opt for personal security and safety over arbitrary privacy. In the wake of multiple calls for restrictions and regulation, a survey published recently found that only 18% of Americans believe facial recognition should be strictly limited at the expense of public safety. And this is where bodycams will come into their own. If we could train our police officers to recognize every known offender, every unidentified person of interest, every vulnerable adult or missing child, to a 99% or greater level of accuracy, then we would. Well, now we can.

by Zak Doffman CEO at Digital Barriers

The Builders of the Desert

Operation Barkhane

From the outset of the security crisis in the Sahel, France has been strongly committed to blocking terrorism. In January 2013, France took action in northern Mali via Operation Serval to prevent al-Qaeda-affiliated groups from taking control of the country. Since then, French operations, which include some 4,500 soldiers, were regionalized under Operation Barkhane, providing essential support to the G5 Sahel countries; Mauritania, Mali, Burkina Faso, Niger and Chad in their actions to fight terrorist armed groups.

The Sahel is made up of many African countries, from East to West Africa, from Dakar to Djibouti.

The Sahel was faced with an increasing threat from terrorism and organised crime, which was destabilizing the region. To address this situation, two initiatives were set up, The G5 Sahel Cross-Border Joint Force which was launched in July 2017, by the presidents of the five states of Sahel. This joint force has been endorsed by the African Union, sanctioned by the UN Security Council and is sponsored by France. It's mandate is to combat terrorism, transnational organized crime and human trafficking in the G5 Sahel region.

At full capacity, the Joint Force comprises some 5,000 troops, 7 battalions spread over 3 zones, the West, the Centre and the East, and covers around 50km on each side of the country's borders, equating to some 5million km2 of desert area.

The second initiative is the Sahel Alliance. The founding members are France, Germany, EU, World Bank, African Development Bank and UNDP. This initiative is a mechanism for strengthening the coordination among partners and providing more rapid, more effective and better targeted assistance, as and when it is needed. The five key sectors are;

- Youth employability - education and training,
- Agriculture – rural development and food security
- Energy and climate
- Governance
- Decentralization and support for the deployment of basic services.

This modern war would be impossible to win without a network of camps capable of holding the equipment and materials for the 5000+ troops and of course the troops themselves.

This is where the French Army Defence Infrastructure Service (Service d'infrastructure de la Défense – SID) comes into its own.

In hostile environments, in 50 degree plus heat, and from the middle of an empty desert, this specialized unit designs, builds and operates complex camps, containing; hospitals, highly computerized command posts, accommodation, fuel and ammunition storage and all the infrastructure necessary for modern combatants including water treatment plants.

Speed is very much of the essence when building these camps. In just 6 months a camp of some 500 military personnel, with the infrastructure of a small village but conforming to operational requirements is in operation.

When designing and building the camp the SID always take into account the threat protection aspect of the exterior and in the case of camps in Sahal, the one source that is plentiful is… sand, gravel and rocks, making one supplier of the SID perfect for this type of operation; DefenCell.

J&S Franklin's DefenCell MAC is a rapid to deploy barrier system engineered from geotextile lined welded mesh gabions. Filled on site with earth, sand or other locally available material, DefenCell MAC units form defensive structures and barriers to protect personnel and infrastructure against a wide range of ballistic threats and hostile vehicles as well as floods and storms.

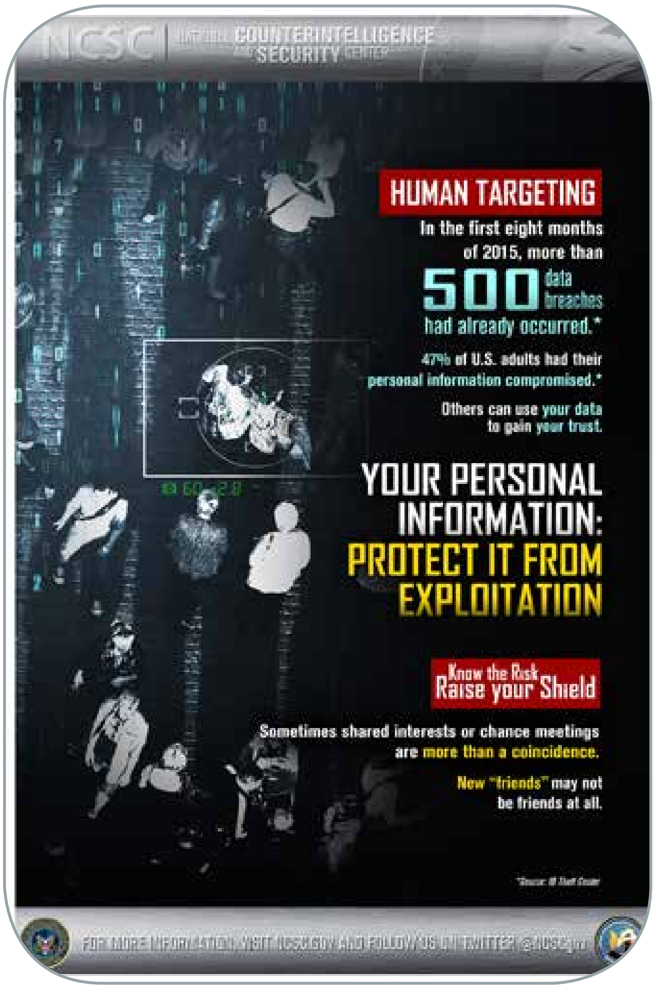
The Service d'infrastructure de la Défense has to adapt to the ever-changing situation of this modern-day war. They have to manage the complexity of a camp that can increase from 500 and 1800 personnel in just four years, and so the whole camp must be re-thought, borders extended, and all the necessary infrastructure required to accommodate this increase in personnel.

In the Gao Base in Mail, the SID has built the biggest munitions depot ever built in OPEX. The design of the ammunition storage was far from simple, as not only did the ammunition need to be protected from an outside attack but also from any possible kinetic energy released in one container that could detonate any of the other containers. The final storage solution was that the five containers of ammunition are now housed under walls and roofs of DefenCell MAC protective welded mesh metal gabions. There is now nearly 70 thousand kilos of ammunition fortified and safely stored thanks to the Service d'infrastructure de la Défense and J & S Franklin's DefenCell MAC.

Jeremy Milton of J & S Franklin said, "We work with many Engineering sections of many Military forces worldwide and have been working with Service d'infrastructure de la Défense for some time, in fact over the last two years, we have delivered over 4 million euros worth of DefenCell MAC to them."

US National Counterintelligence & Security Centre Launches Campaign to Help Guard Against Threats from Nation State Actors

The National Counterintelligence and Security Center (NCSC) has disseminated videos, brochures, and other informative materials to help the private sector guard against growing threats from foreign intelligence entities and other adversaries.


NCSC | NATIONAL COUNTERINTELLIGENCE AND SECURITY CENTER
HUMAN TARGETING
In the first eight months of 2015, more than
500 data breaches
had already occurred.*
47% of U.S. adults had their personal information compromised.*
Others can use your data to gain your trust.
YOUR PERSONAL INFORMATION:
PROTECT IT FROM EXPLOITATION
Know the Risk Raise your Shield
Sometimes shared interests or chance meetings are more than a coincidence.
New "friends" may not be friends at all.
*Source: ID Theft Center
FOR MORE INFORMATION, VISIT NCSC.GOV AND FOLLOW US ON TWITTER @NCSCgov

"Make no mistake, American companies are squarely in the cross-hairs of well-financed nation-state actors, who are routinely breaching private sector networks, stealing proprietary data, and compromising supply chains. The attacks are persistent, aggressive, and cost our nation jobs, economic advantage, and hundreds of billions of dollars," said NCSC Director William Evanina. "To enhance private sector awareness, we're arming U.S. companies with information they need to better understand and defend against these threats."

Recent examples underscore the foreign intelligence threats faced by U.S. companies:

- Last month, cyber actors associated with China's Ministry of State Security were indicted by the U.S. for global computer intrusion campaigns targeting intellectual property, confidential business information, and other data at managed service providers, as well as at more than 45 U.S. technology companies and U.S. government agencies.

- In September 2018, U.S. charges were announced against a North Korean, state-backed hacker for his role in the Global WannaCry 2.0 ransomware, the cyberattack on Sony Pictures, spear-phishing attacks on U.S. defense contractors, and other activities.

- In March 2018, the FBI and Department of Homeland Security issued a joint technical alert about an ongoing intrusion campaign by Russian government cyber actors to reconnoiter U.S. energy sector networks.

- In March 2018, the U.S. levied charges against nine Iranians for a massive hacking campaign at the behest of Iran's Islamic Republican Guard Corps that targeted intellectual property and other research at more than 144 U.S. universities.

Accordingly, NCSC is distributing its trademarked "**Know the Risk, Raise Your Shield**" materials specifically to raise awareness among private sector organizations and equip them with best practices for protecting their data, assets, technologies, and networks. These materials were previously distributed to raise awareness in the federal workforce.

The "Know the Risk, Raise Your

Shield" materials are featured on NCSC's website (NCSC.gov) or at https://www.dni.gov/ncsc/knowtherisk/tools/ and include videos, posters, brochures, and flyers. They address numerous topics, including supply chain risks, economic espionage, social engineering, social media deception, spear-phishing, mobile device safety, and foreign travel risks. At a minimum, the materials provide basic tips to help mitigate risks faced by the private sector.

These include:

- Corporate supply chains are growing targets of foreign intelligence entities. Adversaries are bypassing hardened corporate defenses by using less-secure suppliers and vendors as surreptitious entry points to surveil, sabotage, and steal information from companies' networks. Supply chain security can be expensive, but lack thereof is costlier and can result in pronounced, long-lasting damage. This is a place where an ounce of prevention is worth a pound of cure. TIP: Know your suppliers, the equipment and services they provide, and their service providers. Ask the right questions before procuring their products or services. Integrate acquisition and procurement personnel into your organization's enterprise-wide risk management and security program.

- Spear-phishing e-mails, in which the recipient is asked to click on a link or attachment, remain a common tool for foreign intelligence entities to compromise networks and access data. In October 2018, two Chinese intelligence officers and eight others were indicted for hacking U.S. and European aerospace firms over five years to steal trade secrets on commercial aircraft engines. They allegedly used spear-phishing and other tactics to penetrate company networks. TIP: Never click on suspicious links or attachments, particularly from unverified or unknown sources.

- Social media deception is another technique used to target private sector individuals. Adversaries may create fake profiles on social media, posing as a job recruiter or someone with a shared interest, to connect with and elicit information from business persons. China's intelligence services use social media platforms to spot, assess, and target Americans with access to business or government secrets. A former CIA officer convicted of espionage conspiracy in 2018 was first approached by a Chinese intelligence operative posing as a job recruiter on social media. TIP: Maximize your social media privacy settings; use caution in what you share; never accept friend requests from strangers; and validate friend requests through other sources.

- Foreign travel presents critical risks to private sector individuals, particularly those bringing smart phones, laptops or other electronic devices. When abroad, don't expect electronic privacy. Wi-Fi networks overseas are regularly monitored by security services and others who can insert malicious software into your device through any connection they control. They can also do it remotely if your device is enabled for wireless connection. TIP: If possible, leave your electronic device at home. If you bring it, always keep it with you; the hotel safe isn't really "safe."

Another resource available to the private sector is NCSC's 2018 Foreign Economic Espionage in Cyberspace report, which provides the latest unclassified information on foreign intelligence efforts to steal U.S. intellectual property, trade secrets, and proprietary data via cyberspace.

NCSC
SOCIAL ENGINEERING
Deceiving and manipulating people into revealing information.
Their Deception: Posing as representatives from familiar organizations.
Their Manipulation: Asking for passwords and account numbers for seemingly legitimate use.
YOUR PERSONAL INFORMATION:
PROTECT IT FROM EXPLOITATION
Know the Risk Raise your Shield
ASK questions.
REMEMBER that familiar ≠ legitimate.
VERIFY any request for sensitive information.

Released in July 2018, the report identifies the most pervasive nation-state threat actors, including China, Russia and Iran; those U.S. industrial sectors of greatest interest to foreign threat actors; and several emerging threats that warrant attention, including

- Software supply chain infiltration, which has already threatened the U.S. critical infrastructure and is poised to threaten other sectors.

- Laws in foreign countries, such as those in China and Russia, that can pose an increased intellectual property risk to U.S. companies doing business there.

- Foreign technology firms that are subject to foreign state influence or have links to foreign governments with high-threat intelligence services.

NCSC is a center within the Office of the Director of National Intelligence. NCSC is the nation's premier source for counterintelligence and security expertise and a trusted mission partner in protecting America against foreign and other adversarial threats.

by Karen Kingham
Features Editor

A word from the Chairman

John Donlon
Chairman
International Association of CIP Professionals
(IACIPP)

As we enter 2019, we can reflect on the year gone by and hopefully look forward to a more peaceful period of time. Is that wishful thinking? Maybe it is. The globalised environment remains turbulent and dynamic and we have to be ever mindful of the challenges we may face and as a response to today's threat complexities the International community involved in the protection and resilience of National Infrastructure needs to constantly review and revise the posture it adopts to remain effective.

The current geopolitical situation alongside the ever evolving threats that we face tend to suggest that this year will be as demanding as previous. Some analysts believe the geopolitical environment at this time is the most dangerous it has been in decades. One report I read predicts that 2019 could turn out to be the year the world falls apart, that maybe a little dramatic, but it does catch your attention. That report cited a number of potential scenarios to support their reasoning including such things as:

- A Russian cyberattack gets out of control.
- Iran and Saudi Arabia (or Israel) trigger a Middle East war.
- The Chinese and Americans get into a trade war that causes a deep recession
- The Americans and North Koreans fall out…and
- Brexit creates more of an international disaster than predicted

All of these have the potential to cause real concern and only time will tell how they may play out.

From an IACIPP community perspective I personally believe the major concerns, in terms of security and resilience remain around:

Terrorism
Natural Disasters/Adverse Weather
Cyber-attacks
Major Accidents and
Pandemics

There was a really interesting presentation at the CIPRA conference in Sarawak last June where the results of a survey undertaken from a Business Continuity perspective were discussed. The survey was carried out across 76 countries with over 650 respondents looking to identify the greatest concerns around major disruptions that would have an impact on critical infrastructure to their business.

The top three concerns across the globe were broadly the same and fell within the areas of:

- Natural Disasters/Adverse weather conditions
- Unplanned IT & Telecom Outages and Interruption to Utility Supply – which could be due to a natural disaster or a terrorism act either physical or cyber
- A Cyber Attack as an issue on its own

I think we can all understand why these would top the list within the context of current times.

The Natural Disaster 2017 report which was published late last year tends to support those concerns, and certainly in some parts of the world more than others. It shows there were 335 natural disasters which affected over 95.6 million people, killing 9,697 and costing a total of US $335 billion.

This burden was not shared equally, as you would expect. Asia seemed to be the most vulnerable continent for floods and storms with 44% of all disaster events, 58% of the total deaths and 70% of the total people affected.

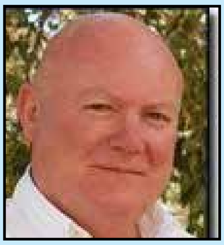
Differing threats will continue to create differing risks to the various parts of our critical infrastructure. Some we can prevent and some we can only prepare for. We have to continue to learn from past events and from the experiences of others and continually review the policies, plans and processes we have in place to enable us to respond to and recover from such incidents.

I am looking forward to Chairing the CIPRNA conference in Orlando in May this year. A significant part of the agenda will be exploring recent natural disasters and adverse weather occurrences within the USA and discussions will centre on the learning that has taken place and what is being introduced to ensure a higher level of future preparedness.

I hope to see some of you there to contribute to and learn from the experiences of others. If you can't make it we will provide an update on our website for all IACIPP members in the summer edition of the World Security Report.

Two new key appointments

IACIPP is delighted to announce two new key appointments, that of Dr Bill Bailey, BA(Hons) MA, MCIL, PhD. as Regional Director – Australasia and Lance Davis as Deputy Regional Director – Australasia



Bill Bailey is currently a security management consultant working in the oil and gas industry predominately in Papua New Guinea (PNG). Bill also remains an Adjunct Senior Lecturer with Edith Cowan University, Security Research Institute, Perth, Australia after having taught in the Security Science Department, specialising in: counter insurgency, terrorism and countering terrorism, critical infrastructure protection, security management, physical security, security, health and safety, business continuity, strategic risk and emergency management.

Lance Davis is currently serving as Security Superintendent responsible for Managing all Security functions in Oil Search (PNG) Ltd., Field Operations which includes Hides Gas Field, Kutubu, Agogo, Moran, Gobe, Kopi and Kumul Terminal. He has a long history of working in the oil and gas industry in PNG. In 2015 he was engaged by PNG Police Force to conduct an overall security risk assessment for the Pacific Games held in PNG. Prior to that Lance served in the PNG Armed forces completing six operational tours as Patrol Commander and Acting Recon Platoon Commander during the Bougainville crisis. Finishing his army career as an instructor at the PNGDF Training unit responsible for training PNG soldiers for roles within PNG's elite Recon and Special Forces operations.

John Donlon QM Chairman of the IACIPP said: "We are extremely pleased to have new directors of such experience and high calibre. They bring a depth of experience in both the public and private sectors that will be of tremendous value to us as we continue to develop the range of programmes we offer the CIP community."

Assistant Director for Infrastructure Security Brian Harrell to deliver opening keynote at CIPRNA

Critical Infrastructure Protection and Resilience North America (CIPRNA) has announced the US Assistant Director for Infrastructure Security, Brian Harrell, will deliver the opening keynote at this year's event in Tampa, Florida, 7th-9th May 2019.

Brian Harrell was appointed by the President of the United States in December 2018 to serve as the Department of Homeland Security's Assistant Secretary for Infrastructure Protection. However, Brian now serves as the first Assistant Director for Infrastructure Security within the newly renamed U.S. Cybersecurity and Infrastructure Security Agency (CISA).

Recently recognized as Security Magazine's Most Influential People in Security, Brian is the former Managing Director of Enterprise Security at the Duke Energy Corporation. He is also the former Director of the Electricity ISAC and Director of Critical Infrastructure Protection Programs at the North American Electric Reliability Corporation (NERC) where he was charged with helping protect North America's electric grid from physical and cyber-attack. Brian has spent time during his career in the US Marine Corps and various private sector agencies with the goal of protecting the United States from security threats.

Critical Infrastructure Protection and Resilience North America is the only event of its kind in the US and is supported by the US Chief DISA/DoDIN Critical Infrastructure Protection (CIP) Program, as well as the International Association of CIP Professionals, the Government Technology & Services Coalition and Global Institute for CyberSecurity & Research.

In addition to a whole conference programme of expert speakers from across the critical Infrastructure (CI) community, the City of Tampa itself will present a true-life, multi-discipline, multi-agency case study on the practical application of critical infrastructure protection and resilience.

Critical Infrastructure Protection & Resilience North America provides a unique forum in which to meet and discuss the issues with some of the most influential and experienced infrastructure security and resilience policy makers and practitioners in the world.

The event will be held at the Doubletree Hotel Tampa Airport – Westshore just five minutes from Tampa International Airport. Further details can be viewed at www.ciprna-expo.com.

Free EU-funded eLearning platform on Insider Threat now live

After 2 years of intense work, the outcome of the Insider Threat project co-led by Securitas, DHL, Palmyra Aviation Advisors and CoESS becomes available to all players in Critical Infrastructure.

Help2Protect.info is an online platform hosting two sets of eLearning tools: an Awareness Training and an Insider Threat Program Builder. The target audience is mainly transportation and energy ecosystems, but also other types of Critical Infrastructure. The ultimate objective is to help Infrastructure Operators enhance their resistance against Insider Threats.

If you think that the Insider Threat is not your problem, think again. Companies like British Airways, Belgium's nuclear power in Doel, the French CERN Large Hadron Collider, and many more around the world, have been the target of Insider Threats' attempted sabotage, which – if they had been successful – could have caused major damage and casualties.

Mitigating the Insider Threat, in particular in Critical Infrastructure, is therefore one of the top priorities of the European Commission and, as a result, one of the hot topics that CoESS (the European organisation representing the national private security associations) has been busy with for the last four years.

So, what is 'Insider Threat'?

Defining the Insider Threat is relatively simple: it is anyone who can have access and damage your organization. Whilst the vast majority of employees are loyal and honest, a very small but potentially very dangerous minority may try to damage your organisation for a variety of reasons.   The threat may also come from sub-contractors, consultants, interim and temporary staff.

Whilst jihadist terrorism is a very obvious source of concern nowadays, the Insider Threat is not just about ideology-driven attacks. It can go from petty theft to wide-scale espionage, from the employee stealing consumables to people stealing crucial data and leaking it to the rest of the world (e.g. Edward Snowden, who was a sub-contractor for the CIA). It can also go from minor sabotage by disgruntled employees, to the same becoming active shooters on their (former) workplace.

Trying to find facts and figures about the Insider Threat in the EU is not easy. One of the reasons is that, because many companies don’t have an Insider Threat programme in place, they are unlikely to detect them until they have caused major incidents.

The aviation industry is particularly vulnerable because it has been the target of terrorist attacks since decades, and the possibility of having help from the inside is therefore very attractive. With little resources, great damage can be done.

7,000 items stolen daily

On the other side of the Atlantic, the Transport Security Administration (TSA) has made some figures public: for example, around 7,000 items are stolen each day from checked luggage in security restricted areas; 5% of the total airport ID cards are missing in the USA, some of them probably still active. This represents several thousand cards. Whilst the Insider Threat is not the most numerous type of threat, with about 1,900 reported incidents in the last ten years, it is the most costly and damaging kind, with an average cost per incident of EUR 400,000.

The Jihadist threat (foreign fighters and so-called returnees) is still the key threat, but Europol’s TE-SAT also lists amongst future trends right-wing extremism and ethno-nationalist terrorism. Against this background, the European Commission has been organizing events and publishing documents since 2015, highlighting the threat and seeking to find best practice to counter it. Whilst there is a vast body of literature about it – from specialized agencies like the FBI, CERT (EU Computer Emergency Response Team) or the CPNI (British Centre for the Protection of National Infrastructure), consultants, or experts in this field – there was, until now, no free, accessible to all, web-based training in the EU that could be used in order to raise the awareness of a very wide and varied public, such as the people who work in airports. The Help2Protect training modules are designed to close this gap.

Web-based modules

In response to the call for applications for EU Funds (Internal Security Fund) in 2015, Securitas, DHL, Palmyra Aviation Advisors and CoESS partnered up to produce two web-based modules aimed to the transportation ecosystems, such as aviation, and transposable to other critical infrastructure environments, such as energy. The project lasted two years and its deliverables have been made available just before the end of 2018.

The team organized fourteen workshops and digested a vast number of documents, books, and manuals into two simple and easy to use modules. The first one is an awareness module, aimed to any worker and employee working within or with a CI. The second one is a thorough Insider Threat policy builder aimed to executives who need to build their own Insider Threat Programme from scratch. Some templates are also available, as well as a downloadable PDF manual to make these Executives’ work as easy as possible.

Multiple protection purposes

The ultimate goal of Help2Protect is to engage all stakeholders to protect themselves, their colleagues, their company and the infrastructure they work for. The Help2Protect modules are designed to make sure that the Critical Infrastructure are able to function smoothly, without unwanted disruption and are well protected for the good of society. This implies spotting and stopping those who seek to harm them before it is too late.

The modules have been designed by Splintt, a Dutch eLearning company and are hosted here: https://help2protect.info

Information about the project and its partners can be found here: https://help2protect.info/wp-content/uploads/2018/12/coess_background-information.pdf

For any further information or queries, please contact us at Help2Protect@coess.eu

16th-18th Sept 2019 | Milan Italy

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

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

SAVE THE DATES

Italy faces some of the most challenging natural threats in Europe.

In western Europe, the region with the highest seismic hazard is the mountainous backbone of Italy, the Apennines. It has a long record of earthquakes spanning back to Roman times.

But recent earthquakes have been some of the most dramatic. In August 2016 there was a 6.2-magnitude earthquake near Amatrice that killed more than 250 people. That was followed by a 6.1 earthquake, which struck Visso on 26 October. Four days later, the village of Arquata del Tronto was destroyed by a 6.6 earthquake. Scientists predict that more earthquakes are highly likely.

In southern Italy the highly populated city of Naples is located near Vesuvius and within the larger caldera volcano Campi Flegrei, and some scientists are warning that Campi Flegrei is showing signs of activity that could mean that an eruption. This is on top of the active stratovolcano of Mont Etna on the island of Sicily.

In October 2018 severe storms caused widespread and severe flooding across Italy causing numerous casualties.

In addition to natural threats Italy along with Greece has borne the brunt of mass migration into Europe, which places stress on and poses security threats to its critical national infrastructure.

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

We look forward to welcoming you on 16th-18th September 2019.

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

To discuss exhibiting and sponsorship opportunities contact:

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

Sam Most - (Mainland Europe (excluding France), Turkey & Israel)
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

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

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

www.cipre-expo.com

Leading the debate for securing Europe's critical infrastructure

Owned & Organised by:

Supporting Organisations:

Media Partners:

S&T is Delivering Emerging Smart Cities Technologies to First Responders, Industry

In large and small communities across the country, emergency responders, commercial infrastructure building owners and operators have a common objective: public safety.

As smart phones, devices, and sensors evolve to allow for more interconnectivity, communities are becoming more resilient, allowing for earlier and improved alerts, warnings and notifications. The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) is bringing key industry and government partners together to ensure Smart City and IoT technologies are integrated and applied to meet critical infrastructure needs and the first responders.

S&T established the Smart City IoT Innovation (SCITI, pronounced 'CITY') Labs in collaboration with the Center for Innovative Technology, TechNexus and Smart City Works to focus on applying new and existing technologies to public safety needs, with an emphasis on extensive validation and go-to-market support through industry partners. In its first year, the SCITI Labs partnership funded development and initial testing of several prototype technologies in three overarching program areas. Moving forward, the ultimate goal is to make Smart City and IoT capabilities commercially available for industry, public safety and national security partners by 2020.

Laying Groundwork for Prototype Development and Operational Testing

After a highly competitive selection process, 12 performers were awarded funding to develop initial prototypes of unmanned aerial systems (UAS), in-building sensors, and a sensor and communications SmartHub. SCITI Labs, managed by DHS S&T's Jeff Booth, identified new and existing public safety technologies in these areas, assessed prototype capabilities and gained end-user and stakeholder input—particularly from industry partners who are critical to bringing these tools to market.

"We are looking to integrate and advance existing technologies applied to new challenges faced by first responders and the critical infrastructure commercial industry," said Booth of the initial awards and resulting prototypes. "If we can address the commercialization hurdles, then adoption by both the responder and real estate communities will be more likely."

In June 2018, the 12 SCITI Labs performers began work on prototype technologies in the three capability areas, which were selected based on emergency responder operational needs. Booth explained that for the work related to UAS, focus remained on indoor search and rescue, where missions in difficult environments—such as tunnels or collapsed or damaged structures—are difficult and endanger responders and those they aim to rescue.

For the in-building sensors, performers focused on developing intelligent suites (digital imagery, video, thermal or Wi-Fi finder) that can be mounted on fixed indoor building features, such as smoke detectors or exit signs. This will allow building operators to improve day-to-day operations and first responders to rapidly prioritize search and rescue areas when emergencies occur.

Finally, for efforts related to creating a SmartHub, performers focused on developing a body-worn responder interoperability platform that integrates personal area network communications with third-party sensor packages. The SmartHub will enhance emergency responder situational awareness and support enhanced mission-critical operations.

Industry and End-User Engagement Fosters Innovation and Technology Adoption

Throughout this first phase, S&T and SCITI Labs ensured each of the technology providers have market access and development capital and that their technologies align with commercial opportunities in broader infrastructure-related industries. To achieve this, the partners work hand-in-hand with industry to identify the best business approaches for transitioning these technologies into daily use.

Ronald White from the Boston Fire Department expressed why Boston is involved with SCITI Labs when he said, "For us, it's the ability to see what's on the horizon. To see what people are looking at developing in order for us to have an easier job doing what we do. It's incredible what is out there and the amount of data we can accumulate and how people can give it to us in different ways to improve the way we do our job."

The relationships built with these stakeholders are critical to the success of the SCITI Labs effort, as they will ultimately own the environment in which these technologies operate and will foster adoption by emergency responders.

In July 2017, SCITI Labs held an industry and end-user technology showcase in Chicago to introduce the technology providers to private sector partners and first responders in order to validate capabilities and work together to guide development, adoption and commercialization strategies.

The 12 performers incorporated feedback gathered in Chicago into final prototypes, which were then tested at the SCITI Labs Developmental Test and Evaluation (DTE) Event in October 2018 at the Texas A&M Engineering Extension Service (TEEX) using simulated search and identify scenarios to ensure they meet the needs of public safety stakeholders. The stakeholders were also on hand to provide feedback about how each of the technologies will contribute to daily and emergency operations.

Booth explained that the results and findings of the DTE will inform the selection of Phase II technology performers. Feedback from stakeholders will be used to refine the activities and objectives of Phase II operational tests and commercialization activities.

Initial SCITI Labs Successes

The DTE provided a key platform for the technology performers to demonstrate the applicability of their technologies to public safety operations and the potential overall impact, such as improved first responder efficiency and situational awareness.

For instance, during a simulated search and identify scenario, responders were able to adjust baseline operating procedures using the information provided by SCITI Labs technologies—changing the building ingress point based on video data, donning protective gear outside instead of inside because of a gas sensor reading or modifying clearance patterns based on sensor detection of individuals inside buildings.

More specifically,

· SmartHub performers were able to demonstrate GPS location, physiological sensors, hands-free communication and video streaming. The critical aspect of the SmartHub technologies was the ability to seamlessly move and share information up and down the chain of command.

· In-building sensor performers demonstrated the ability to connect disparate capabilities in very short periods of time, providing interoperability and timely information to inform decision-making.

· UAS performers demonstrated capabilities for mapping interior spaces using LiDAR and sonar capabilities. The ultimate goal of the UAS performers is to develop automated flight capabilities for degraded and confined spaces.

While the SCITI Labs technologies are at different stages of product maturity, a number of the technologies funded in Phase I have already demonstrated impact in the market and to the public safety community.

Operational Testing and Technology Transition

The second phase of the SCITI Labs initiative will launch in early 2019 with a more focused scope. Half a dozen performers will be selected to receive funding to execute additional product enhancements and operational tests with DHS Components, responders and industry stakeholders. S&T and its SCITI Labs partners will work with performers to bring the technologies from prototype to market-ready and to develop commercialization and adoption strategies.

A New Approach to Digital Maps & Geospatial Data

Has the time come for rethinking processes, workflows and tools in order to leverage the massive amounts of geospatial data available? And how do we ensure that all this geospatial data can become the foundation from which the majority of geospatial 2D and 3D maps, charts and simulation databases are produced?

> “People used to derive data from maps, now they derive maps from data”
>
> *Dr. Mike Tishcler - Director National Geospatial Program, US Geological Survey, GEOINT & Open Source Analytics Summit*

We are witnessing an explosion in the amount of geo-located information collected on a daily basis. In fact, there is more geospatial data being collected now than ever before. In just five years, there is likely to be a million times more geospatial data than we have today.

One. Million.

Why does this matter? And how did we get here?

You Are Here

Historically, many different governmental organizations have been building maps, charts and simulation databases based upon perceived differing collection and exploitation requirements. For example, the maps produced by the military to plan an offensive, would not necessarily be useful to first responders dealing with a crisis.

Today, many governments have central, dedicated mapping or geospatial organizations responsible for collecting, processing, validating and curating geographical and geo-localized information. These organizations often strive to provide the vast majority of all geographic data necessary for government use and thus tend to work in a centralized approach, which can sometimes lead to delays and data access restrictions due to national security reasons. Consequently, individual defense, intelligence and security agencies seek more independence from these central geospatial agencies in order to gain agility, autonomy to reduce the time between the collection and exploitation of geospatial data.

More Data. More Problems.

> "To manually exploit the imagery we will have over the next 20 years, we would need eight million imagery analysts. Even now—every day—in just one combat theater—with a single sensor, we collect the data equivalent of three NFL seasons in high definition"
>
> *Robert Cardillo, Director, United States National Geospatial-Intelligence Agency, GEOINT Symposium, June 5, 2017*

Whether it is sourced from satellites, drones, mobile phones, autonomous vehicles, open or commercial sources, or other means, the sheer volume of data is forcing agencies to rethink the way they produce maps, charts, simulation databases, and single or multi-source intelligence analysis material.

Agencies and organizations focused on security and defense – such as the Department of Defense, the Department of the Interior, Department of Homeland Security, and FEMA – traditionally employ a manual and siloed information/data storing technique when dealing with geospatial data. Traditionally, these silos, or stovepipes, were designed to provide very specific information for that agency's needs.

As the amount of geospatial data increases, and more demands are placed on these organizations, their inability to quickly adapt or scale their processes, or integrate new data or data streams makes them vulnerable to bottlenecks and inefficiencies.

However, this no longer needs to be the case.

From Months to Hours

The time has come to rethink processes, redefine workflows and seek new tools to enable and streamline the continuous consumption/ingestion of geospatial and sensor data to a centrally curated data repository. From this repository, agencies could very quickly generate and deliver nearly all geospatial 2D and 3D maps, charts, simulations, and derivatives to the point of need.

The benefits of this approach are multiple:

- **Increase in quality and accuracy:** through the fusion of multiple sources, maps can provide better situational awareness through access to the latest picture of the mission theater. For example, firefighters will have the most recent information to plan firebreaks, or FEMA can more accurately plan disaster assistance.

- **Faster production:** The application of these technologies will allow for augmented throughput of geospatial data and allow agencies to provide better quality of service to its stakeholders.

- **Less expensive:** This new approach requires less manual intervention, thereby permitting a strategic uses of your workforce. Additionally, the automation of tasks renders maps less prone to errors and ensures a more consistent quality.

By introducing and implementing cloud computing, computer vision, machine learning and artificial intelligence, the herculean task of quickly processing, ingesting, and transforming geospatial data into time-sensitive, useable, actionable intelligence is now possible. What used to take a large team of people several months to accomplish, can now be accomplished by a single computer in a matter of hours.

Leveraging Technology

In his GEOINT 2017 allocution, Robert Cardillo also stated: "We intend to automate 75 percent of the repetitive tasks our analysts perform so they have more time to analyze that last play and more accurately anticipate the next one. And then they can look much harder at our toughest problems—the 25 percent that require the most attention."

"VELOCITY responds directly to that challenge," says Stephane Blondin, Vice-President of Presagis. Presagis has over 20 years of experience providing geospatial processing tools and services to the defense and security simulation industry.

Presagis has developed VELOCITY, an automated solution supporting the continual production of 3D terrain and maps for use in defense and security personnel training, critical mission planning and intelligence analysis.

"By automating data cleanup and formalizing transformation processes, VELOCITY gives agencies and organizations the ability to produce 2D, 3D, or VR environments for a wide range of applications while providing traceability and repeatability. It also allows the drastic reduction – and sometimes the outright removal – of man-in-the-loop operations," adds Blondin.

Regardless of the solution or processes used, it is clear that the path forward requires the latest and best technology, tools, and architecture.

Cloud Computing

Given the unprecedented amounts of geospatial data now available, it is unrealistic to adhere to traditional storing and processing methods. Cloud computing allows for the storage of massive amounts of data and externalization of resources and also gives agencies the ability to massively scale-up operations when timing is imperative.

Additionally, a cloud computing approach facilitates the integration and deployment of large "System of Systems" and the integration of complex business processes based on a wide array of technology from a disparate set of vendors that can evolve over time. Companies such as Google, Microsoft and Amazon have paved the way to define technologies and software architectures that facilitate the integration of these System of Systems.

Computer Vision & Artificial Intelligence

Computer vision allows for the acquisition, processing, analyzing and understanding of digital images, and extraction of high-dimensional data – without a "human in the loop".

The combination of computer vision and artificial intelligence (AI) algorithms opens one of the most interesting avenues to automate the processing, integration and analysis of GEOINT data. Thanks to the massive storage and processing capabilities in the cloud, the field of machine learning is progressing more rapidly than ever and can automate numerous tasks once relegated to human, manual interventions. These tasks include:

- Digital Terrain Model (DTM) extraction
- Road network extraction
- Building footprints, height and rooftop extractions
- Vegetation extraction
- Land use classification
- Temporal change detection
- GIS data and sensor fusion

The Advantage of 3D

The dynamic nature of digital maps allows better tracking and measurement of changes in land use and land cover and, of course, a third dimension.

Aside from the obvious visual appeal of 3D representations, is there an advantage?

"Absolutely," says Blondin, "3D gives you the ability to represent and navigate complex datasets and concepts. Whether it be the trajectory of an aircraft, line of sights, electro-magnetic signals, or the verticality of a dense urban environment, 3D maps are extremely effective at helping visualize space and relativity in an intuitive and natural way."

Instrumenting 3D maps also opens the door for simulation. The instrumentation of roads and lanes allows the simulation of ground vehicles on streets, the identification of sidewalks and pathways permits the simulation of crowds, adding airport runways, signage and navaid let virtual aircraft take off and land, while material definitions of terrain and features allow physics-based sensor simulations, such as IR, or night-vision. The possibilities are virtually endless.

Next Steps

As the amount of geospatial and geo-located intelligence data explodes, national geospatial agencies need to consider bringing automation to the siloed and manual processes that exist today.

A convergence of cloud computing, computer vision, and AI in solutions like VELOCITY can accommodate the coexistence of both centralized and decentralized approaches while still converging towards an integrated geospatial system.

Through its ability to rapidly and continually combine and fuse GIS data into a central 3D geospatial data repository, VELOCITY is able to support the production of maps, charts, and simulation databases in days rather than months. Because of its modular open architecture approach, VELOCITY workflows can be customized to meet any specific need. By leveraging widely used and recognized automation technologies such as Python™ and HTCondor™, and by integrating market best solutions from the geospatial, simulation, gaming, architecture and entertainment industries such as GDAL, Terra Vista™, Unreal Engine™, CityEngine™ and Cinema4D™, VELOCITY promises important productivity gains through automation and scalability and the assurance of coherent situational awareness at the point of need.

All product names, trademarks and registered trademarks are property of their respective owners. Use of these names, trademarks and brands does not imply endorsement.

Fraud on the Tennis Court: Criminal Network Gained Millions Fixing Professionals Matches

An organised crime group involved in manipulating professional tennis competitions was dismantled in an operation led by the Spanish Civil Guard and coordinated by the National High Court of Spain (Audiencia Nacional), supported by Europol. In total 83 suspects were arrested, 28 of them are professional players.

The investigation was triggered in 2017 when the Tennis Integrity Unit (TIU) denounced irregular activities related to pre-arranged matches in the ITF Futures and Challenger tournaments. The suspects bribed professional players to guarantee predetermined results and used the identities of thousands of citizens to bet on the pre-arranged games. A criminal group of Armenian individuals used a professional tennis player, who acted as the link between the gang and the rest of the criminal group. Once they bribed the players, the Armenian network members attended the matches to ensure that the tennis players complied with what was previously agreed, and gave orders to other members of the group to go ahead with the bets placed at national and international level.

On the action day, 11 house searches were carried out in Spain in which €167 000 in cash was seized, alongside a shotgun, over 50 electronic devices, credit cards, five luxury vehicles and documentation related to the case. Furthermore, 42 bank accounts and their balances have been frozen.

Europol has supported the investigation from the beginning by providing continued analytical support. On the action day, three Europol experts were deployed to Spain to provide on-the-spot assistance including real-time cross-checks, IT forensic support, and data analysis during the operation. International police cooperation across the European Union and beyond is a crucial factor in the fight against sports corruption.

International Motor Vehicle Crime in Germany

Four arrest warrants were issued this morning against two Germans, one Jordanian and one Polish national between the ages of 30 and 52. 18 search warrants in Berlin, Brandenburg and Lower Saxony against 16 other suspects were issued as well. As a result of the house searches, various pieces of evidence were confiscated, among which eight cars, a motorcycle, various data carriers, specialised tools for breaking into vehicles as well as cash and drugs. The operation involved around 250 police officers and was supported by Europol. Yesterday, investigators already arrested a 46-year-old suspended police officer, who is allegedly involved in the case.

The complex investigation was coordinated by a specialised Office for Organized Crime at the Berlin Public Prosecutor's Office. Overall 23 suspects of different nationalities were identified and accused of different crimes; among them theft, fraud, falsification of documents and violations of the arms act as well as bribery.

The investigations were initiated in November 2017, and revealed the registration of vehicles in addition to falsified Slovenian and Austrian documents as well as falsified registration certificates from Belgium, France, the Netherlands, and Sweden. The investigations covered various EU Member States (Austria, Belgium, France, Italy, Lithuania, Poland, the Netherlands, and Sweden) as well as Algeria.

Kenya hotel attack: INTERPOL deploys team to assist terror probe

INTERPOL has deployed an international team to Kenya to assist with investigations into the Riverside hotel complex terror attack which left at least 20 dead and dozens wounded.

The expertise provided by the Incident Response Team (IRT) includes disaster victim identification, cyber analysis to decrypt seized mobile phones and other portable devices, biometrics, explosives and firearms, as well as photo and video analysis.

The IRT was deployed at the request of Kenyan authorities and its specialists will carry out real-time comparisons against INTERPOL's global databases on evidence gathered from the crime scene.

“INTERPOL's role is to help coordinate the international investigative response in support of the Kenyan authorities as they investigate this appalling terrorist attack,” said INTERPOL Secretary General Jürgen Stock.

INTERPOL and UN join forces to counter exploitation of Internet for terrorist activities

INTERPOL and the United Nations Counter-Terrorism Centre (UNCCT), the capacity building arm of the United Nations Office of Counter-Terrorism (UNOCT), jointly conducted a workshop on “Enhancing Member State Capacities to use Social Media to Prevent and Counter the Foreign Terrorist Fighters Phenomenon”.

The three-day workshop brought together law enforcement officers and investigators from Iraq, Jordan, Lebanon, Morocco, Tunisia, the United Arab Emirates and Pakistan. The objective was to raise the understanding of the Foreign Terrorist Fighters (FTF) phenomenon, including the gender dimension and the importance of respecting human rights and fundamental freedoms while countering and preventing the phenomenon through the use of social media.

The joint INTERPOL-UNOCT/UNCCT workshop included practical exercises aimed at developing the ability of Member States to use information on the Internet and social media to counter the FTF threat. It focused on the role of law enforcement agencies to collect, analyse and share information found online, particularly on social media platforms, to assist in detecting, preventing, investigating and prosecuting terrorism-related crimes.

Integrity in Sport: INTERPOL and IOC collaboration in Qatar

INTERPOL and the International Olympic Committee (IOC) have conducted a joint workshop in Qatar to help develop a coordinated national approach on the integrity of sport.

With Qatar due to host major sport events including the 2022 FIFA World Cup, the two-day workshop was held in close partnership with the Supreme Committee for Delivery and Legacy of Qatar.

It brought together more than 100 representatives from Qatari law enforcement, government, sports bodies and the Olympic movement.

International experts from the United Nations Office on Drugs and Crime, Council of Europe, FIFA and the Athletics Integrity Unit reviewed and highlighted existing legislation, international instruments and best practices to protect the major sport events from competition manipulation and other breaches of sport integrity.

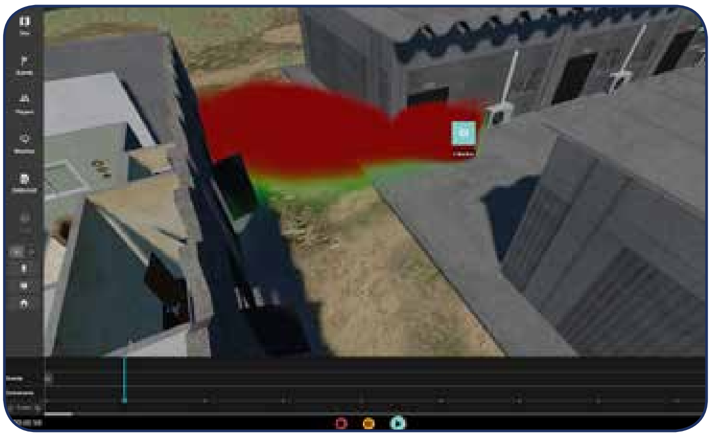
“Such initiatives aim at providing a safe environment for the management of safety and security operations in general and in major sporting events in particular. These workshops form part of a global capacity-building and training programme to help countries meet the new criminal challenges posed by competition manipulation, corruption and other threats to the safety of sport,” said Brigadier Ibrahim Khalil Al-Mohannadi, Head of Consultancy Office, Supreme Committee for Delivery and Legacy.

The event also provided an opportunity for INTERPOL to link up with potential new investigators for its Match-Fixing Task Force for the sharing of information, intelligence and best practices.

José de Gracia, INTERPOL Assistant Director, Criminal Networks Sub-Directorate said: “In recent years, the manipulation of sports competitions has become a mechanism for profit of organized crime structures. One of the key learnings of this training is that cooperation and information sharing is crucial. This is why stakeholders in law enforcement, government and sports have come together to discuss how we can build a global network to tackle competition manipulation.”

INTERPOL and the IOC recently expanded their joint global capacity-building and training programme until 2021 to protect the integrity of sports.

New CBRN Training Simulator for Military and First Responders



Bagira Systems and Van Halteren Defence (VHD), have won the Netherlands' Ministry of Defense tender to supply the simulator for their National Chemical, Biological, Radiological and Nuclear (CBRN) training center, and to maintain and operate it for a period of 15 years. The center provides education, training and support in the CBRN domain for both military personnel and first responders. The system will simulate, teach and train for various CBRN scenarios, ensuring mission readiness of all trainees' levels and responsibilities.

The new simulator is based on Bagira's unique highly realistic B-ONE 3D imagery software, which is the engine and at the core of Bagira's simulators. It includes various elements which together enable interactive training in a highly realistic and dynamic environment. With a special standardized skeleton and interchangeable animation, B-ONE flexibly, rapidly and accurately enables the creation and presentation of many different types of scenarios. By empowering the realistic nature of the simulated environment, B-ONE optimizes the training experience.

Using B-ONE the Bagira CBRN simulator realistically and dynamically simulates changing CBRN events, exercising all levels of command and all relevant functions involved to operate under changing conditions and environmentally effected situations.

Bagira's simulation accurately monitors the positions of each trainee at their physical location within the training area, and follows up on the individual's performance while identifying hazardous substances and reacting to changes at the scene and to threat evolvement. It allows after action review, feedback and lesson-learned assurance, and makes use of the latest versions of smart devices and applications for ease of operation.

"Awarded this project is yet another link in the Bagira's strong chain of unique training and simulation capabilities, and is a testimony to our precise adaptation of solutions to customer's needs", says Yaron Mizrachi, Bagira's General Manager. "This is the second system we shall supply to The Netherland's Ministry of Defense, following the Joint Fires Training and Exercise System (JFTES) to be supplied in 2019.

MARSS Secures Critical Infrastructure Protection Project

MARSS, NiDAR system has been selected to secure and protect a critical national infrastructure (CNI) site in the form of a major dam facility.

The NiDAR command and control (C2) system has been selected to integrate a thermal camera and a sonar system to protect the dam from potential underwater and surface approaches.

NiDAR is an advanced long-range surveillance system designed to protect maritime and land-based critical infrastructure from air, surface and underwater approaches.

NiDAR is systems agnostic, enabling it to integrate with any existing hardware or systems, and due to its modular design, not only does it meet the current contract needs, but it also offers the flexibility to meet any future expansions or requirements.

NiDAR can track, monitor, detect, classify, and respond to multiple objects, 360° in real time, of over 500 known and unknown, air, surface and underwater objects thanks to the software algorithms. It can intelligently analyse and rank unknown objects to determine potential threat levels and automatically trigger the appropriate alert. When the user determined warning and alarm zones are breached the system can automatically or manual deploy integrated countermeasures to deter potential approaches and de-escalate threats.

The intuitive C2 interface provides an enhanced awareness picture, in real-time, through a touchscreen user interface and multi touch control.

Rob Balloch, Sales Director of MARSS said, "NiDAR was chosen for this critical national infrastructure as it is robust and suited to all environments, however challenging.."

Globalstar Europe Satellite Services has announced that its SPOT X two-way satellite communications device is now available across Europe and North Africa

The latest generation of the popular SPOT family of products, SPOT X offers full two-way SMS and email as well as GPS tracking and a one-touch SOS button that instantly sends the user's GPS location to the GEOS International Emergency Response Coordination Centre (IERCC) over Globalstar's satellite network. The IERCC then transmits details to local first responders to dispatch help to the user's precise location.

SPOT X is the only satellite messenger on the market to give users a permanent phone number, easy check-in function and a full, backlit QWERTY keypad for intuitive typing. SPOT X also offers the industry's longest battery life in both tracking and SOS modes and is priced competitively.

While SPOT is primarily known for providing SOS and tracking for adventurers including hikers, sailors and paragliders, SPOT has been increasingly adopted by enterprises and non-commercial organisations to safeguard personnel working in remote or dangerous locations where mobile and radio communications are unreliable or non-existent.

"Staff welfare, as part of increasingly important employee duty of care initiatives, is high on the agendas of enterprises across many industries. We anticipate that SPOT X's two-way messaging will be enthusiastically received by businesses who understand the value of communicating with workers in the field, and giving them reliable, highly functional devices to improve safety," said David Phipps, Managing Director of specialist distributor, Global Telesat Communications.

"We believe that many individuals who already rely on SPOT to deliver added safety for their outdoor pursuits and adventures will be keen to take advantage of the new two-way communications options enabled by SPOT X," said Phipps.

"SPOT X is a true game-changer for safety and communications for any user whose business or leisure activities takes them beyond the reach of traditional telecoms networks," said Mark O'Connell, General Manager of Globalstar EMENA. "With an increasing number of third-party applications now integrated with SPOT, delivering added value through customised mapping and data management, organisations can now better protect employees as they perform their roles even in the most isolated or hazardous locations."

ODSecurity Announce New Contracts of SOTER Body Scanner at Chilean Customs

ODSecurity has announced a new contract to supply an unspecified number of their SOTER RS Body Scanners to Chilean Customs

The SOTER RS will increase the level of security operations for Chilean Customs not previously possible using conventional metal detectors. Non-metallic objects hidden under clothes, in natural cavities or within the human body cannot be detected by conventional metal detectors and typically, these non-detectable items, such as narcotics, explosives, precious stones, plastic weapons, or other contraband, can only otherwise be detected by highly intrusive total body searches.

The SOTER RS is a low dosage body scanner, that combines ultra-low radiation with maximum visibility. It is compact and extremely user-friendly: there is no need for extensive training. The high quality scan image is achieved with a minimum amount of radiation which is not harmful and will provide immediate results detecting any foreign material being smuggled.

SOTER RS is successfully deployed in correctional facilities, in airports, detention centres, police and customs facilities worldwide including; Australia, Denmark, Ghana, Hong Kong, Kuwait, Malaysia, Mexico, Nigeria, The Netherlands, The United Arab Emirates, The United States of America, The United Kingdom, Chile, Sri Lanka and Vietnam.

Detect-and-avoid radar to improve air traffic safety

The sensor solutions provider HENSOLDT has successfully concluded flight tests with its collision avoidance radar system for UAVs or drones. This sensor is intended to improve safety in both military and civilian air traffic.

HENSOLDT has developed a demonstrator of a so-called detect-and-avoid radar system, which uses the latest radar technology to detect objects in the flight path of a drone and to give early warning of any threat of collision following precise evaluation of the flight direction. At the same time, the sensor also assumes all the functions of a weather radar system.

In the flight tests, which were carried out on behalf of the German procurement authority BAAINBw and in collaboration with the German Aerospace Center (DLR) in Brunswick, the radar demonstrated its capabilities in a real setting, thus confirming the results previously achieved in ground tests. In test flights lasting several hours, the radar installed in a Dornier Do 228 belonging to the DLR reliably detected the test aircraft approaching at different altitudes and angles.

The detect-and-avoid radar system uses state-of-the-art AESA technology (Active Electronically Scanned Array), which allows several detection tasks to be carried out at the same time and enables objects to be detected extremely fast. It replaces the pilot's visual assessment of the situation. Thanks to its excellent detection capabilities, the multifunction radar is equally suitable for both military and civilian UAVs, e.g. for the delivery of cargo. A second series of flight tests is planned for the coming year.

Apstec's Human Security Radar to Enhance Security at Turkey's Esenboga International Airport

Late last year Apstec Systems™ announced that its Human Security Radar® (HSR®), has been selected by Esenboga Airport, Ankara, to significantly boost security in land side areas. Chosen following a rigorous selection process, including a pilot installation, HSR will be installed at the terminal entrances as part of ongoing security enhancement measures by the Turkish State Airports Authority. It will enable people screening without slowing down the flow of traffic, with each system capable of scanning up to 10,000 individuals per hour. The technology was deployed in partnership with local distributer AKBA.

The devastating attacks on Ataturk Airport in Istanbul and Brussels Airport highlighted the vulnerability of the land side of airports to terrorism. Since these events there has been global interest in securing the land side of airports, but traditional aviation style security checkpoints or manual searches, which scan one individual at a time, are not suited to purpose and result in large queues of passengers, which are vulnerable to attack in their own right. With existing approaches to security screening providing impractical, inconvenient and expensive to operate, terminals have remained susceptible to attack, or are subject to intrusive and disruptive security screening regimes.

HSR® was designed to address this challenge, and offers a practical and cost-effective solution to security screening in such high footfall scenarios. The first fully automated, real-time mass screening solution, HSR ® provides seamless security to protect public places from terrorist attacks. The walkthrough system uniquely combines unparalleled high throughput, speed and accuracy, simultaneously screening multiple subjects in real-time for threats, without the need for an operator to inspect suspect materials. With 40,000 passengers traveling through Esenboga Airport every day, the deployment of HSR will be instrumental in improving security for millions of people.

Esenboga Airport's uptake of HSR is the latest major deployment of the technology, which is currently utilised by some of the world's largest airports, as well as sports stadiums, entertainment venues, mass transport hubs and networks, places of worship, hotels and high-end retail and entertainment centres.

Openview and Bold Announce New Technology

Bold Communications, a leading developer of alarm communications and management systems, has announced a new technology partnership with Openview Security Solutions, the UK'S largest privately owned independent security company and provider of integrated control room systems. The two companies already have a proven track record of working together on a number of high profile public sector projects including Loughborough University, Stockport Homes and the City of Cardiff. This new partnership will enable clients, particularly in the public sector, to take advantage of the significant expertise and capabilities accumulated by both companies over many years in the deployment of innovative alarm and CCTV-based security systems that deliver best value.

Bold Communications Managing Director, Brian Kelly, commented: "Combining OpenView's project delivery expertise with Bold's specialised development and support skills will help to de-risk installations and ensure that control rooms deliver the highest level of service."

The monitoring sector has evolved significantly in recent years away from just simple alarm receiving and toward complete remote management solutions. The monitoring platform is now the central receiving and processing point for a wide range of security products and applications including fire and intruder alarms, public address systems and CCTV networks. The increasingly complex nature of such integrated systems demands the highest level of technical skills and resources making the relationship between software suppliers and systems integrators more important than ever.

Anti-Drone Sheild, Test in the Most Complex Environments

The presence of drones recently forced the closure of Gatwick airport for three days, suspending 1,000 flights and disrupting the plans of about 140,000 passengers during Christmas, and Heathrow for one hour. Indra is one of the few companies in the world that has a comprehensive solution specifically prepared and tested to protect an airport or any other space against drones flying without authorization.

It is an intelligent shield, called ARMS (Anti RPAS Multisensor System), which detects the presence of drones kilometers away, identifies the model and learns their weaknesses to neutralize them if they invade the space to be protected.

The company has tested its solution in countries where this type of threat is much more common and dangerous than in Europe. The extraordinary results obtained have made Indra one of the first companies in the world to have signed firm agreements with government clients, after meeting highly demanding criteria.

The situation experienced by London airports is not new. In August 2017, Arlanda airport, in Stockholm, was also forced to close for the same reason for one hour. Pilots from all over the world regularly report cases of lesser severity but that generate excessive uncertainty to the aeronautical sector, which historically has been obsessed with safety.

However, the risk affects many other areas and types of facilities. Industrial plants, nuclear power plants, infrastructures, official buildings, prisons, sport stadiums or any place where a public event is held face the same problem.

A drone can be used to invade the privacy of people, spy, perpetrate an attack, or simply cause an accident unintentionally, when colliding with a vehicle or person.

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.

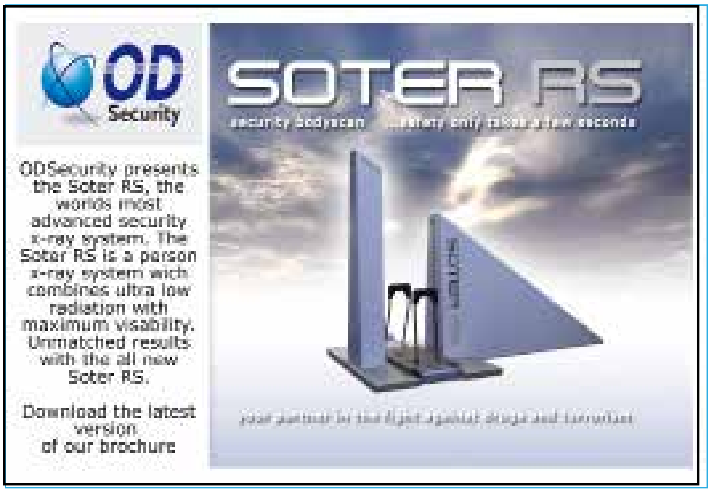
Discrete tracking devices for personal protection and vehicle security.

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

In use by Police, Military and Government organizations worldwide.

Border Security Report

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


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

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

Download the latest version of our brochure

Wagtail International leading specialists in detection dogs and dog handler training

Click here to view our profile

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

February 2019

2-9
SANS Security East
New Orleans, USA
www.sans.org/event/security-east-2019

12-13
European Information Security Summit
London, UK
www.teiss.eu

26-28
Secura North Africa
Algiers, Algeria
securalgeria.com

March 2019

5-6
Security & Counter Terror Expo
London, UK
www.counterterrorexpo.com

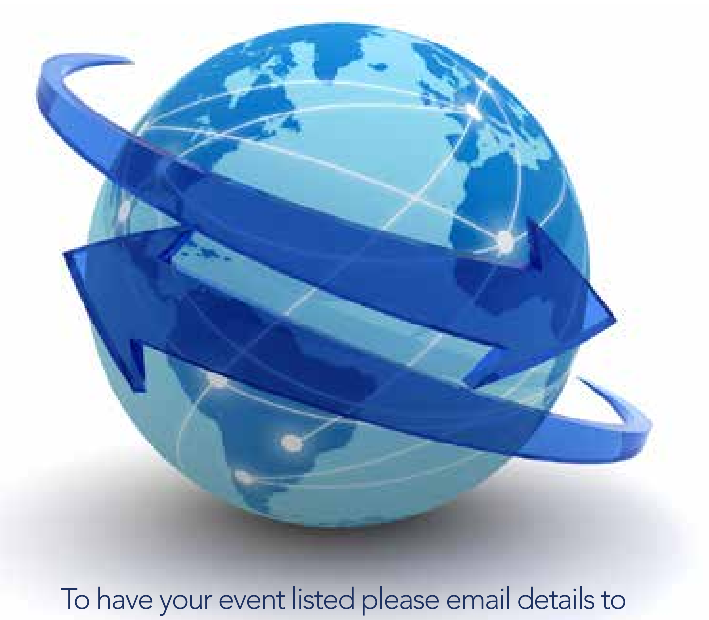
5-7
Security & |Policing
Farnborough, UK
www.securityandpolicing.co.uk

6-8
SECON
Seoul, Korea
www.seconexpo.com

19-21
World Border Security Congress
Casablanca, Morocco
www.world-border-congress.com

April 2019

9-11
The Security Event
Birmingham, UK
www.thesecurityevent.co.uk



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

May 2019

7-9
Critical Infrastructure Protection & Resilience North America
Tampa, Florida, USA
www.ciprna-expo.com

21-23
Behavioural Analysis
Minneapolis, USA
www.behaviouralanalysis.com

September 2019

16-18
Critical Infrastructure Protection & Resilience Europe
Milan, Italy
www.cipre-expo.com

ADVERTISING SALES

Sam Most
(Mainland Europe (excluding France), Turkey & Israel)
E: samm@torchmarketing.co.uk
T: +44 (0) 208 123 7909

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

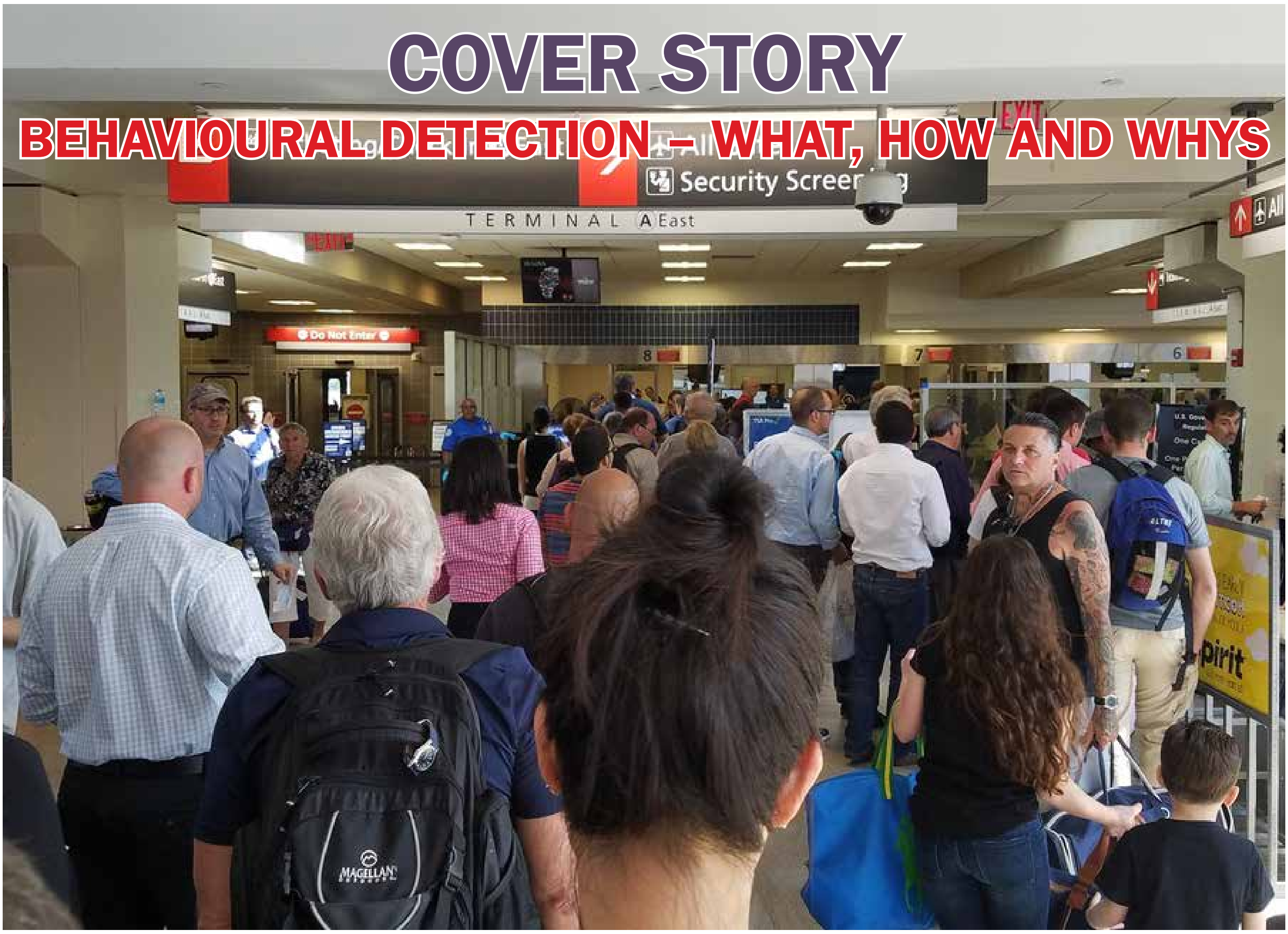
BORDER SECURITY REPORT

VOLUME 13
JANUARY / FEBRUARY 2019

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

COVER STORY

BEHAVIOURAL DETECTION – WHAT, HOW AND WHYS



SPECIAL REPORT

Increasing the Collection and Use of Passenger Data and Biometrics p.12

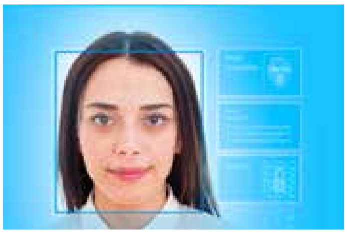
AGENCY NEWS

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

SHORT REPORT

WCO publishes new tool to assist countries in the prevention of illicit trafficking of cultural heritage p.4

INDUSTRY NEWS



Latest news, views and innovations from the industry. p.29

CONTACTS

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

Assistant Editor:
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.

Crisis, What Crisis?

It is rare that an issue of this magazine passes without 'Borders' being top of the news and political agenda, and this months issue is no exception.

In the US, the government shutdown over funding for President Trumps wall rumbled on for over a month and has only been temporarily suspended with a climbdown by President Trump. But the issue of the border wall is not going away and the Democrats, not wanting to look weak on immigration, are looking about ready to fund a dramatic increase in border security, which may include some sort of border barrier. This is despite the fact that many commentators would say that, with illegal crossings at record low levels, there really is no border crisis at all.

In the UK we had a border 'crisis' in the Channel that prompted the return of the British Home Secretary from a holiday in South Africa, to handle the situation personally. Whether there really is a 'crisis' in the Channel or not, the net result is more UK/French co-operation in the form of a joint intelligence centre, which can only be good.

Then of course there is the so called 'Back Stop' agreement on the border between the Republic of Ireland and Northern Ireland (UK), which is the chief sticking point in the ongoing UK/EU Brexit negotiations. Clearly, a hard border within the island of Ireland is in nobody's interest, so why is it so difficult to resolve?

What these crises have in common is that they are much more to do with politics and politicking than they are to do with any real security situation on the borders. A workable solution in each case is entirely doable, whether that's a soft (tech) border or hard border, with a wall or without.

All that is really required is a level of political will and co-operation that unfortunately remains elusive. After all, it was the migrant crisis that gave rise to the sort of populist politics that makes anti-immigration central to their reason for being and forces mainstream parties to follow their lead.

So, don't hold your breath for real solutions anytime soon!

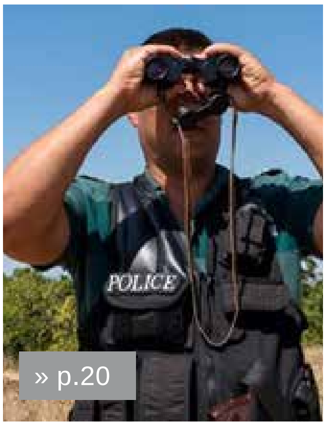
Tony Kingham
Editor

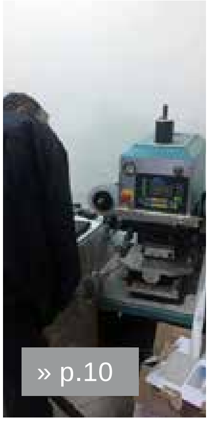
READ THE FULL VERSION

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





WCO publishes new tool to assist countries in the prevention of illicit trafficking of cultural heritage

The WCO has published its Training Handbook on the Prevention of Illicit Trafficking of Cultural Heritage (PITCH). It is a unique specialized tool, aimed at improving the knowledge and know-how of Customs officers deployed in the field, and goes hand in hand with a training programme.

The catastrophic events affecting - and continuing to affect - the North of Africa, Near and Middle East and the West and Central Africa regions, besides causing great suffering and loss of life, have had dire consequences on major cultural heritage sites. Trafficking of cultural objects has gained the attention of senior policy makers and law enforcement officers around the world, particularly due to its links with money laundering and terrorist financing. Growing political awareness of this illicit trade has led to the adoption by the United Nations Security Council of specific Resolutions addressing this problem, including UN SC Resolutions 2199/2015 and 2253/2015. Similarly, at its annual Council Sessions in July 2016, the WCO Council (then representing 180 Customs administrations) unanimously adopted a Resolution on the Prevention of Illicit Trafficking of Cultural Objects, which calls for greater vigilance and commitment in preventing this type of trafficking.

WCO Members agreed to strengthen their efforts to address this issue, but also asked for the development of specific tools to help them do so. That sentiment is echoed in UN SC Resolution 2347/2017, which calls for the WCO, along with other partner organizations, ''as appropriate and within their existing mandates, to assist Member States in their efforts to prevent and counter destruction and looting of and trafficking in cultural property in all forms''.

The WCO will only deliver the Handbook to Members through the deployment of face-to-face training which can be tailored to the needs of every region, thanks to the gap analysis workshops conducted prior to the deployment of the tool. The PITCH training programme focuses on Customs techniques, but also includes modules delivered by experts from the museum community, academia, Ministries of Culture and the Police, with the objective to ensure that all those involved in countering illicit trafficking in cultural objects adopt a consistent and harmonized approach, and coordinate their actions.

The WCO started conducting training on this subject in 2017, beginning with countries in the North of Africa, Near and Middle East region that met in Beirut, Lebanon, and with members of the Container Control Programme's Port Control Units, who met in Amman, Jordan. PITCH Training for the Customs administrations of West and Central Africa is planned for December 2018.

''I am delighted that the WCO has been able to step up its game and respond to this global threat in a very efficient and concrete manner, by providing operational support and training to its Members. While we have done a great deal on the awareness-raising front, what really makes the difference is practical application on the ground – and this is what we aim to do through PITCH training. The Handbook is our tangible contribution to implementing UN SC Resolution 2347/2017, as well as the WCO Council Resolution of 2016, and we hope that it will be used to improve the operational reality of our Member Customs administrations'', said Dr. Kunio Mikuriya, WCO Secretary General.

The WCO thanked all those who have supported and provided input into developing the training modules underpinning the PITCH Handbook, namely : the French Customs Administration, United States Customs and Border Protection (CBP), United States Immigration and Customs Enforcement (ICE) Homeland Security Investigations (HSI), the Dutch Ministry of Culture, Helicon Conservation Support, the French Ministry of Europe and Foreign Affairs, the French Embassy to Libya, INTERPOL and the UNESCO Regional Office in Beirut (Lebanon).

BEHAVIOURAL DETECTION – WHAT, HOW AND WHYS

Article courtesy of Baseline Plus Limited, for more information please contact info@baseline-plus.com

For the majority of people the most important thing in their life is family, so let's look at things from that perspective. Top of the list would have to be the family home. So how do you protect your home from threats? Well the most common security feature would be a locked front door and for a lot of people it stops there, but there are other options. Maybe a burglar alarm, but they're already in your house by then. You could get a big dog, but you'll end up being the one who always has to walk it. Perhaps you could build a six foot high brick wall circling your house, that would be pretty effective but it's not very welcoming to those who you actually want to visit. Ok so how about a passive infrared sensor light? One of those little lights that comes on when people step onto your property. You can't cover your whole house in the things, well you could, but it wouldn't be a level approach. So perhaps just one or two, intelligently placed. People can still approach and of course could walk straight past and continue on regardless, but that's one of the benefits. If you're a welcome visitor, such as the postman, then you would probably appreciate the light helping you find your way. However, if you're there for less honest purposes then the last thing you want is a light shone on you, drawing attention to what you're doing.

Now let's move the idea into the world of border management and critical infrastructure protection. At an airport for example, central search areas with their x-rays and metal detectors are the locked front door. Again, a brick wall is no good so having something that can shine a light on those with hostile intent whilst not negatively impacting those you welcome to your site is ideal – that's where behavioural detection comes in.

A specialist skillset available to security professionals and control authorities whose aim is to deter, detect or deny individuals who may pose a security threat. Behavioural Detection is a method of observing individuals for the purpose of identifying those displaying physical signals, which indicate an individual may have hostile intent

Simply by presenting themselves at a site or border crossing point, individuals offer an opportunity to recognise their intent and therefore a chance to promote the failure of their task by detecting their actions, denying them success in achieving it or deterring them from conducting it.

Through the practise of baselining, individuals trained in behavioural detection have the capability to recognise behaviours outside of the norm – that is to say above or below the baseline. This technique allows for the inevitable change in the behaviours baseline of an environment which would vary from location to location and across time periods. This permits operators to recognise that behaviours recognised as of potential interest in one situation are perfectly normal in another. An example would be the effects of a traffic jam on the main driving route to an airport which could be expected to cause the baseline of behaviours within the airport to raise due to the number of individuals running late for their flight. All perfectly reasonable behaviour.

In order to understand the reason for behaviours being shown, Behavioural Detection process leads the security professional to engage in a resolution conversation with the individual. Analysing an individual's personal baseline and response during a guided conversation, infused with elicitation techniques and all presented in a customer service delivery style (offering a positive effect on legitimate individuals) results in the behavioural detection practitioner having the necessary knowledge available when determining their next steps.

Let's go back to our house. We've added the PIR light, we could tell our neighbours about it. Like a neighbourhood watch scheme, we're not asking them to become police but just to be aware of what's going on around them. What's the down side? You have to say "good morning" to your neighbours when you see them!

As Head of Security, doing this at your site this creates a force multiplier. Whether it's airport check-in staff, a hotel doorman, the office receptionist, staff bus drivers, the list goes on. Everybody baselines, they know what normal behaviour looks like in their area of work, they get that feeling that something or somebody just isn't right. By giving them the confidence to believe in it and teaching how they can respond to it they become a vital part of the security team, helping to protect your site. After all, even if it turns out not to be of any concern then there are

many positives beyond security when your staff engage visitors or customers with a simple "Are you ok there?" or "How can I help you?"

A site where the workforce is aware and engaged, alongside a specialist team who are actively looking for behaviours every day, creates a challenge for hostiles that they really don't want. This would even help to deter the insider threat as they would recognise that you have created an environment that they find difficult or uncomfortable to operate in.

We're all well aware of the expense associated with new technologies and the relatively small scope of threats that each seeks to mitigate. This supports another positive for Behavioural Detection in that it is a long lasting tool which can assist in mitigating many different security threats. That's not to say technology doesn't have its place. In actual fact the developing thought process of combining the two, such as BDOs operating high footfall screening equipment is fast gaining recognition as best practise.

Behavioural Detection itself can't target a specific threat and that's a positive. If someone is up to no good then you don't want them doing it at your site. Whether it's theft at a shopping centre, ticket touting at a music venue or terrorism at an airport or train station, the emphasis is placed on identifying individuals who are looking to carry out an illicit action rather seeking to counter a specific threat.

The results of employing behavioural detection can be tangible such as an individual being arrested but equally it may never be known. So don't expect television documentaries about the CT plot you foiled as you may never know the good you've done. You can count how many times the light comes on, good practice would be to record the stops made by Behavioural Detection Officers, but this won't allow you to always label something a success or failure. You won't know how many and who you've deterred, sometimes even if you've spoken to them. However, the deterrent effect of such processes is an incalculable force.

By incorporating Behavioural Detection within a security strategy alongside other tools such a technologies, deterrent communications and a wider security culture with all individuals having a behavioural awareness, organisations can be considered to be offering an environment which is hostile to hostiles.

Defining and implementing Behavioural Detection against a backdrop of ever changing operational and commercial demands permits a high degree of security assurance, balancing an informed and pragmatic approach to mitigating multiple aspects of threat within the security environment.

If nothing else, I've talked myself into buying a light for the front of my house!

ePassport gates to open to visitors from Singapore and South Korea

Singapore and South Korea will be added to the list of countries whose nationals will be eligible to use ePassport gates to enter the UK from summer 2019, under plans announced by the UK Home Secretary.

The proposals build on those set out recently to allow nationals from the US, Canada, New Zealand, Australia and Japan to use ePassport gates, and demonstrate the government's commitment to develop a new global immigration system as the UK leaves the EU.

Criminal Gang Recruiting Portuguese Women into Sham Marriages Dismantled

An organised criminal group recruiting dozens of women into sham marriages was detected and dismantled by Belgian and Portuguese authorities, with the active support of Europol and Eurojust. Altogether 17 suspects were arrested today in Belgium and 3 in Portugal in an internationally coordinated action day.

The criminal group was involved in the facilitation of illegal immigration by organising sham marriages, predominately between Portuguese and Pakistani nationals. Portuguese women were recruited to marry Pakistani men they had never met and in return, received several thousands of euros. The couples then travelled to Belgium, where the wives were soon employed by (believed to be bogus) Belgian companies. By purchasing shares in the companies, this allowed the husbands to stay in the EU, obtain resident permits and then profit unjustly from social and other benefits. The shares were later transferred between the wives, allowing new recruits to become partners of the companies. The women usually travelled back to Portugal and would occasionally return to Belgium for police and immigration checks.

The investigation started in Belgium by the Belgian Federal Police in 2015 after authorities discovered a suspicious increase in the number of mixed marriage certificates in Ieper (Belgium). Due to the international nature of the crime, a Joint Investigation Team (JIT) was set up which culminated in a Joint Action Day .

International Drug Trafficking Between South America and Europe Disrupted by Police: 48 Arrested

Police officers from the Spanish National Police (Policía Nacional), together with the Argentine National Gendarmerie, the Italian Finance Corps (Guardia di Finanza) and Europol have dismantled a criminal organisation responsible for cocaine trafficking from South America to Italy and Spain. Almost 50 suspects were arrested thanks to this joint operation involving more than 750 police officers: 31 in Spain, 17 in Argentina and 3 suspects are under investigation in Italy.

This organised crime group was involved in the cultivation, sale and distribution of marijuana in the Costa del Sol region in southern Spain, and cocaine trafficking via maritime containers from Argentina, Bolivia, Colombia and Peru to Europe. The suspects, living in Argentina and Spain, were laundering money coming from the drug activities, sending it back from Europe to Argentina to then invest it into the property market.

The Argentine law enforcement authorities have had this international criminal group on their radar for the last decade. Since the start of the European investigation in 2017, the suspects moved more than two tonnes of cocaine: 1 200 kg seized by the Spanish National Police and 1 100 kg by Argentine National Gendarmerie when it was being transported from Bolivia to Argentina, destined to Europe..

EMPACT Joint Action Days Generate Big Results in 2018

In 2018 the Member States of the European Union joined forces with Europol and its institutional partners to fight organised crime groups active in the ten priority crime areas which fall under the European multidisciplinary platform against criminal threats (EMPACT). The outcomes of the Joint Action Days exemplify the tremendous impact that they had on some of the EU's most threatening organised crime groups.

2018 EMPACT Results:

1, 026 investigations initiated; Over €1.4 million in cash seized; 1,137 suspects arrested; 337 victims of human trafficking identified (including 52 minors); 730 kg of heroin seized; 207 firearms seized.

Europol's Executive Director Catherine De Bolle: "I am very pleased to see this year's results of the Joint Action Days 2018. They are more than just numbers and figures, as they clearly show how successful strategically planned international cooperation with strong partners can be.

Mauritania: Securing borders, building capacity

The arrest of an Iraqi citizen travelling on a stolen Danish passport has highlighted the importance of INTERPOL's policing capabilities to secure borders against people smuggling.

The man, who was arrested following a passport check against INTERPOL's Stolen and Lost Travel Document database, admitted to purchasing the stolen passport in Turkey, and was due to travel through Morocco on his way to Europe.

The arrest came as a direct result of INTERPOL's Smuggling Training Operation Programme (STOP), which helps frontline officers handle and recognize instances of document fraud and fight people smuggling.

The five-day STOP session, led by INTERPOL's People Smuggling unit, trained 20 frontline officers on key INTERPOL policing capabilities such as I-24/7, its secure communications network, databases, Notices and biometrics.

Detecting fake travel documents focus of INTERPOL training

Boosting border security in West Africa by developing its ability to detect and investigate counterfeit travel document crime was the focus of an INTERPOL course.

The three-day security training course, jointly delivered by INTERPOL's Counterfeit and Security Documents Branch (CCSD) and international digital security company Regula, enabled regional experts to examine new printing methods, latest document security features, recent document verification technologies and current examination techniques.

To strengthen the region's ability to detect criminals and terrorists at border control, the 6th joint CCSD- Regula Security Document Examination Training course gathered in Abuja 23 border control officers, security officials and forensic document examiners.

African Union agreement to boost fight against terrorism and organized crime

INTERPOL and the African Union (AU) have signed an information sharing agreement which provides a platform for cooperation with AFRIPOL in the fight against terrorism and organized crime.

Under the accord, AFRIPOL will have access to INTERPOL's nominal, stolen motor vehicles, and stolen and lost travel documents databases.

In addition, the AFRIPOL Secretariat will be able to exchange messages with National Central Bureaus in African region via I-24/7, INTERPOL's secure police communications network.

National Training on Behavioral Analysis and Identification of Foreign Terrorist Fighters (FTFs)/criminals at the airports, Podgorica, Montenegro

A national training course on behavioral analysis and identification of foreign terrorist fighters (FTFs) and criminals at airports for 24 border and customs officers from Montenegro's Podgorica and Tivat airports, the Civil Aviation Agency and the Intelligence Agency of Montenegro was held from in Podgorica.

Organized by the Border Security and Management Unit of the OSCE Transnational Threats Department, in co-operation with the OSCE Mission in Montenegro, the interactive course was conducted with the support of the Israeli National Police and the United States Federal Bureau of Investigation experts focused on profiling, controlled cognitive engagement, detecting deception and vulnerability assessments for better and easier detection of FTFs and other potential criminals at airports. Participants were engaged in practical exercises, using video materials and applying different interviewing techniques.

This activity is part of the OSCE Transnational Threats Department's project on airport security in Montenegro launched in co-operation with the OSCE Mission in Montenegro in 2017. This project aims to develop and implement the Border Community Security Programme of Montenegro, designed to improve information exchange and co-operation between law enforcement and private sector personnel. The aim of the project is to reduce the risk of criminal and terrorist acts, particularly those related to the cross-border movement of FTFs through Montenegro's airports.

OSCE trains border guards in Serbia on detecting forged and counterfeited documents

Border Security and Management Unit of the OSCE Transnational Threats Department in co-operation with the OSCE Presence in Albania and the Security Academy of Albania had organized a one-week advanced training course for 15 Albanian border officers from various regions of the country on increasing their operational awareness regarding the detection of forged travel documents. The training took place in Tirana. The training course provided the participants with up-to-date information on the latest trends in document fraud as well on the wide range of new security features available for travel documents.

During practical exercises participants learned how to use mobile document-checking devices and magnifiers to identify the main security features in passports, driving licenses and foreign banknotes. The OSCE also handed over 15 high-quality magnifiers to each participant with the aim of supporting the technical capacities of Albanian law enforcement personnel.

Study visit for members of the OSCE Gender Equality Platform

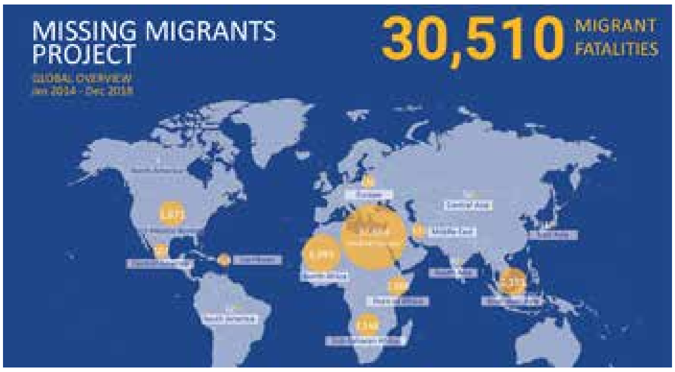
The BMU of the OSCE Transnational Threats Department organized a study visit for the members of the OSCE Gender Equality Platform in Border Security and Management with the purpose to expose the participants to best practices of promoting gender equality and mainstreaming in border and law enforcement agencies in Sweden.

The group was comprised of 11 border guards, customs service officers, and officers from the Ministry of Internal Affairs of the OSCE pS. During the visit, the participants discussed and debated: good practices on inclusive recruitment policies; mechanisms facilitating women's entry into workplace (border related agencies and security sector in general); preventing gender-related discrimination, harassment and abuse; addressing allegations; career development and promotion for women; women's peer-to-peer programmes, mentorship initiatives.

osce

Organization for Security and Co-operation in Europe

30,000 Irregular Migration Deaths, Disappearances Between 2014-2018



At least 30,510 people died during irregular migration between 2014 and 2018, the IOM Missing Migrants Project reports. More than 19,000 deaths and disappearances were recorded due to drowning, not only in the Mediterranean Sea, but also in the Rio Grande, the Bay of Bengal, and many other overseas routes.

Nearly half of the five-year total fatalities of at least 14,795 men, women and children were recorded on the Central Mediterranean route between North Africa and Italy. The Missing Migrants Project estimates that there were at minimum 17,644 lives lost at sea on all three trans-Mediterranean routes in the last five years, equivalent in these five years to roughly ten times the number of people who drowned when the luxury liner Titanic sank in 1912.

Deaths recorded during migration throughout Africa comprise the second-largest regional total of the 30,000 deaths recorded since 2014, with 6,629 fatalities recorded since 2014. Nearly 4,000 of those deaths occurred in Northern Africa, where a lack of reliable data and extensive anecdotal reports indicate that many more migrants have died than are recorded.

In Asia, where data are similarly scarce, the deaths of more than 2,900 people were recorded during migration, including 2,191 in Southeast Asia and 531 in the Middle East.

Continued Winter Assistance Needed for Displaced and Vulnerable Iraqis

As winter temperatures set in, accompanied by winds and rain, the International Organization for Migration (IOM) in Iraq has completed the three-month distribution of 25,000 winter non-food item kits. Consisting of heaters, blankets and jerrycans, the kits meet the most urgent needs of 150,000 vulnerable individuals across the country.

IOM's winterization assistance reached 13,000 displaced households in camps, thousands of displaced families in informal settlements, and thousands of others who have returned to their home communities.

Mediterranean Migrant Arrivals Reach 4,883; Deaths Reach 203

203
DEATHS OF MIGRANTS RECORDED IN THE MEDITERRANEAN IN 2019
59
2
142

The IOM reports that 4,883 migrants and refugees have entered Europe by sea through the first 20 days of 2019, a slight increase over the 4,466 arriving during the same period last year. Deaths on the three main Mediterranean Sea routes through almost three weeks of the new year are at 203 individuals, compared with 201 deaths during the same period in 2018.

At this point in 2017 a total of 3,156 migrants or refugees had landed in either Greece, Spain or Italy after crossing the Mediterranean, and IOM had recorded a total of 228 deaths.

IOM's Missing Migrants Project (MMP) reports that January 2019 marks the fourth straight year in which January has seen at least 200 migrants and refugees drowning trying to reach Europe via one of three Mediterranean Sea routes.

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

INCREASING THE COLLECTION AND USE OF PASSENGER DATA AND BIOMETRICS

In the second of this two-part series, Simon Deignan, Counter Terrorism Officer at Organization for Security & Co-operation in Europe (OSCE) and Thomas Wuchte, Executive Director, International Institute for Justice and the Rule of Law (IIJ) examine the impact of the increasing the collection and use of passenger data and biometrics.

Both commercial and security priorities have led to great technological advances being made at formal points of entry to facilitate bulk movement of travellers and to detect potential threats. Although the technologies exist, they were often viewed as nice to have rather than necessities.

UNSCR 2396 has changed that by mandating that all States collect Advance Passenger Information, Passenger Name Record, and biometric data.

Advance Passenger Information (API)

On 24 May 2014, four people were killed at the Jewish Museum in Brussels by a man armed with a Kalashnikov rifle. This man was Mehdi Nemmouche, the first Daesh returnee to carry out an attack in Europe. He managed to do so

despite being on several terrorist watch-lists. Because his data was not checked against these watch-lists before he travelled, he managed to fly back to Europe undetected.5 If his API data had been checked in advance against these watch-lists, he would likely not have been allowed entry.

But what is API? It is the biographic data contained in a passenger's travel document that is submitted to the airlines during check-in, as well as the flight information of that airline. When it is received in advance of a passenger's arrival it allows law enforcement authorities the time to do two things. Firstly, to check the name, date of birth, nationality and other travel document information in the MRZ (Machine Readable Zone) against watch-lists and databases. If the traveller appeared on one, like Mehdi Nemmouche, they would be stopped at the border for further questioning.

Secondly, it allows law enforcement authorities to compare the traveller's details against risk profiles. For example, a young male, travelling alone, with no luggage, from Algeria to Madrid via Kiev, would be more suspicious than an old French couple travelling to Spain for the weekend.

Put simply, API allows States to check travellers against known suspects and known risks, as well as unknown suspects and known risks.

API has been a global requirement since September 2014 when the UN adopted Resolution 2178 to prevent the movement of FTFs. Since then, ICAO, the International Civil Aviation Organisation, has established API as a binding standard, and many international and regional organisations are supporting States to overcome the technical, financial and legal issues to establish national API systems.

Passenger Name Record (PNR)

A second, more detailed type of border screening involves PNR, passenger name record data. This is the information a traveller gives to an airline when booking a flight – phone number, email address, home address, credit card details and so on. It is much more detailed information; hence there are more concerns regarding data privacy, particularly in Europe.

Although the information is not backed by a government-issued travel document, like API, PNR data can be very useful for intelligence, analysis and border security because it can identify suspicious travel patterns by examining what other flights that person has booked using that credit card. This can flag threats that otherwise might have escaped attention.

With the adoption of UNSCR 2396, all States are required to collect passenger data in advance and cross-check this information against watch-lists and databases.

Probably the most valuable use of PNR is to illuminate hidden connections between known threats and their unknown associates – the unknown unknowns. For example, if a flight for an unknown person is booked using a credit card that was previously associated with a known suspect – the person travelling immediately becomes a person of interest. Taking the example one step further, if that person uses a home address previously unknown to law enforcement officials, the other people living in that house may also be associated with a crime.

The United States Counter Terrorism Coordinator gives the real-life example of Faisal Shahzad. Faisal was a US citizen who had received explosives training in Pakistan. In 2010, he arrived at the US on a one-way ticket from Islamabad. He matched a PNR targeting rule based on his travel pattern, and so was stopped but subsequently released. Three months later, a car bomb failed to detonate in Times Square. Investigators linked Faisal to the car, through his credit card. An alert for him was placed in its system.

When he booked a flight to flee the country, the system flagged it.6 He was arrested and is now serving a life sentence.

Biometrics

In November 2017, US authorities arrested Naif Abdulaziz M. Alfallaj, a Saudi citizen residing in Oklahoma who trained with Al Qaeda in late 2000.

The FBI was able to identify the man when they matched his fingerprints

against those taken from an application form for the terrorist group's Al Farouq training camp that was seized in Afghanistan.7 Biometrics can be a valuable tool for verifying that individuals are who they say they are. Terrorists and organised criminals will try to mask their identities in several ways: whether by using a fake passport or taking on another identity. However, it is a lot harder to fake, for example,

fingerprints. Face recognition, eye recognition, fingerprints, all the way up to DNA – these are ways to identify someone using human characteristics.

The technology for biometrics already exists and is moving fast. The majority of countries in the world are now issuing biometric passports, which contain a photo and a fingerprint – when a traveller uses an e-gate, a live image of the traveller's face is compared with the photo in their passport. Apple uses fingerprint recognition technology in its iPhones, the United Kingdom uses fingerprints instead of library cards and even Disney World uses face recognition to ensure a three-day pass is not transferred to someone else. Some States have begun to collect fingerprints and facial scans of travellers to their country. This data can be used to validate the traveller's identity and their travel documents. Some States also have watch-lists with biometric data of known and suspected terrorists.

UNSCR 2396 mandates that all States "develop and implement systems to collect biometric data, which could include fingerprints, photographs, facial recognition, and other relevant identifying biometric data, in order to responsibly and properly identify terrorists, including foreign terrorist fighters". Most States do not yet have the capacity or the means to do this; therefore, assistance from both international organisations and other States will be necessary.

Data protection considerations

The routine gathering, storing and sharing of large amounts of the personal data of potentially everyone who travels across borders may have a substantial impact on the enjoyment of individual human rights of ordinary people too – their right to privacy and freedom of movement or even their right to liberty and security.

In accordance with international privacy and data protection standards, the collection, storing and processing of personal information must be prescribed by law, strictly necessary for a legitimate purpose and proportionate towards that purpose. The information gathered must not be used for other purposes than those for which it was collected; and the law must also provide for appropriate procedural safeguards against abuse.

For API and PNR, there is a human rights backstop in place, as airlines, European ones, will not send the data to a country that does not first have the correct legal provisions in place to safeguard data privacy. However, more work will be needed to ensure that biometric information is collected responsibly for counter-terrorism purposes as this effort expands.

Improving Our Sharing of Information, Both among States and within States

In the aftermath of the November 2015 Paris attacks, we learned that Belgian intelligence services had known about the jihadi backgrounds of Salah Abdeslam and some of his associates for some months before the attacks. Unfortunately, this information was not shared among other European intelligence services.8 Dealing effectively with transnational threats like terrorism requires constant cooperation and intelligence sharing between law enforcement authorities. This is the reason why UNSCR 2396 stresses the need to increase information exchange both within States and among States.

Inter-State information sharing

INTERPOL, Europol and many national and international law enforcement and border agencies gather, collate and disseminate a broad range of data relating to stolen and fraudulent travel documents, watch-lists of suspects, and notices requiring actions, ranging from reporting sightings to immediate detention of individuals. As with all forms of information, the data coming out of the system is only as good as that going in. If States are not populating these databases with relevant and up-to-date data, their usefulness is severely diminished. A second problem is that not all border control points have access to these databases – some INTERPOL members have previously had no connection at their air, land, and sea ports of entry to the Stolen and Lost Travel Document (SLTD) and other databases, potentially allowing known terrorists and criminals to travel more freely. 9 UNSCR 2396 also encourages States to share information through bilateral and multilateral mechanisms. The level of information sharing before and after the Paris attacks demonstrates the contrast in how effective the response can be. As pointed out above, the main protagonists were known to intelligence services beforehand, but this information was not shared outside of national borders. In contrast, after the Paris attacks, States actively cooperated and shared operational intelligence with one another much greater, leading to the arrest of many associates of the attackers across Europe.

Of course, this principle of sharing assumes that all States value privacy equally and do not misuse information to target individuals outside of the rule of law; and that information practices, including integrity, anonymity, and destruction as appropriate, are rule-of-law-based. In addition to sharing this information with one another, States need to ensure that appropriate safeguards against abuses in bilateral and multilateral information exchange and law enforcement cooperation are strengthened.

States should also put in place appropriate safeguards to ensure that information received from other countries has not been obtained in contravention of international human rights standards, and that information shared with other countries is not used for purposes that do so. Those who are arbitrarily included in terrorism watch-lists or databases will face serious consequences, including arrest and detention, when travelling across borders. Practice has shown that this is not a theoretical question; but remains a problem for too many human rights defenders, journalists, political activities and others who have been unfairly labelled "terrorists" by their governments.

Intra-State information sharing

Many State agencies still treat information as need to know rather than need to share. This results in multiple information silos where nothing comes in or out, leading to resource duplication and missed opportunities to identify potential terrorists. The US learned this after September 11 and progressed to a model where information is shared among a host of security agencies. Many European agencies are now following suit, although in most countries there remains more work needed to form interagency information sharing. Inadequate interagency processes severely impede a country's ability to provide frontline screeners and law enforcement agencies access to terrorism information, and to screen against this information and other key data at borders and ports of entry. Without such up-to-date operational information, a frontline border officer may allow the entry or exit of a terrorist being sought by another security agency.

In addition to information sharing between state agencies, we should look to increase information sharing with the private sector. In many countries the private sector owns and operates a vast majority of the nation's critical border infrastructure, such as information and communication technology (ICT), energy and traffic and transportation. There is then a further need to strengthen the sharing of best practices with the private sector on countering terrorism. Partnerships between the public and private sectors are essential to maintaining security and resilience. These partnerships create an environment to share critical threat information, risk mitigation, and other vital information and resources. In many countries, businesses have understood and taken responsibility for cooperating and collaborating with state security agencies. "Intelligence-derived knowledge shared more widely beyond intelligence circles" is one of the Step Changes highlighted in the UK Anderson Report.

Support and interaction among States, the public and private sectors, as well as international and regional organisations is paramount in tackling threats posed by terrorism. Recognising each other's roles and responsibilities and stronger collaboration will benefit all stakeholders in countering terrorism in all its forms.

Hong Kong police seize more than a tonne of illegal fireworks and firecrackers near border checkpoint

More than a tonne of illegal fireworks and firecrackers smuggled into Hong Kong from mainland China were confiscated by police in an outdoor container yard near the Lok Ma Chau border checkpoint in the run-up to the Lunar New Year.

With the help of a sniffer dog from the force's Explosive Ordnance Disposal Bureau, the HK$2 million (US$254,900) haul was found hidden in a shipping container at Ki Lun Tsuen off Kwu Tung Road, Lok Ma Chau.

Inside the yard, officers arrested a 62-year-old man on suspicion of possession of illegal fireworks and firecrackers – an offence which carries a maximum penalty of a HK$25,000 fine and six months in jail. He was in charge of the container yard, according to police.

Chief Inspector Lam Sze-yi of the New Territories North regional crime unit said the 1.1 tonnes of fireworks and firecrackers found in the operation was the largest seizure of this kind in recent years.

Plan de Choque makes it pay

In Development of the Plan de Choque, the one who makes it pay "More Close to the Citizen", the Department of Police Choco, in fulfilment of the National offensive against crime ordered by the president of the Republic and the General Direction of the National Police of the Colombians, in the framework of the Comprehensive Strategy against Narcotrafficking, the National Police through the Directorate of Anti-narcotics, Investigative Aircraft Unit, in coordination with the Colombian Air Force, the Antidrug Agency DEA and the Specialized Directorate against Narcotrafficking of the Attorney General of the Nation, obtained the seizure of 600 kilograms of cocaine hydrochloride, inside a private aircraft and the capture of 2 men of Colombian nationality, among them the pilot of the airplane.

The operation was carried out at the airport "Reyes Murillo" Nuqui Choco, the substance was hidden in suitcases destined for the country of Guatemala.

The captured were placed under orders from the Prosecutor's Office for their respective prosecution for the crime of trafficking, manufacture or possession of narcotics, as well as the aircraft and the substance seized.

Drug Around Columbia Simulated to be Ginger Powder

The Secretariat of Security and Citizen Protection reports that elements of the Regional Security Division of the Federal Police, deployed at the Guadalajara International Airport, Jalisco, secured a box containing 100 kilos of apparent methamphetamine.

The operation was carried out when the corporation's staff received a report that reported a box with unusual content, at an airport parcel company.

The items were moved to the place, where when opening the package, from Bogota, Colombia, they located four boxes inside that contained a green powder that simulated to be ginger. However, using a portable substance identifier in the contents of the boxes tested positive for methamphetamine.

Faced with a possible criminal act, the boxes, with a total weight of approximately 100 kilograms, were placed at the disposal of the Agent of the Public Ministry of the Federation in Guadalajara, Jalisco, where the investigations will be followed up and the weight and type of substance insured.

Celebrating 11 Years of AMERIPOL

AMERIPOL recently celebrated its 11th anniversary and has established itself as an effective hemispheric mechanism that serves the purpose of promoting and strengthening police cooperation in the field of information exchange, which contributes to the neutralization of transnational threats, capacity building and technology transfer.

AGENCY NEWS AND UPDATES

Federal Police, Border Force raids in Perth net 21kg methamphetamine haul

A drug bust in Perth has seized about 21kg of methamphetamine, worth about $19 million, which was concealed in an industrial oven.

Two men have been arrested over the bust and a third has been summonsed after Federal Police and Border Force officers raided several Perth properties.

The industrial oven the drugs were concealed in was sent to Perth from Canada in early 2019, according to Federal Police.

WA Police and the Australian Criminal Intelligence Commission assisted in the investigation.

The AFP says the methamphetamine seized has a street value of up to $19 million and the potential to produce 210,000 street deals.

Thai Police Investigation Reveals Cross Border Tiger Syndicate

New findings from a three-month investigation reveal professional gangs were dispatched across Thailand's borders to target the Kingdom's wild tigers.

The investigation was initiated after the successful arrest of two Vietnamese males by Thai Police following a tip-off from a Thai driver-for-hire.

The driver was traveling between the west-central towns of Tak and Pitsanalok Provinces. He considered the suspicious baggage belonging to two foreign customers, so he called the police. The police stopped the vehicle, inspected the bag, and discovered a fresh tiger skeleton inside. The police arrested the owners of the bag, took the suspects and tiger remains to the Nakorn Sawan Police station, and inspected the suspects' belongings, including their phones.

Vietnamese Poachers Recorded Their Kills of Wild Tigers in Thailand. Police then contacted Freeland for analytical assistance. Freeland's forensics experts were dispatched to the scene and provided on-the-job training. Using Cellebrite digital forensics technology, police found evidence that the poachers, originating from Vietnam, had crossed Laos into Thailand for targeted hunting inside Thailand's forests. The poachers documented their trips on their phones, including tiger kills.

Turkey to reaffirm priority of border security with actors in Syria

Ankara is determined to prioritize

Turkey's border security in enhanced diplomatic talks with the U.S. and Russia, aiming to avoid steps that would be advantageous for terrorist groups in Syria. With the U.S. decision to withdraw from Syria, the actors on the ground have been increasing their efforts to shape the upcoming period. Turkey has enhanced its talks particularly with the U.S. as it seeks steps that will eliminate terrorist threats along its borders. In order to reach its objective to ensure border security, Ankara has been focusing on a plan to set up a safe zone that is free from the PKK-affiliated People's Protection Units (YPG) along its borders..

Indian police arrest Rohingya group stuck at Bangladesh border

Police in India's northeastern state of Tripura have arrested 31 Muslim Rohingya who were fleeing a recent crackdown by India's Hindu nationalist government.

The group, which included 16 children and six women, was arrested after it was denied entry into Bangladesh and border officials from the two nations failed to agree on what to do with them.

India regards the Muslim-majority Rohingya as illegal aliens and a security risk and has ordered that tens of thousands of them who live in scattered settlements and slums around the country be identified and repatriated to Myanmar.

As many as 1,300 Rohingya have crossed into Bangladesh from India in recent weeks as fears of deportation to Buddhist-majority Myanmar sparked an exodus. .'

Video of drug bust as dozens of smugglers meet at Israel-Egypt border

Rare police footage broadcast by Channel 13 news this week shows an attempt to smuggle around 100 kilograms (220 pounds) of drugs into Israel across the Egyptian border.

The footage, captured in January 2018 but only made available for publication now, shows several dozen smugglers congregating near the border fence while, unbeknownst to them, an Israel Border Police force lies in ambush nearby.

The Egyptian smugglers place ladders along the six-meter high fence and begin throwing drug packages into the hands of the Israeli Bedouin smugglers waiting on the other side.

At that point, heavy fire is directed at the smugglers from the Egyptian side, possibly by Egyptian security forces. Israeli police officers then emerge from hiding and also begin firing. One Egyptian smuggler can be seen falling from a ladder after being shot.

The Israeli Bedouin smugglers load the drugs onto their vehicles and flee, with authorities giving chase.

The smugglers were eventually caught and arrested, and their drug haul was confiscated.

Lebanon arrests US man for crossing illegally from Israel

The Lebanese army says it has arrested a US citizen suspected of entering Lebanon illegally through a breach in the border fence with Israel.

The official National News Agency cited the army's directorate of intelligence as saying its officers were questioning the man.

He was found "hiding in one of the alleys in the city of Tyre", it added.

The militant group Hezbollah posted what it said was a photo of him at a clothes shop where he was arrested.

Honduran Border Police Arrest Organizer Of New Migrant Caravan For Warrant On Rape Charge

The new migrant caravan from

Honduras is off to a bad start after one of its leaders was arrested for having a rape warrant dating back to 2015.

Juan Molina, who was identified as one of the caravan's main organizers, was reportedly caught at a national police checkpoint and taken into custody.

The US President repeated his promise to tackle the issue of mass migration from Central America by cutting off funding to the countries that don't take action to stop new caravans from forming.

Meanwhile, Border Patrol agents at the Yuma sector are remaining busy as nearly 30 undocumented migrants required medical attention.

CBP's commissioner added, the agency is facing an "unprecedented crisis" that is putting "vulnerable populations" at risk.

Number of irregular crossings at Europe's borders at lowest level in 5 years

Last year the number of illegal border-crossings at Europe's external borders has fallen by a quarter compared with 2017 to an estimated 150 000, the lowest level in five years. The total for 2018 was also 92% below the peak of the migratory crisis in 2015.

The drop was due to the dramatic fall in the number of migrants taking the Central Mediterranean route to Italy. The number of detections of irregular crossings on this route plunged 80% compared to 2017 to slightly more than 23 000.

The Central Mediterranean route saw the smallest number of irregular entries since 2012. The number of departures from Libya dropped 87% from a year ago, and those from Algeria fell by nearly a half. Departures from Tunisia stayed roughly unchanged. Tunisians and Eritreans were the two most represented nationalities on this route, together accounting for a third of all migrants.

Indo-Tibetan Border Police wins ice hockey tournament in Ladakh

For the third consecutive year, the Indo-Tibetan Border Police (ITBP) has won the final match of Ice Hockey Tournament organised by Ladakh Autonomous Hill Development Council in Leh. Team ITBP defeated Skara in the final match by six goals to five to lift the running trophy for the third time.

BSF officer killed by Pakistani sniper firing

An assistant commandant of the Border Security Force was killed in sniper firing by Pakistan Rangers along the International Border in Jammu and Kashmir's Kathua district.

The BSF troops were carrying out border domination along the International Border, when snipers of Pakistan Rangers opened fire on them at around 10:50 hours in Hiranagar-Samba sector of Kathua district, a senior BSF officer said.

Border Agents Help Mexican Police Bust Human Smuggling Stash House

Border agents and Mexican police are working together to bust a human smuggling operation. A Guatemalan father and teen aged son caught by the Border Patrol in New Mexico told the agents about a stash house from where they had just escaped in Colonia Rancho Anapra right across the border from Sunland Park near El Paso.

A report says the agency then worked with Chihuahuan state police who found another immigrant locked in a stash house the smugglers were using in the kidnapping and entrapment of immigrants.

The smugglers were extorting the immigrants to force them or their families to make large payments in exchange for getting them into the United States.

Four arrested after $100 million of heroin and 'ice' seized

Four men have been charged following a joint agency investigation into the importation of more than 150 kilograms of heroin into Sydney via air cargo from Malaysia.

A consignment purporting to be gym

equipment and supplements arrived in Sydney from Malaysia.

The consignment, which was found to contain various handicraft items and timber souvenirs, was x-rayed by Australian Border Force (ABF) officers, who noted anomalies in the packed crates.

During a subsequent deconstruction of the consignment, 400 blocks of heroin with a total weight of 154 kilograms were located concealed in three of four crates.

The heroin has an estimated potential street value of more than $77 million.

Investigators from NSW Police Force (NSWPF) Organised Crime Squad, Australian Border Force (ABF), NSW Crime Commission (NSWCC) and Australian Criminal Intelligence Commission (ACIC) established Strike Force Roath to investigate the import.

Third man extradited from Serbia over 1.28 tonne cocaine seizure

A 35 year-old man has been extradited from Serbia and is scheduled to appear before Sydney Central Local Court, to face charges related to the seizure of 1.28 tonnes of cocaine more than 18 months ago.

The man – an Australian national who was a resident of the United Arab Emirates – was detained in Serbia by local authorities. He was extradited from Belgrade to Australia, arriving into Sydney International Airport under Australian Federal Police (AFP) escort.

He is the third and final man to be extradited from Serbia in connection with Operation Amorgos, after a 43-year-old NSW man arrived in Sydney in March 2018 and a 49-year-old man in August 2018.

Operation Amorgos is an AFP-led investigation into an organised crime syndicate believed to be responsible for the importation of 1.28 tonnes of cocaine in Sydney, concealed within pre-fabricated steel, in April 2017..

Border guards in Jazan, Najran and Asir areas foiled attempts to smuggle a total of 876 kilograms of cannabis

A spokesman for the Border Guard stated that the continued monitoring of attempts to smuggle narcotics through the kingdom's land and sea borders resulted in the foiling of several attempts to smuggle a total of 876 kilograms of cannabis and the arrest of 38 persons involved, including (19) Yemeni nationality, (8) of Ethiopian nationality, (7) Saudis and (3) of the Somali nationality and one person Sudanese nationality, after monitoring exceeded the land and sea borders of the Kingdom of Saudi Arabia, Accused and narcotics seized in their possession to the competent authorities.

Wildlife criminal jailed for rare bird eggs importation attempt

A man who tried to smuggle 19 rare and endangered bird eggs into the UK strapped to his body has been jailed for 3 years and 1 month.

The smuggling attempt was uncovered by Border Force officers at Heathrow Airport when officers stopped Jeffrey Lendrum after he arrived on a flight from Johannesburg.

Lendrum was wearing a heavy jacket which officers thought was unusual due to the very warm weather conditions. When asked whether he had anything to declare, Lendrum stated he had some Fish Eagle and Kestrel eggs strapped to his body. During a full search, he was found to be wearing a body belt concealing 19 bird eggs as well as 2 newly-hatched chicks.

Border Force specialist officers identified that the eggs were protected under the Convention on International Trade in Endangered Species (CITES), the import trade for which is controlled by the issue of permits. Officers ensured that both the eggs and the live chicks were kept warm and quickly transported to the Heathrow Animal Reception Centre, managed by the City of London Corporation. The live chicks and the eggs were later moved to a specialist care facility at the International Centre for Birds of Prey.

BORDER MANAGEMENTS ANNUAL GATHERING

EVENT PREVIEW

World Border Security Congress

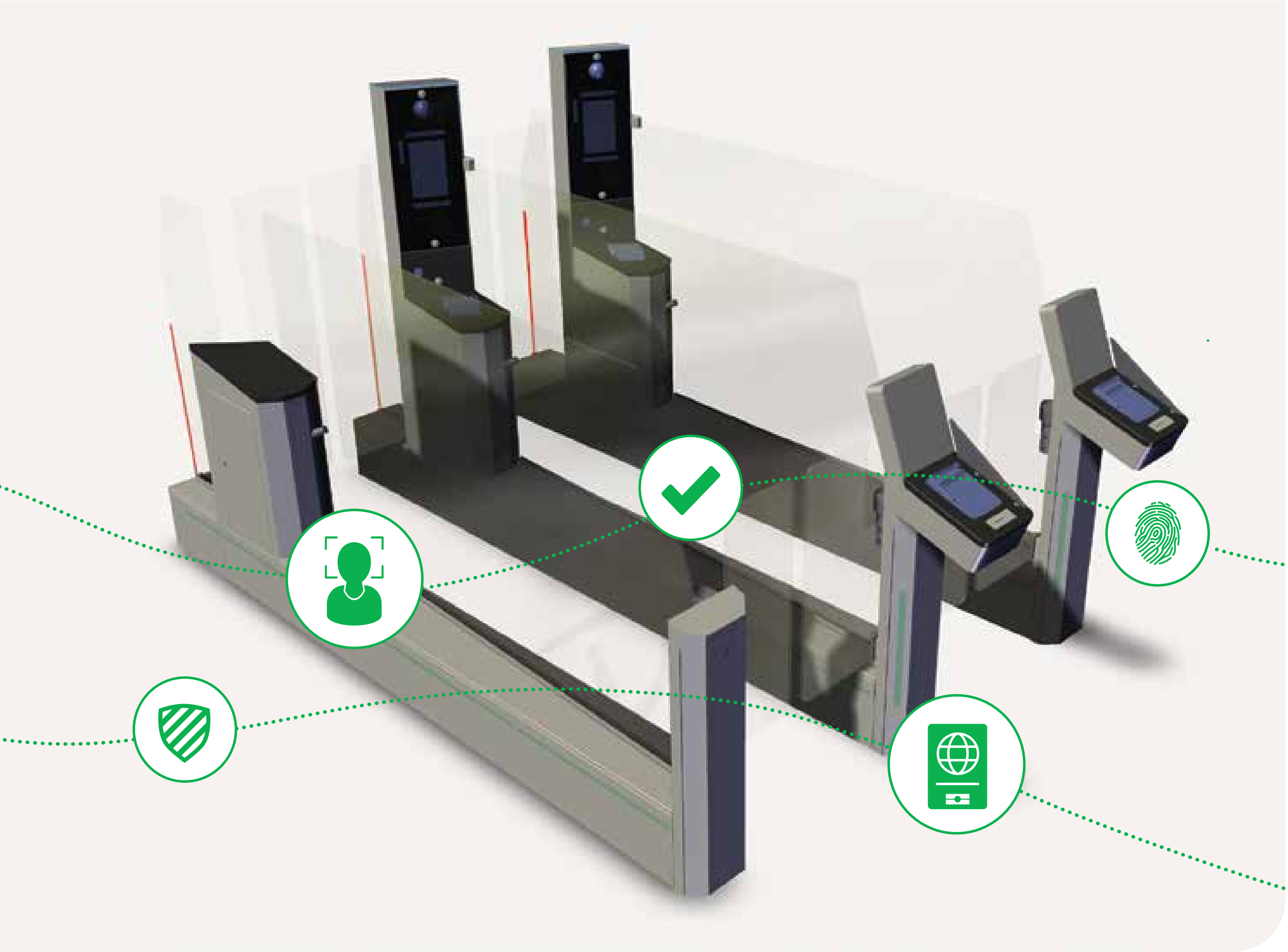
19th-21st March 2019
Casablanca, Morocco
www.world-border-congress.com

The annual gathering of the international border management and protection community will take place in Casablanca, Morocco on 19th-21st March 2019.

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

The 2019 World Border Security Congress will see the largest international gathering of border security and management policymakers and practitioners from more than 50 countries gather for the 3 day meeting for some great discussions, meetings, workshops and networking with colleagues and peers from the global border security community.

Borders in the Maghreb are increasingly dangerous. Armed with tools designed for the pre–Arab Spring



environment, Morocco, Algeria and Tunisia face a complex new world of transnational actors that leverage borders for profit and for sanctuary. Rather than protecting states, a Moroccan Ministry of Foreign Affairs (MFA) official noted, the borders themselves are now the “challenge and threat.” Radical change is needed in national and regional approaches to border security to combat today’s threats. Going it alone is no longer an option in North Africa.

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

Closed Agency Only Workshops

FOR BORDER AGENCIES AND AGENCIES AT THE BORDER ONLY – If you are interested in participating in the Closed Agency Only Workshops, in order to obtain clearance to attend the Closed Workshops, please register via the Online Agency Registration complete the Agency Registration Form and return, to begin the approval process. For details view www.world-border-congress.com.

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

Border agencies and agencies at the border can benefit from the ‘Closed Agency Only Workshops’, **hosted by the Moroccan Directorate for Migration and Border Surveillance, Directeur de la Migration et de la Surveillance des Frontiers**, Organization for Security & Co-operation in Europe (OSCE) and International Organization for Migration (IOM) with a series of behind closed door discussion and working group opportunities.

This years Closed Agency Only Workshop topics are:

Wednesday 20th March 2019 - 11.15am - 12.30pm
International Border Security Challenges - Operational Planning and Rapid Reaction
Chair: Senior Representative, International Organization for Migration (IOM)
Preparing for unforseen operational spikes in border activity is essential, from the development of rapid reaction teams to sharing operational intelligence on the ground. This session aims to discuss and share experience and operational techniques.

Wednesday 20th March 2019 - 4.15pm - 5.30pm
Biometrics – The way forward
Chair: Simon Deignan, Counter Terrorism Officer, OSCE
Biometrics technology has come of age and is now in widespread use in border control applications around the world. However, there are still practical issues around privacy, data protection, information sharing and best practice. This workshop will discuss these challenges and issues surrounding implementation.

Thursday 21st March 2019 - 11.15am - 12.30pm
Information Exchange and Cooperation
Chair: Moroccan Ministry of Interior, General Directorate for Border Surveillance & Migration
Everyone agrees that the sharing information is essential for secure borders. How can we manage data to insure its security and interity, whilst implementing a system of data exchange based on trust to make this a viable and enhance border management?

Congress Agenda

Tuesday 19th March

8:30am - 12:00pm Casablanca Port Site Tour

1:30pm - 2:00pm MINISTERIAL OPENING AND WELCOME

2:15pm - 3:30pm OPENING KEYNOTE

Khalid Zerouali, Wali, Director General of Migration and Border Surveillance, Morocco

Senior Representative, African Union ECOSOCC

TBC

4:00pm - 5:30pm Plenary Session - Identifying and Understanding the Latest and Evolving Threats and Challenges for Border Agencies

As border management techniques and technologies evolve, so too will the threats as criminal gangs, terrorists, traffickers and smugglers develop new ways to evade detection. Identifying and understanding new threats and disseminating information to frontline agencies and partners is key to future success.

Combatting Illicit Trafficking in Cultural Property
Gorancho Stojkowski, Border Security and Management Unit, Transnational Threats Department (TNTD), Organization for Security and Co-operation in Europe (OSCE)

Illicit Goods and Narcotics Trafficking Challenges in Morocco and the Mediterranean
Ahmed Adnane Dahmani, Head of Division of Prevention, Customs Administration and Indirect Taxes, Morocco

James Pigg, Chief Inspector, UK Counter Terrorism Policing Border Operations, UK

Wayne Salzgaber, Director, INTERPOL Washington

Small Arms and Light Weapons and its link to migration and border security
Gabor Kemeny, Project Co-ordinator (ExB), Public Safety and Community Outreach Department, OSCE – Mission to Skopje

Director General, Indo-Tibetan Border Police Force*

Assistant Director of Immigration Services, Ministry of Interior, Kenya*

7:00pm - 9:00pm Welcome Reception (invitation only)

Wednesday 20th March

9:00am - 10:30am Plenary Session - Border Management - from Risk Management to Foreign Fighter and CT Strategies

US intelligence estimates in excess of 40,000 total foreign fighters have gone to the conflict. These men and women present a massive threat to the international security and a huge challenge to the global border management community. Identifying these individuals at border crossing points still presents the best opportunity apprehend these individuals. Developing strategies and technologies to do must be a priority.

Risk Management through risk based decision making processes
Renée L. Yengibaryan, Deputy Director – IPD, Operations Support, U.S. Customs and Border Protection

Dr Nasser Segayer, Libyan National Team for Border Security and Management

The Dutch Approach on Irregular Migration
Neda Katalina MS, Strategic Advisor People Smuggling & Human Trafficking & Nella Kadic MSc, Acting Coordinator International Relations and Crime Investigation Expert, Royal Netherlands Marechaussee

Senior Representative, United National Office for Counter Terror (UNOCT)*

Comprehensive Integrated Border Management System (CIBMS)
Director General, Border Security Force, India*

11:15am - 12:30pm Breakout Session - Implementing Biometrics and Advanced Passenger Information

Biometrics is playing a key role in traveller identification, but how can it be used in a holistic approach, with API and PNR, to enhance traveller facilitation and improve border management.

Simon Deignan, Counter Terrorism Officer, Organization for Security & Co-operation in Europe (OSCE)

Dr Enrique Belda, Deputy Director General of Information Systems and Communications for Security Secretary of State for Security, Ministry of Interior, Spain

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

Research Officer, Frontex*

** invited*

Congress Agenda

Wednesday 20th March

2:00pm - 3:30pm Plenary Session - Migration and Human Trafficking Challenges on Global Border Management

Borders are the 'frontlines' for anti-trafficking interventions, but still very few victims are picked up at the border. What strategies, policies, training and technology should be implemented to stamp out this oldest of human scourges.

Securing and protecting EU external borders
Alvaro Rodriguez-Gaya, Senior Specialist, European Migrant Smuggling Center (EMSC), EUROPOL

Border Security in Ghana and its impact on World Migration issues
Justice Cornelius Amevor, Aflao Sector Commander, Ghana Immigration Service

Desert Border Management Challenges
Baptiste Amieux, Immigration & Border Management Programme Manager , IOM Niger

Major General Md. Shafeenul Islam ndc, psc, Director General of Border Guard Bangladesh

Head of Department of Border Gates and Deputy Head of Department for Anti-Smuggling and Human Trafficking, National Police, Turkey*

The Smuggling of Migrants in Africa: Questions of (Missing?) Protection - Cristiano d'Orsi, Research Fellow/ Lecturer, South African Research Chair in International Law (SARCIL)/University of Johannesburg

Challenges through the Balkans - Senior Representative, Ministry if Internal Affairs, Macedonia

4:15pm - 5:30pm Breakout Session - Data, Cyberborders and the challenges of developing them

Cyber crime has no borders, whether data sharing/flow of information between countries, airlines or agencies, or criminal gangs and the darkweb. What place and function do border agencies have and what strategies do they need to develop to protect cyber borders.

The cyber border and the EU
Bartel Meersman, Head of Unit, Transport & Border Security, European Commission Joint Research Centre

Head of the IT Department, Staff Commander RNLM, Royal Netherlands Marechaussee*

How can AI technology help borders?
Chris Brown, VP International, Basis Tech, UK

5 Digital Intelligence Challenges all Border Agencies are Facing Today
Leeor Ben-Peretz, EVP Products & Strategy, Cellebrite

Thursday 21st March

9:00am - 10:30am Plenary Session - Border Security Information and Coordination

Whether it is returning foreign fighter, human training, cross border organised crime, protecting cyberborders interagency co-operation and information sharing is the key to success. What else needs to be done to make the aspiration a reality, and is there a business transformation approach beyond technology that tackles processes, regulations and security?

Establishment of a Caribbean Border Security Information and Coordination Center
Max Antoine, Executive Secretary, Commission for Border Management of Haiti

Role of intelligence in border security
Babatunde Olomu, Deputy Comptroller of customs, Nigeria Customs Service

Building Cooperation on Discussion and Dialogue
Peter Nilsson IPMc, Police Commissioner and Head of AIRPOL

SHADE-MED Challenges to Successful Cooperation in the Mediterranean
Rear Admiral Enrico Credendino, Italian Navy EUNAVFORMED

Cargo Risk Assessment Demystified
Implementing ACI and PLACI Systems - Emad Muhanna, VP Government Sector, SITA

11:15am - 12:30pm Breakout Session - Surveillance Systems and Technologies on the Border

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

Morocco's National Border Control System
Senior representative, General Directorate for National Security (DGSN), Morocco & Senior Representative, Veridos

SMILE Project
Lenard Zsakai, Local coordinator, border policing expert, Hungarian National Police

FOLDOUT - Protecting Green Borders - Through-foliage detection, including in the outermost regions of the EU
BG lt. col. dr Urszula Młodziejowska- Seredyn, Expert, Border Management Department, Polish Border Guards

Integrated Coastal Surveillance System
An Essential Toolbox for Aiding Maritime Security
Olivier Yvon, SIE Maritime Program Manager, Airbus Defence & Space

Thursday 21st March

2:00pm - 4:00pm Plenary Session - Future trends in International Border Management

As the global economy continues to develop at unprecedented rates, with ever increasing interdependencies and complexities. The global economy depends increasingly dependent on the free movement of people and goods. Understanding future trends in international trade, people movement and crime will drive the development of international and integrated border management in the future.

Florian Forster, Head, Immigration and Border Management (IBM), Dept of Migration Management (DMM), International Organization for Migration (IOM)

Ahad Miah, International Operations, Middle East & North Africa (MENA) Region, Border Force UK

From Management to Governance: Comprehensive Border Governance at A Global Scale
Borut Erzen, Head of Programme, Border Management and Security, International Centre for Migration Policy Development (ICMPD)

Women in Border Security
Inesa Nicolaescu, Associate Border Security Officer, Organization for Security and Co-operation in Europe (OSCE)

Commissioner, Trade, Customs, Free Movement and Tourism, ECOWAS*

IATA Open Borders Strategy and Future Initiatives (1ID -API/PNR initiatives)
Kashif Khalid, Regional Director – Africa & Middle East, Airports, Passenger, Cargo, Security & Facilitation, IATA

4:00pm Congress Round Up and Close

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.

2019 World Border Security Congress Sponsors:

Gold Sponsor:

AIRBUS

Silver Sponsor:

Rapiscan systems

AS&E

S2 GLOBAL

Networking Reception Sponsor:

SITA

Create success. Together

Lanyard Sponsor:

Cellebrite

Delegate Folder Sponsor:

MSAB

Bag Sponsor:

gemalto

security to be free

AU-ECOSOCC Workshop:

Migration – Creating Opportunities for Young People In Africa

AFRICAN UNION
ECONOMIC, SOCIAL AND CULTURAL COUNCIL, AU-ECOSOCC, NIGERIA

Workshop Part One
Tuesday 19th March 2019 : 9am – 12:30pm

Workshop Part Two
Wednesday 20th March 2019 : 9am – 12:30pm

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

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

The Workshop therefore is expected to identify the root causes, share experience with local and international development partners and civil society organizations with a view to curbing irregular migration of African youths and even families to Europe.

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

For moe details visit www.world-border-congress.com

Airbus Confirmed as Gold Sponsor of 2019 World Border Security Congress

The Organisers of World Border Security Congress are delighted to announce that Airbus, one of the world's leading aerospace, defence and security manufacturers and systems providers are the Gold Sponsor at this year's World Border Security Congress in Casablanca, Morocco on 19th-21st March 2019.

AIRBUS

The Organisers of World Border Security Congress are delighted to announce that Airbus, one of the world's leading aerospace, defence and security manufacturers and systems providers are the Gold Sponsor at this year's World Border Security Congress in Casablanca, Morocco on 19th-21st March 2019.

As a world leader in providing large-scale integrated border security systems, Airbus develops complete land and maritime surveillance and protection systems with a multi-level portfolio of precision sensors and C4ISR solutions Airbus designs, develops and im-plements integrated systems including platforms and services across national, regional and local levels, addressing the following business segments: Land border security, maritime security and safety and Critical National Infrastructure (CNI).

Hugh Sinclair, Head of Marketing Security Solutions, said: "Having attended WBS Congress as both exhibitor and speaker for the past two years and engaged with many of the distinguished delegates we recognize the high value of the event. The conference provides Airbus with a unique opportunity to meet and influence government representatives and decision makers in the growing market for border management and maritime security."

The 2019 World Border Security Congress in Morocco will be co-hosted by the Ministiere de l'Interieur (Moroccan Ministry of Interior) and Directeur de la Migration et de la Surveillance des Frontiers (General Directorate for Migration and Border Protection). Morocco is one of the safest and securest countries in Africa with a high effective programme to tackle the migration crisis in West Africa.

Site Visit to Port of Casablanca

Tuesday 19th March 2019 : 8:30am – 12:00pm

The Port of Casablanca is one of the largest artificial ports in Morocco and in the world.

Casablanca's port handles more than 21,3 million tons of traffic annually, 38% of Moroccan traffic, and carries out a sales turnover of more than 894 Million Moroccan Dirhams.

The port covers 605 hectares and extends more than 8 kilometers in length. It can accommodate and treat more than 35 ships at the same time.

The Port of Casablanca is also a major cruise ship stopping point for tourists to visit some of the wonders of Casablanca, such as the Medina, Hassan II Mosque and world famous Rick's Bar.

Processing over 800 thousand TEUs, 21.3 million tons of containerized cargo and more than 200,000 cruise passengers annually, the Port of Casablanca has a number of challenges.

The Site Tour of the Port of Casablanca will offer an insight into these challenges and how the relevant authorities tackle these through traditional and technological solutions.

Spaces are limited so register your place on the Site Tour early. For further details and to register visit www.world-border-congress.com.

Supported 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 ew ways through new challenges and treating those challenges as opportunities to do things better in the future.

REGISTER TODAY
WWW.WORLD-BORDER-CONGRESS.COM

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

The World Border Security Congress is open for members of federal government, border management agencies, law enforcement or inter-governmental agencies, the European Union, INTERPOL, EUROPOL, AFRIPOL, ASEANAPOL, AMERIPOL, OSCE and associated Agencies and members (public and official) involved in border security, management and protection. Applications will be reviewed and considered on an individual basis. Delegates are requested to register sufficiently early to ensure participation. For all above mentioned communities the World Border Security Congress early registration is “Free of Charge“.

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

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

osce Organization for Security and Co-operation in Europe

European Association of Airport and Seaport Police

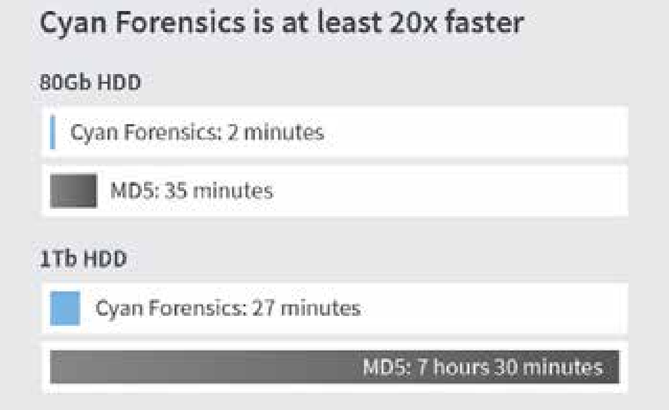
AFRICAN UNION

International Association of CIP Professionals

NS&RC

Innovative Digital Search Tool for Border Stops

Cyan Forensics, a UK startup which develops ultra-fast digital forensic technology to help law enforcement catch criminals faster, is extending its products in to Counter Terrorism and prevention of Domestic Extremism.



Launching to a global Counter Terror audience at the International Security Expo [last month], Cyan Forensics has built a new generation of tools that can scan devices for previously known content (such as terrorist propaganda, and bomb making manuals, and radicalisation materials) in seconds or minutes instead of hours or days.

Examples of applications for rapid triage include border stops searches (Schedule 7 stops in the UK), for pre-charge triage of devices at locus, for compliance monitoring of known offenders, and for rapid post incident examination of known associates' devices.

Currently in use by UK police and law enforcement for triage in child sexual exploitation investigations, the tool can be used to scan seized computers, hard drives and media devices, and can even find partially deleted files.

Finding evidence fast can change the course of an investigation and improve decision making, enabling a rapid response that reduces risks to the public.

The company claims that its tools are 'at least 20x faster' than MD5 hash searches, the closest current equivalent search.

X-ray scanners to meet the demands for vehicle screening

UK-based 2X Systems has developed a range of 2X-300 x-ray scanners to meet the demands for vehicle screening at ports, border crossings and secure facilities – as well as a selection of container systems to cater for a range of security screening scenarios

When it comes to installation, 2X understands the difficulties involved and the requirement for high-skilled personnel to carry it out – which is why its innovative designs are based on delivery to site and out-of-the-box operation, eliminating the need for highly-skilled engineers where possible.

The scanners consist of the rapid deployable 2X-300DT, a fully self-contained system with minimal support required for installation – as well as the fixed 2X-300DF for situations where the system is to be operated on a permanent or semi-permanent basis, and the 2X-300DC conveyor which enables autonomous scanning of vehicles.

Our security systems include the 2X-833, a class-leading metal detector offering security operators a reliable system for use in various operational environments, and the Secupod security solution which can be operational in under an hour. 2X also offers a range of mobile security space solutions (temporary buildings and structures that can be customised to meet customers' specific needs), which have been designed to accommodate security checkpoints and multiple search areas – ideal for sports events and high-security venues.

PureTech Systems' Command and Control deployed to support Border Patrol in San Diego

PureTech Systems recently announced a delivery milestone for the next phase of the Border Patrol's Mobile Video Surveillance Systems (MVSS) program.

The latest deliveries, consisting of ruggedized Ford F-150 trucks outfitted with telescoping surveillance payloads, are being deployed in San Diego, CA and will support mobile video surveillance up to 6 miles away. The event was followed by Fox 5 News and ABC 10 News in San Diego and highlighted the value to Border Patrol agents in the field, including rapid deployment and ease of use.

The MVSS platform utilizes PureTech Systems' PureActiv software as its central command and control, providing video intelligence, user interface display and sensor collaboration logic for the surveillance suite which consists of visible and thermal cameras mounted on a telescoping mast which extends over 35 feet in the air.

In the interview with ABC 10 News, Michael Scappechio, a supervisor with the Border Patrol, said, it's their increased rate of arrests that landed the trucks here, "nearly a 90 percent increase is significant, that's going to get attention, that's going to get resources, that's going to get man power, infrastructure and technology." Border Patrol also furthered that these trucks won't replace the border wall but instead, will go hand in hand with it.

Gemalto awarded Uganda's new e-Immigration solution with fast-track border crossing eKiosks at Entebbe Airport

Gemalto, in cooperation with local partner SCINTL, has been awarded the contract for the supply of a Border Management System (BMS) including airport self-service eKiosks at Entebbe, creating a faster and more convenient border-crossing experience for travelers and strengthening homeland security. jointly developed by Maersk and IBM to promote more efficient and secure global trade.

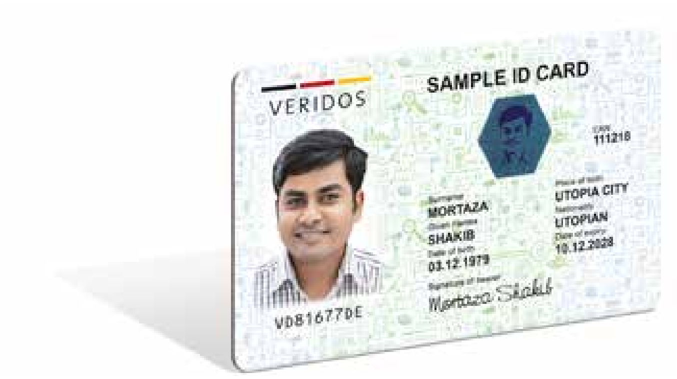
The said e-Immigration solution uses Gemalto's state-of-the-art fingerprint and facial recognition technology, combined with a passport scan to ensure swift and accurate identification of passengers leaving the country. It is built on the Gemalto Visa Management System (VMS) that was first deployed in 2014 by the Directorate of Citizenship and Immigration Control (DCIC), part of Uganda's Ministry of Internal Affairs.

Boosting Uganda's ability to manage international visitors

Entebbe International Airport, servicing Uganda's capital, Kampala, welcomed over 1.5 million travelers in 2017, and the new eKiosks will further boost its capacity to handle the growing number of business and leisure visitors heading to Uganda, a progressive east African state with a population of over 40 million. Once implementation of the e-Immigration solution is complete in 2019, passengers will enjoy the option of a rapid, self-guided pathway through border control, whilst authorities are provided with comprehensive, real-time data on departures from Uganda.

Veridos launches new color image technology

Veridos has announced the release of a new security feature that will allow governments to apply secure, durable and vibrant color ID photos with high process flexibility. Veridos now offers two color image methods for polycarbonate identity documents: POLYCORE® technology and a new solution.

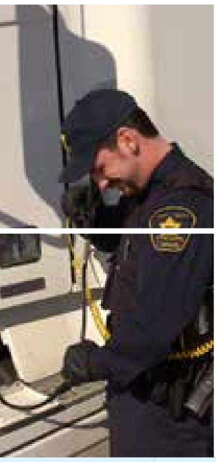


Veridos has announced the release of a new security feature that will allow governments to apply secure, durable and vibrant color ID photos with high process flexibility. Veridos now offers two color image methods for polycarbonate identity documents: POLYCORE® technology and a new solution.

Veridos's new color image technology is called CLIP ID – short for Color Laser Image Protected ID. The solution is being implemented in Bangladesh's new ePassport and will be presented during a joint speech by the Bangladesh Government and Veridos on December 11, at the APSCA Border Management and Identity Conference in Bangkok. Major General Md Masud Rezwan, Director General of the Bangladesh Department of Immigration and Passport, said: "We are proud to offer our citizens ePassports with high-quality color images. With more than 160 million inhabitants, Bangladesh is the world's eighth most populous country and will provide the highest output of passports with color photos worldwide."

Fabiola Bellersheim, Head of Sales Asia at Veridos: "CLIP ID combines laser engraving and color printing within a customized lenticular structure. This guarantees utmost security and long-lasting product lifetime without the need for additional protection layers. It can be applied by any laser engraving and ink-jet printing, making it a very cost-effective technology."

The solution is suitable for both centralized and decentralized personalization processes. Customers placing a higher importance on centralized, combined production and personalization, on the other hand, will still be able to rely on the POLYCORE® technology provided by Veridos's shareholder Bundesdruckerei.



World Border Security Congress

19th-21st March 2019

Casablanca, Morocco

www.world-border-congress.com

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

Building Trust and Co-operation through Discussion and Dialogue

REGISTRATION ONLINE TODAY

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.

Register your place online at www.world-border-congress.com

Confirmed speakers include:

– Goranacho Stojkowski, Border Security and Management Unit, Transnational Threats Department (TNTD), Organization for Security and Co-operation in Europe

– Renée L. Yengibaryan, Deputy Director – IPD, Operations Support, U.S. CBP

– Florian Forster, Head, Immigration and Border Management (IBM), Department of Migration Management (DMM), International Organization for Migration (IOM)

– Simon Deignan, Counter Terrorism Officer, Organization for Security and Co-operation in Europe (OSCE)

– Dr Enrique Belda, Deputy Director General of Information Systems and Communications for Security Secretary of State for Security, Ministry of Interior, Spain

– Alvaro Rodriguez-Gaya, Senior Specialist, European Migrant Smuggling Center (EMSC) , EUROPOL

- Romana Fabbro, Border Advisor, European Union Integrated Border Assistance Mission (EUBAM LIBYA)

For speaker list visit www.world-border-congress.com

for the international border management and security industry

Supported by:

Media Partners: