

World Security Report



For the latest news, features, essential analysis and comment on security, counter-terrorism, international affairs, warfare and defence

July 2015

[Subscribe Here](#)

G4S Global Forecast for Q3

Insider Theft

Securing the airport perimeter

Understanding the Limitations of
Software Security Technologies

US Correctional Facilities: Strip
Search or Scan?

Industry News



4th World BORDERPOL Congress
8th-10th December 2015
The Hague, Netherlands

www.world-borderpol-congress.com

critical infrastructure 2-3 MAR 2016
PROTECTION AND RESILIENCE EUROPE The Hague Netherlands

www.cipre-expo.com

critical infrastructure 15th-16th June 2016
PROTECTION & RESILIENCE ASIA Bangkok Thailand

www.cip-asia.com

www.worldsecurity-index.com

Editorial:

Tony Kingham

E: tony.kingham@worldsecurity-index.com

Contributing Editorial:

Neil Walker

E: neilw@torchmarketing.co.uk

Design, Marketing & Production:

Neil Walker

E: neilw@torchmarketing.co.uk

Advertising Sales:

Tony Kingham

T: +44 (0) 208 144 5934

M: +44 (0)7827 297465

E: tony.kingham@worldsecurity-index.com

Paul Gloc (UK & Europe)

T: +44 (0) 7786 270820

E: paulg@torchmarketing.co.uk

Denne Johnson (Americas)

T: +1 918 863 9792

E: dennej@torchmarketing.co.uk

Subscriptions:

Tony Kingham

E: tony.kingham@worldsecurity-index.com

World Security Report is a bi-monthly electronic, fully accessible e-news service distributed to 39,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, armed and security forces and civilian services and looks at how they are dealing with them. It is a prime source of online information and analysis on security, counter-terrorism, international affairs, warfare and defence.



Copyright of KNM Media and Torch Marketing.

Islamic State's call to fight the mushrik'n [enemy] wherever they are found!



The merciless slaughter of helpless tourists in Tunisia was as abhorrent as it was predictable. In the UK it has sparked off the debate again about how we can deal with the radicalisation of our Muslim youth. The trouble is that this attack did not happen in the UK, nor did the more recent bombing in Turkey.

According to a statement by Islamic State of Iraq and Syria (ISIS), "These were the latest in a line of attacks carried out over the past year by soldiers of the Khilfah around the world in response to the

Islamic State's call to fight the mushrik'n [enemy] wherever they are found."

Radical Islam is at war with the western world, its institutions and values. But not only that, it is at war with the Shia Muslim world and any other religion or state that does not conform to its interpretation of Islam.

The reality is that radical Islam, like a cancer, is only likely to grow and the current international response amounts to not much more than half hearted containment.

To the more malleable and disgruntled Islamic youth around the world, ISIS fighters in Syria and Iraq look like hero's, taking on the world and if not winning at least holding their own against overwhelming odds. This is an incredibly attractive and intoxicating mix to young men driven by testosterone, religious zeal and righteous indignation. This is not a new phenomenon, the young are often attracted to a cause, wanting to change the world and be part of something bigger than themselves.

Every act of terrorism is seen as an act of defiance and further re-enforces the belief that they are somehow winning. Every terrorist killed during an attack is a martyr to be emulated.

Radicalised Islamic youth are a danger that needs to be tackled but they are a symptom, not the cause. The cancer needs to be tackled and destroyed at its heart. Whilst radical Islam has a 'homeland', from where it can train and recruit more fighters, finance its operations, co-ordinate global campaigns and provide the sham of a perfect Islamic state, any attempts to tackle national youth problems will have little hope of success.



ISIS will continue to look for soft western targets wherever it can and by so doing de-stabilise vulnerable states like Tunisia and Algeria, dependent on Western tourism or oil for their economy. It will continue to attract foreign youth who can one day return home as trained terrorists.

Only when ISIS is defeated on the ground and is seen to be defeated, will we stand a chance of tackling our national issues.

Clearly, for this to happen it would mean that the coalition military operations in Syria and Iraq would have to be ramped up dramatically. But given the current lack of appetite in the west for military intervention and military spending, this not likely in the foreseeable future.

The belated intervention of Turkey could have proved to be a game changer. But their decision to break their truce with the Kurds could negate the benefits and seriously complicate an already complicated situation.

At some point in time, ISIS will manage to commit an atrocity so awful, like 9/11, that public opinion in western nations will demand action and western leaders will be forced to do what they know they should be doing already. What that atrocity is and when, only time will tell.

In the meantime, ISIS will continue to grow, spread its influence and commit further atrocities, either itself or through its growing number of acolytes.

Tony Kingham
Editor
World Security Report

G4S Risk Consulting Global Forecast 2015 Quarter 3



The G4S Global Forecast for Q3, 2015 focuses on the key thematic threats faced by countries around the world in the coming three months. These include militancy, political and civil unrest, health and disease, terrorism, economic risk and the impact of major geopolitical developments.

Militancy remains a key theme of our forecast for the coming quarter. Islamic State (IS)-related activity continues to be reported in Europe and further arrests across the continent are expected throughout Q3, with the associated risk of a terrorist attack. Recent events in France and Tunisia amply demonstrate the potency of the threat just days before the UK commemorates the tenth anniversary of the 7/7 terrorist attack in London.

The risk of further attacks is fuelled by the resurgence of territorial victories by IS in the Middle East, where affiliates continue to capitalise on gaps in state control and chaotic security environments. The threat posed in Africa by Somalia's al-Shabaab and Nigeria's Boko Haram appears to be in decline following joint military campaigns, but in Asia, the fighting season in Afghanistan

is set to reach its peak in Q3. Meanwhile, to the west, fears mount in the CIS region over the potency of the IS ideology.

Pressure on national borders and international institutions stems not only from insurgents, but can also originate from economic risk. The ongoing fiscal crisis in Greece and the potential for the country's "Grexit" from the Eurozone casts doubt over how the EU may respond to an unprecedented situation in the coming months.

Political unrest is another global theme in Q3 with many African nations set to hold elections, or leaders seeking to amend constitutions. Unrest in Burundi is unsettling neighbouring countries as a result of the numbers of displaced people, but its example is unlikely to deter incumbent leaders set on holding onto power. In Nigeria, however, the outlook is good despite looming

fiscal tightening.

In Latin America, civil unrest will remain a major concern in Venezuela and political tensions are set to rise ahead of Argentina's presidential elections in October. In Russia and the CIS, the separatist insurgency in eastern Ukraine is growing steadily more desperate. In Asia, though the momentum of Hong Kong's pro-democracy movement has slowed, there remains a risk of a return to street protests.

One of the most dynamic geopolitical developments currently emerging concerns the South China Sea (SCS) and the disputing claims to its islands and waters. These are set to shape regional relationships and tensions in Asia, but political spats are unlikely to escalate into armed confrontations at present.

Meanwhile, health and disease

remains a core theme in some parts of the world. A threat to health is posed in Africa in the coming quarter, where populations face Ebola, cholera and meningitis, while an outbreak of the Middle East Respiratory Syndrome (MERS) virus is cause for concern in South Korea, Thailand and China.

These are the core risks that we believe will unfold over the coming quarter. We hope that the Global Forecast series continues to inform your assessment of risk.

Africa



Health poses key risk

Medical threats will remain a major risk for parts of Africa in the coming quarter. Although Liberia was declared Ebola-free on 9 May, the outbreak continues in Guinea and Sierra Leone, where occasional breaches of emergency protocols still occur. Cholera is another major threat; not least as more than 100,000 refugees flee the crisis in Burundi into Tanzania and other neighbouring countries. Of the more than 20,000 cases of cholera recorded in the first quarter of 2015, at least 90 percent were identified in Mozambique, DR Congo, Nigeria, and Kenya, where inadequate environmental management, particularly in peri-urban slums and displaced camps, increases the risk of transmission. There have also been a series of

meningitis outbreaks reported in Nigeria, Ghana and Niger, where the largest outbreak has affected 13 districts. The continuing threat posed by disease in Africa should remain a priority in the private and public sectors.

Insurgents face firmer military responses

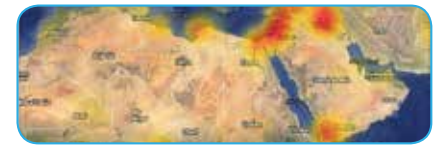
The continent's two leading insurgencies – Somalia's al-Shabaab and Nigeria's Boko Haram – are now facing improving military campaigns by joint regional forces. Irregular cooperation between the armies of Nigeria and its neighbours, particularly Chad, has begun rein back the jihadists, and Nigeria's President Buhari is preparing to revamp the counter-insurgency campaign. Nevertheless Boko Haram continues to attack civilians and security forces in Nigeria and over its borders. Although al-Shabaab continues to pose a threat in East Africa, it is slowly being forced back by the AMISOM mission. Despite the group's apparent decline, terrorist attacks will remain likely over the coming months in AMISOM contributor countries, most of all in north-eastern Kenya, but with a threat also in Uganda, Djibouti, Burundi and Ethiopia. Similarly, Mogadishu, Puntland and Somaliland continue to face the prospect of further attacks on government and foreign targets in Q3.

Infrastructure the key development hurdle

Constraints on infrastructure will continue to hold back economic growth across the continent. The power crisis in South Africa threatens to impact its economic performance as state energy company Eskom is forced to impose load-shedding across cities, damaging business continuity and increasing costs. A meeting of heads of state at

the annual African Union (AU) summit in Johannesburg agreed that more than USD 90 billion in regional infrastructure funding is needed. Only half of that is currently financed. Nevertheless, the recent agreement to combine three regional economic blocs bodes well for the AU's plan to begin negotiating a Continental Free Trade Area (CFTA) by 2017, opening up the continent to investment.

Middle East & North Africa



Resurgence of Islamic State

Islamic State (IS) militants will continue to target new territory, especially in Syria, following a series of symbolic victories in Q2 with the capture of Ramadi in Iraq and Palmyra. Further territorial losses to IS are expected in northern Syria, raising concerns in Turkey over the possibility of over-running moderate rebels, adding to the pressure on the Turkish government to take more decisive action to prevent the movement of militants and illicit trade across the border. IS gains have come despite the US-led coalition airstrike campaign and the use of predominately Shi'a militias to fight the group in Iraq. The fall of Ramadi demonstrates how Iraqi security forces are struggling to counter IS in Sunni areas and how the dependence on militias poses systemic risks to the Iraqi state. Further IS territorial gains in Q2 will be a vital recruitment tool as its victories fuel counter-hegemonic jihadist narratives that the group is out-manoeuvring its enemies.

Elsewhere, IS affiliates continue to capitalise on the vacuums of state power and contests for political

legitimacy, expanding operational capabilities in several other countries. In Libya, IS militants have seized control of Sirte airport, while also carrying out high-profile attacks near Misrata and Tripoli. Yemen and Egypt are likely to see an increase in IS-claimed attacks in Q3 amid worsening security environments across Yemen and in the Sinai Peninsula.

The risk of IS-inspired attacks remains extant across the region, particularly in areas frequented by Western tourists. The 26 June attack on a beach resort in Sousse, Tunisia, will impact heavily on tourism, damaging the economy.

Oil output glut continues

High levels of oil production are forecast to continue in Q3 as Saudi Arabia remains firm in refusing to use its swing power to bring up the barrel price. The conflict in Yemen is costly, but the financial cost of its intervention will not be immediately felt in Saudi Arabia, and is therefore unlikely to impact oil prices in the immediate term. Declining supply from Iraq and Libya will have limited impact on the worldwide output as the US and Gulf States, among others, continue to fulfil demand.

Iran nuclear deal fall out looms

After political and sectarian rivalry between Saudi Arabia and Iran spilled over into conflict in Yemen in Q2, the hostile relationship poses critical challenges to regional security in Q3. Saudi Arabia is concerned over the opening up of Iran to international investment if a final accord over Iran's nuclear facilities is agreed with the P5+1 group, with Israel aligning as another vocal opponent of the withdrawal of sanctions on Iran. Although a major shift in US alliances in the region is unlikely, the US-Saudi relationship will cool if an accord is reached, as is expected.

Asia



Brinkmanship in the South China Sea

China's land reclamation activities and rhetoric over its claims to disputed areas in the South China Sea will continue to be a flashpoint for the whole region, and a defining factor in relations with neighbouring countries, such as the Philippines, Vietnam and Japan. Tokyo's deliberations over amendments to its pacifist constitution will cause disquiet in China. The US will step up monitoring activities in the South China Sea, causing sharp rebukes from Beijing. A military standoff or event that China deems provocative could lead to Beijing declaring an Air Defence Identification Zone (ADIZ) over the region, but the immediate-term risk of outright armed conflict remains minimal.

Hong Kong's pro-democracy campaign

Although the pro-democracy movement's momentum has slowed, the issue will continue to simmer in response to key triggers over the next quarter. The Hong Kong government's controversial proposal calls for all candidates to be screened, which effectively ensures that the outcome matches Beijing's desires, means that opposing parties will engage in a public relations battle across the city to win over public opinion. There remains a latent risk of a return to street protests that may be smaller in nature, but comprised of radical elements pursuing more direct action in the name of a Hong Kong identity.

Terrorism & Insurgency

Insurgency will intensify in Afghanistan as the fighting season reaches its peak. The Philippines's military continues to combat the New People's Army (NPA) in Mindanao, as the Myanmar military persists against the MNDAA rebels in Kokang. There is a high risk of sectarian terrorist attacks in Pakistan, as Sunni militants become emboldened in the wake of recent attacks on minorities. Authorities will also continue to make arrests of suspected Islamic State (IS) sympathisers in Bangladesh, Malaysia and Indonesia.



Environment & Health

Screening of passengers at exit and entry points will increase due to the outbreak of the Middle East Respiratory Syndrome (MERS) virus in South Korea, China and Thailand. Improved coordination between national health bodies ensures a proactive response, but a prolonged outbreak would cause localised business continuity disruption. Meanwhile, an above-average NW Pacific typhoon season is forecast in Southeast Asia, with a high possibility of the El Niño weather phenomenon. In Pakistan and India, the traditional monsoon season is forecast to be below normal, but extreme conditions ranging from flooding to heatwaves are expected. Poor infrastructure in affected countries means that the risk of casualties is high.

Americas



Civil unrest ahead of controversial elections

Public unrest remains a key concern in Venezuela as the opposition continues to demand the release of political prisoners and the resignation of President Nicolas Maduro. Meanwhile, the ruling party faces declining support as the economy enters crisis amid rising levels of violence across the country. In Argentina, political tensions are projected to increase ahead of the presidential election in October.

President Cristina Fernandez will remain an influential political figure despite poor economic performance and a series of corruption scandals. Large-scale, disruptive demonstrations by both supporters of the government and its opponents are highly likely, particularly in the capital, Buenos Aires, and other major cities.

Mexican government faces increasing political and social pressure

In Mexico, the ruling PRI party will continue to face strong political pressure following the results of the June 2015 mid-term elections. Although President Enrique Peña Nieto's party retained a majority in the lower house of Congress, its victory was only by a small margin. The elections demonstrated that the three largest parties – the PRI, the conservative PAN and the left-wing PRD – will need to address the loss of their supporters to either independent candidates or smaller parties as a result of widespread social discontent with the current political, economic and security environment. The government will continue to face severe levels of unrest in Guerrero state, as well as strikes and protests by teachers' unions across the country. A key test for the Peña Nieto administration's performance will be the effective implementation of the controversial energy reforms, particularly after the announcement of the first auction winners in July, which will open the oil and gas exploration industry to private and foreign investment. Strikes and demonstrations, particularly by left-wing activists opposing the reforms, are likely over the coming months, especially in Mexico City.

Tense peace negotiations to continue

The announcement of a truth commission following peace

negotiations between the FARC rebel group and the Colombian government was an unprecedented step towards a comprehensive agreement. Nevertheless, the suspension of FARC's ceasefire has disrupted momentum after a number of violent confrontations with the military. Public support for the peace dialogue is declining as a result of rebel attacks against key energy, police and military targets. As President Juan Manuel Santos continues to push for concrete agreements on the negotiation agenda, the pace of the talks is likely to remain slow. The risk of further political violence is expected to remain high as other smaller rebel groups, particularly the National Liberation Front (ELN), continue to demand similar peace negotiations with the government.

Europe



Ongoing threat from Islamist-related terrorism

Authorities across Europe are expected to continue to make counter-terrorism arrests in relation to Islamic State (IS) and wider Islamist extremism, particularly in light of the lone-wolf attack by a jihadist sympathiser on his boss in a factory in Lyon, France. Arrests have been recorded in a number of countries including the UK, Sweden and Austria. Individuals have also been sentenced to lengthy jail terms in Belgium,

Austria and the UK, among other countries. Authorities are also introducing tougher legislation to curb the threat of Islamist-related terrorism, including in the Netherlands and Italy. Major counter-terrorism offensives have been conducted in the Balkans. Further arrests and aggressive counter-terrorism operations are likely, which could escalate community tensions and lead to possible individual or small-cell attacks in the region. The threat of Islamist-related attacks in Western Europe also remains likely, particularly in relation to the possible targeting of the media, Jewish interests and government assets.

Pressure on EU and Eurozone

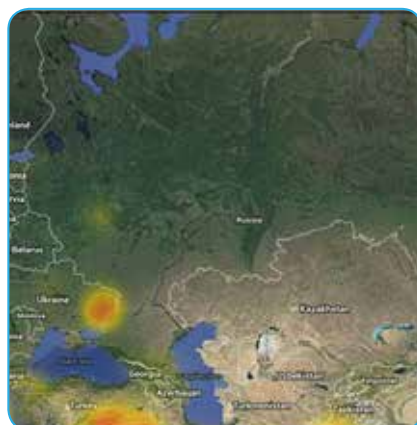
The ongoing Greek crisis and the potential for Greece to leave the Eurozone casts doubt on how the EU and the Eurozone may respond in the coming months. A "Grexit" appears increasingly possible with the imposition of capital controls and the looming referendum. Strategic challenges are anticipated within the EU's financial architecture in Q3 as the role of the IMF, ECB and other bodies is called into question by the rising crisis. European elites are struggling to restrain rising anti-austerity and Eurosceptic sentiment either from the right in Italy, France and the UK or from the left in Spain and Greece, sentiments keenly encouraged in Moscow. While EU leaders are confident that a Grexit will not trigger contagion, there exists a high potential for the gap between political and economic union in the Eurozone adding to the discord between EU members in the event of the country's withdrawal.

Continued growth of anti-austerity movements

Following the success of Syriza in

Greece, the growth of Podemos in Spain and, most recently, the victory of the Scottish National Party (SNP) in the UK in the May general election, it is expected that anti-austerity movements will continue to garner support. Far-right parties such as Poland's Law and Justice Party and France's National Front have seen support grow on an anti-austerity platform. Also anticipated in coming months is the growth of non-political movements that are opposed to austerity. The UK has seen several mass rallies by the People's Assembly Against Austerity since the May general election, while Blockupy activists held protests in Frankfurt, Germany in March. Such rallies could become volatile, resulting in city-centre disruption.

Russia & CIS



Donbass violence to continue as separatist economies collapse

The separatist insurgency in eastern Ukraine is growing steadily more desperate as economic realities curtail Russian expansionist ambitions, forcing Moscow to pull back from its apparent goal of building a land bridge to Crimea. Rebel militias will be forced to rely more on raising informal taxes from local populations, accelerating the pace of collapse as the financial system in separatist-held areas becomes steadily more cash-based and rudimentary. Nevertheless, fierce

localised conflicts will continue along the de facto border, and will continue to undermine Kiev's fiscal outlook as EU and IMF leaders are distracted by the Greece crisis.

Kremlin to refocus on undermining EU unity

Russia's hybrid war in Ukraine is unlikely to intensify to the extent of the worst warnings of outright invasion, but the campaign will extend beyond the hard military sphere and into the deployment of money and disinformation to subvert and disorientate Russia's perceived opponents, most of all those in Eastern Europe. The unity of EU states in support of Kiev is at risk of failure as the Kremlin aims to co-opt anti-systemic parties, notably Syriza in Greece among others, in order to hamper EU sanctions. The risk of subversion and a crisis in the Baltic nations is rising.

Central Asian repression to continue

States in Central Asia remain unremittingly repressive, increasing the long-term risk that the ideology of Islamic State (IS) will gain traction and the movement mobilise in the region. Taliban gains and IS attacks in northern Afghanistan, border clashes in the chaotic Ferghana Valley shared between Tajikistan, Kyrgyzstan and Uzbekistan and the defection of a senior Tajik police officer to IS all bode ill for the region's outlook. In the coming months, however, stagnant authoritarianism is set to continue.



Insider Theft reportedly increased by over 200% between 2011 and 2015.



Verizon 2015 Data Breach Investigation Report

There's probably a decent correlation between the populations of people who read movie credits and those who read the demographics section in a 70 page report.

You might linger to be reminded of that actress's name who was also in that movie you liked years back or see the bloopers at the end of a Jackie Chan film, but otherwise it's a basic stampede or scramble for the door before the parking lot gets slammed...

I, however, do believe that demographics are rather important!

How else do you really know if the findings of all of the various research studies and articles that you read are generally representative, if they're relevant to your organization, etc.?

Such questions are important to proper interpretation and application of a report such as the attached Verizon 2014 & 2015 Data Breach Investigation Reports (DBIR).

All of that said; one thing is painfully clear: Data Theft and Insider Risks are an ever present and very serious problem!

The Online Trust Alliance (OTA) 2015 Data Protection & Breach Readiness Guide reported 740,000+ cases of data theft, the worst year in history!

2015 OTA Breach Highlights:

- 90% Could have been prevented - OTA
- 56% Due to insider threats and physical theft - OSF
- 40% of the largest breaches

OSF

- 91% increase in targeted attacks - SYMC

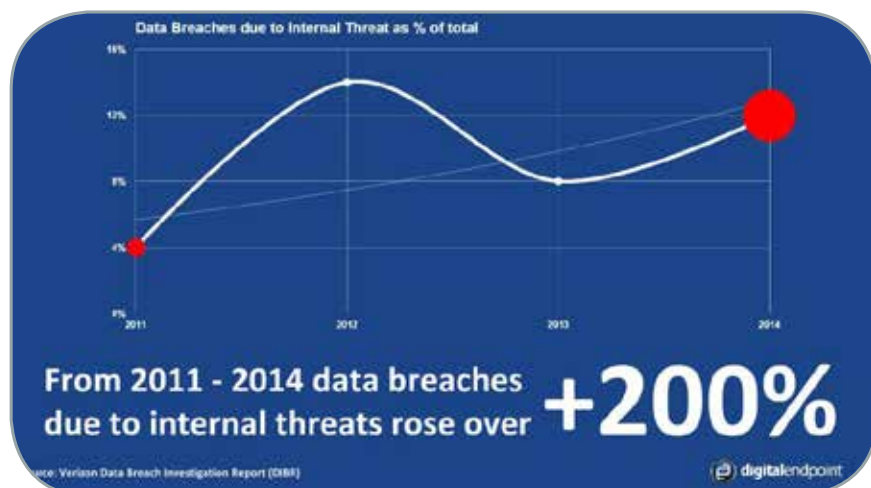
Sources: OTA - Online Trust Alliance, OSF - Open Security Foundation, SYMC - Symantec

Last year's DBIR covered incidents affecting organizations in 95 countries; the updated tally for the 2015 report is 61. So; I guess this obviously means that 34 countries got secured over the last year; great job everyone, right? In truth, we don't really know what's going on there, do we? In terms of volume, two-thirds of incidents occurred in the U.S.A. That's not a big surprise, is it?

The industries most affected look remarkably similar to prior years, and the top three are exactly the same: Public, Information, and Financial Services.

My overall take from these results remains consistent as well: No industry is immune to security failures and insider theft.

Don't let a "that won't happen to



me because I'm too X" attitude catch you napping!

I for one, was almost at a complete loss for words over the Insider Threat Warnings Section and, if you were hoping this would point out a spike in stolen pens and pencils, I'm afraid this report will let you down!!!

The Insider Misuse pattern outlined in the DBIR shines a light on those in whom an organization has already placed significant trust—they are inside the perimeter defenses and given access to sensitive and valuable data, with the expectation that they will use it only for the intended purpose. Sadly, that's not always the way things work folks!

As is the case with this DBIR report, people are people; so, why should it be that we expect

what we don't inspect?

Also, sadly, predictably, folks still steal things from the companies they work for!

Ok so now, there you are, sipping Mai Tais on the beach, enjoying a well-deserved vacation after installing all those shiny, new, advanced threat-mitigation devices at your corporate perimeter, confident in your ability to detect those pesky and insidious external attackers bent on stealing your corporate secrets.

You fire up your shiny new iPhone 6 plus only to be met with an e-mail subject line from Digital Endpoint™ that sends shivers down your back: "What are you doing to prevent insider threats"?

Looks like it's time to get off the easy chair and get back to work, sorry!

Besides this, I will refrain from further commentary on these demographics, Mai Tais, etc., and simply encourage you to look these reports over carefully and decide how relevant its warnings are to your organization and whether they change the way you consider addressing Data Loss Prevention and Insider Threats in your organization!

Our Mission is to provide businesses with tools that enable them to gain total visibility into their operations, protect and secure their most valuable assets and reduce their risk!

Digital Endpoint™ created KnowIT, the world's first Cloud Based Employee Monitoring Software to provide companies with critical information regarding the digital behavior of their employees across Mobile Devices, Macs & PCs.



National Security & Resilience Conference

20-21 October 2015
London, UK

presented by:



REGISTER ONLINE TODAY
Early Bird Deadline - 20th September 2015

The National Security & Resilience Conference, hosted by the National Security & Resilience Consortium (NS&RC), will help you identify the future threats to your organisation and help you strategise and plan for your business security and resilience.

For further information, conference programme and registration details visit www.nsr-conference.co.uk

Sponsored by:



Organisational security and resilience in today's climate of extreme threats

National Security and Resilience combines national security needs with an in-depth understanding of the design and implementation of resilience solutions.

Working collaboratively and cooperatively to provide unique, world-class security and resilience solutions in the face of increasing natural and man-made risks and threats to Governments, corporate organisations, major events, transport systems and critical national infrastructure.

Preparing your organisation for what lies ahead - securing your business future

Securing the airport perimeter



Mark Radford, CEO at Blighter Surveillance Systems believes electronic-scanning radars can help solve the growing 'backdoor' security threats at international airports.

With the continued targeting of aviation by terrorist groups worldwide, attention is turning from the strict levels of security employed for passenger screening to targeting 'backdoor' threats arising from relatively low levels of perimeter security at many of the world's tier one and tier two airports. Other threats include intrusion by political activists or intruders intent on criminal activity, sabotage or attempting to stow away on aircraft.

Hitherto, airports have employed large numbers of CCTV cameras and security personnel to monitor for perimeter intrusions. However, the flat, open nature of airports allows perimeter surveillance radars (PSRs) to be installed as the primary sensor for the detection of breaches of the airport perimeter.

But not all radar technologies are equal in meeting the

specific circumstances and needs of airport operators who have a choice between low cost mechanically scanned ground surveillance radars and sophisticated solid state electronic scanning radar systems, such as those now in operation at major airports such as London Heathrow.

The Shortcomings of Low-cost Short-range Radars for Aviation Security

Over the last five to ten years, many tier one airports have experimented with the installation of relatively low-cost short-range PSRs, usually as part of an integrated perimeter intrusion detection system. Such radars typically offer maximum man-detection ranges of between 400m and 1.6km. The relatively low capital outlay associated with these small, mechanically-scanned radars is initially very attractive to the airport operators.

However, the short detection ranges offered by these radars means that they must be located close to the perimeters and/or boundaries being monitored; this also means that they must be installed close to the airport's operational taxiways and runways. Short-range radars tend to use very high frequencies and have an inherently narrow elevation beamwidth. The combination of short range and narrow beamwidth makes it necessary to site the radars close to the ground in order to avoid a shadow area below the radar and close to the area to be monitored.

This can lead to a number of shortcomings:

- * The view of the radar may be obstructed by the shape of the ground, buildings and other infrastructure, aircraft and vehicles, and leads to increased

multipath effects;

- * Proximity to the fence raises installation costs, often necessitating groundwork to provide networking and power cables for the multiple short-range radar units needed to cover the areas and distances involved. This work is generally disruptive to normal airport operations and often has to be carried out overnight;
- * The detection capability of radars of this type is significantly reduced in rain and they tend to not to have rain filters either, further reducing their usability in poor conditions. Short-range radars are also often positioned at the limit of their range, leaving no room for less-than-perfect weather conditions and the possibility of gaps in coverage that are not apparent to either installer or operator.
- * Low cost radars also tend to rely on plot extraction taking place on a server rather than within the radar. This requires high bandwidth communication from the radar to the server and a server capable of processing data from multiple radars before

information can be presented to the operator. Low-cost radars very often have a basic, unintuitive user interface which provides poor rendering of information relating to targets to the operator and few controls.

False alarms

Short-range perimeter surveillance radars also suffer from high false alarm rates. It can be very difficult for these mechanically-scanned sensors to distinguish genuine targets of interest from the large clutter returns caused by radar reflections from terminal buildings, hangars, fences and other airport structures or objects. The airport apron will also have a large quantity of legitimate moving traffic of all shapes and sizes, from A380 aircraft to small ground support vehicles. The relatively crude filtering techniques used in non-Doppler radars have difficulty suppressing clutter and an inherent inability to distinguish unique targets.

Airport operators have also experienced problems with high false alarm rates during periods of inclement weather (high winds, rain, hail, snow, etc.).

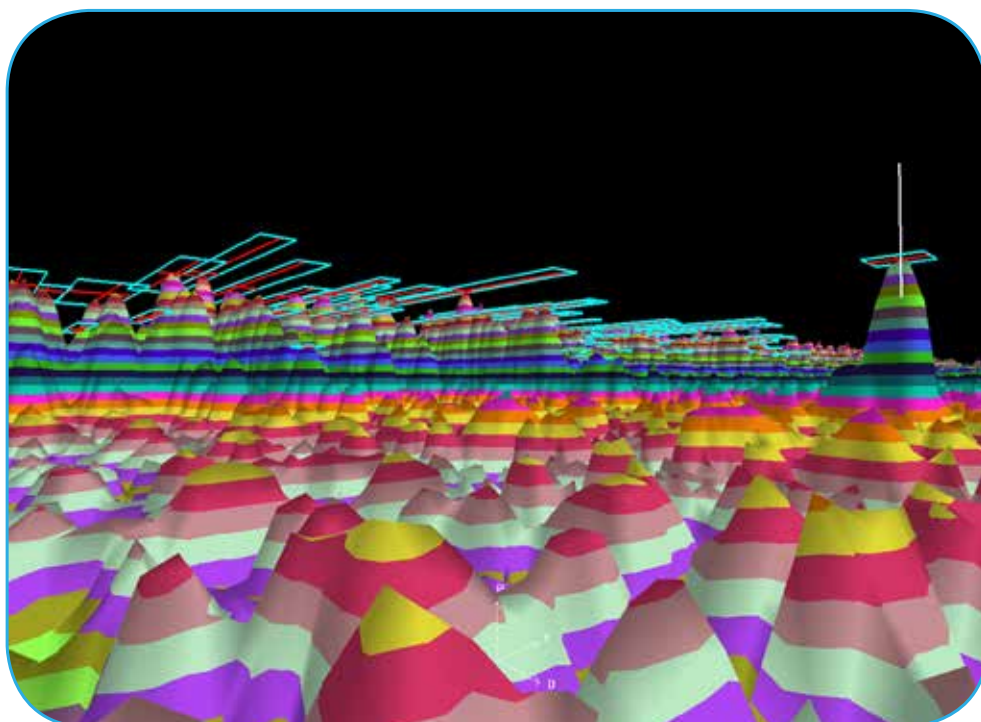
Without Doppler processing, short-range radars will have real difficulty in detecting small targets in the presence of larger targets at the same range. Non-Doppler radar technology is inherently troublesome in all but the simplest environments and airport operators have reported unacceptably high false alarm rates with these radars, to the extent that it has been anecdotally stated that “poorly performing mechanically scanning radars are getting all radars a bad name in airport security”.

Poor reliability

Because of their mechanical operation, rotating radars offer poor reliability compared to solid-state technology. In a desktop PC, for example, it is the rotating hard disks and power supply cooling fans that are most likely to fail. The same is true of rotating radars. Regular routine maintenance of the drive belts and motors of the antenna turning gear is needed to avoid breakdowns. Because of the location of the radars, this maintenance has to be carried-out when the runways and taxiways are not in use. The overall inherent unreliability of mechanical systems leads to much higher through-life costs and longer periods of potential downtime for the security system.

The Benefits of Long-range Electronic Scanning Doppler Radars

Recent developments in electronic-scanning (e-scan) radars have seen a move away from the expensive and power-hungry AESA (active electronically scanned array) military approach to the newer and much lower-cost PESA (passive electronically scanned array) radar technology. The lower entry point allows PESA security radars to be employed for both their traditional military force protection roles and for some



more cost-sensitive applications in the homeland security market, such as securing critical infrastructure like airports and seaports.

Using PESA technology, man detection ranges of up to 3, 5 or 7.5 miles (5, 8 or 12 km) and ultra-wide elevation beams (up to 20 degrees) can be achieved. This allows the radars to stand off from the area to be monitored, mounted on top of existing airport buildings, for example, giving a clear line-of-sight to the airport perimeter, while still maintaining the full integrity of the radar coverage zone. Being able to mount the sensors on the existing airport buildings makes for ease of connection to readily available sources of power and network connectivity.

Fully e-scan radars are entirely solid-state with no moving parts and hence have no requirement for any routine maintenance. Such radars are said to be 'zero maintenance' with much lower associated through-life costs and a long in-service life of 10 years or more.

PESA radars usually include a fully integrated Doppler processing engine, unlike their counterparts, which often require external radar processing servers or PCs that have to be hosted in a remote server room at the airport.

Doppler processing is essential for the cluttered airport environment. As colour is to CCTV images, Doppler is to radar detection. Doppler adds a third dimension to target detection, so not only are targets identified in Azimuth and Range, but they are also discriminated by Doppler velocity – the relative speed of each object. This allows valid targets to be discriminated and separated from the surrounding airport clutter.

Another benefit of e-scanning



radars is that during the scanning process, the radar's microwave beam is entirely stationary, allowing such systems to detect very small and slow-moving targets in extremely cluttered environments.

This improves their detection capabilities and reduces the false alarm rate. It also means that e-scan radars are able to detect wild animals within the airport perimeter, including coyotes, deer and wild dogs. This offers airport operators an unexpected benefit when installing such systems. Contrast this with mechanically rotating radars, where the reflected signals received by the radar are always blurred by the continuous rotational movement of the antenna.

In summary, the benefits of PESA e-scan radars are clear: 24/7 persistent surveillance capability in all-weather with lower installation costs, lower through-life costs and lower false-alarm rates.

Ideal Radar Characteristics for Surveillance at Airports

An efficient and effective radar-based surveillance solution specifically for use at airports would have a number of attributes:

Configurability

As no two airports are the same, a radar system should be configurable in azimuth, elevation beamwidth, range and scan time to suit the particular topography, building and runway layout, traffic and infrastructure arrangements of each in order to optimise performance and efficiency.

Overloading operators with irrelevant information reduces their ability to detect intruders quickly and reliably, so it is highly desirable that there should be a facility to define zones of interest to maximise the possibility of detection of genuine targets and minimise disruption by unwanted information and false alarms. Zone controls may range from suppressing simple arc, rectangular or polygonal areas altogether or filtering results from these areas according to target size or velocity, to more sophisticated techniques in which different parameters are assigned to different areas based on likely activity and potential level of threat.

Flexible Installation and Integration

Radar designs with wide elevation beamwidth can be located high on existing terminal buildings to avoid blocking by objects

'see' over obstacles including aircraft and vehicles. These locations are more likely to be able to make use of existing power and network infrastructure, simplifying installation and radars with on-board signal processing electronics reduce both the network bandwidth required for communication with and the processing burden on the host control station, reducing ancillary computer hardware costs.

Integration with camera and other security systems allows audible alarms to be triggered and cameras to be directed automatically towards the target for visual inspection. Alarm trigger conditions might be based on a range of target attributes such as location, size, velocity or track. Many operators also find it useful to be able to see the raw plot in order to more accurately interpret alarm conditions.

Detail and Distance Performance

In the cluttered airport environment, it's important to be able to discern smaller, slow-moving targets such as intruders on foot from larger and faster objects such as taxiing aircraft or

support vehicles. This requires Doppler processing capability. Adequate range is also essential and ideally this will exceed the designated surveillance area by a comfortable margin in order to allow for degradation of capability in inclement weather.

Blighter e-scan solution at London Heathrow Airport

Heathrow Airport is the world's busiest international airport with over 72 million passengers travelling through to and from more than 85 countries. The Blighter B400 series e-scan PESA radars operate there as part of an integrated perimeter security system, supplied to airport operator BAA Ltd (now Heathrow Airport Holdings Ltd).

BAA needed a highly reliable, maintenance-free system that could provide intensive 24-hour surveillance of the airport in all weather and light conditions. The airport perimeter surveillance solution includes long-range day and night cameras and a network of high definition cameras, capable of identifying and tracking intruders detected by the radar. Since deployment in 2012 it has

led to considerable operational savings, reduced security staff costs and a marked improvement in detection.

The Blighter system also forms part of the perimeter security solution at other major international airports in Europe, United States, South America and Africa. A typical Blighter airport configuration consists of the Blighter B400 Series PESA radar, BlighterView HMI control software and slew-to-cue PTZ (pan, tilt, zoom) thermal imaging surveillance camera systems.

Blighter perimeter surveillance radars meet the unique requirements of airports. They are highly configurable radars that support azimuth from 90 to 360°, elevation beamwidth up to 20°, ranges from 2 to 16 km and four scan rates. Because of their compact size and wide elevation beamwidth they can be mounted high on buildings or other existing infrastructure, gaining an unobstructed view and simplifying power and network access. Because they are solid-state designs they are highly reliable and require near-zero maintenance, giving a low total cost of ownership.

Blighter's combination of technologies including PESA e-scan and Doppler, which are all controlled through sophisticated Digital Signal Processing (DSP) and Waveform Generation (WG) units, allows a wide diversity of radar waveforms and azimuth scan speeds. The Blighter radar allows both fast scanning simultaneous with Doppler velocity filtering using its 'Coactive Doppler fast-scan' capability. Traditional non-Doppler radar can scan fast, whereas traditional Doppler radars rotate slowly.

Blighter's advanced frequency modulated continuous wave (FMCW) transmission technology



is an alternative to the traditional Magnetron pulse transmitters or solid-state pulse-compression transmitters used by older radars. Key attributes of FMCW include an enormous instantaneous dynamic range in the receiver channel, allowing small targets to still be detectable alongside large targets or clutter. FMCW is also very efficient allowing considerably less transmitter power to be required.

In conclusion, sophisticated electronic scanning PSRs are proving increasingly popular with international airports, as they provide highly reliable maintenance-free surveillance of airport perimeters and key airport zones in all weather and light conditions, as well as delivering improved intruder detection performance and considerable



operational cost savings.

Integrated with cameras, the PSR platform combines the strengths of radar – wide area continuous surveillance for detection and location – with the strengths of cameras (recognition and

identification of targets). These technologies also complement each other in other more subtle ways and the platform capability is generally greater than the sum of its component parts.

WorldSecurity-index.com

The Homeland Defense and Security Database



WorldSecurity-Index.com is the only global homeland security directory published in English, Arabic and Spanish on the web and in CD network format.

The Global Security Portal

Advertise on **WorldSecurity-Index.com**
 from only **£515 for 12 months**
 Contact info@worldsecurity-index.com for details
 or call +44 (0) 208 144 5934.



critical infrastructure PROTECTION AND RESILIENCE EUROPE

2nd-3rd March 2016

The Hague, Netherlands

www.cipre-expo.com

Convergence for Enhancing Security

CALL FOR PAPERS

Abstract submittal deadline - 31st July 2015

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.

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.

For further information and to submit your abstract visit

www.cipre-expo.com

"The EU Internal Security Strategy highlights that critical infrastructure must be better protected from criminals who take advantage of modern technologies and that the EU should continue to designate critical infrastructure and put in place plans to protect such assets, as they are essential for the functioning of society and the economy."

Leading the debate for securing Europe's critical infrastructure



www.cipre-expo.com

Exhibit & Sponsorship Enquiries:

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

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

Tony Kingham

Exhibit Sales Director

T: +44 (0) 208 144 5934

M: +44 (0)7827 297465

E: tony.kingham@worldsecurity-index.com

Paul Gloc

Exhibit Sales Manager (UK & Europe)

T: +44 (0) 7786 270820

E: paulg@torchmarketing.co.uk

Denne Johnson

Exhibit Sales Manager (The Americas)

T: +1 918 863 9792

E: dennej@torchmarketing.co.uk

Owned & Organised by:



Hosted by:



Supporting Organisations:



Media Partners:



ECIPS Becomes Inaugurated by Statutory Royal Decree



An historical day for the European Security forces around Europe was that of 14th June 2015, last month when the European Centre for Information Policy and Security (ECIPS) was officially inaugurated by Statutory Royal Decree.

The Statutory Decree was approved by State Justice Department and granted legal powers to by King Philippe of Belgium under article 46 of the Belgian Law in accordance with the International law of International Organization with legal statutory body of its own.

In view of the Act of 27 June on associations not-for-profit and the foundations, articles 46 and 50, 1, respectively modified by articles 282 and 284 of the program act of 2007 December 2004, the ECIPS will function on similar statutory level as any other recognized international organization or agency with one exception that it is to act as the international "Security Watchdog" with its own International Security Council consisting of the 28 European member states.

This is the first time that such powers were granted to act and assemble coordinated partnership not limited to one country, but external information integration and sharing disciplines across borders within the EU. The last time any such structural discipline was approved by any government was when the United States of America established the CIA with similar functions limited to

the 50 states within the USA. This is good news for the fight against terrorism and international crime as a whole, since it is long overdue to have such a body in place that could collectively work internationally under mandate as an independent organ that can remain independent to avoid outside political influences.

What makes this event of significant historical value since the United Nation's inauguration, is the fact that the ECIPS under Article 2 of the statutory Decree, is now officially recognized and given the distinctive function as the Global Security Watchdog on all international security and policy matters effecting the European Union as a whole.

More important is the recognizable reality in that, the newly approved Statutory Decree allows ECIPS to conduct multiple functions to investigate any terror threats across borders whilst mandated to create special multidisciplinary investigation centers to investigate and address high-priority issues such as nonproliferation, counterterrorism, counterintelligence, international organized crime and narcotics trafficking, environment, and arms control intelligence.

Article 6 of the statutory decree allows the formation of the "International Information Policy and Security Council" the "IIPSC" that will be the body of supreme authority in the Organization consisting of the 28 Member States of the European Union.

The new statutory decree give several main tasks with its focuses on the critical global security threats, critical infrastructure threats, cyber threats and research and the develop of pragmatic solutions which aids to the prevention and management of international security risks of security. The ECIPS whom is the controlling body of the CYBERPOL (Cyber-Police) program, paved the final way for the International Cyber Policing Organization, CYBERPOL's statutory decree to be inaugurated.

Mr. Ricardo Baretzky was re-elected by the General Secretariat to remain the President of the ECIPS. The ECIPS Statutory Decree can be read and downloaded on the following page for public use. Link: http://ecips.eu/european_centre_for_information_policy_and_security_033.htm

Understanding the Limitations of Software Security Technologies



Critical infrastructure is essential to all modern economies and is at the core of national security as well. With today's threat landscape having evolved significantly over the past several years and with modern threats increasingly targeting critical infrastructure, we increasingly see successful cyber-attacks causing physical damage to our infrastructures. Damaged critical infrastructure cannot simply be restored from backup the way email and web servers can be restored, nor can loss of life be restored. For these reasons and others, it has become paramount that we provide credible protections to our critical infrastructures and stop relying on ineffective IT-centric solutions.

Modern cyber-attacks are more than just viruses and bot-nets. Modern attacks provide remote control of compromised equipment to remote attackers. These attacks routinely defeat all IT-centric security measures. And, the attackers are not in a hurry; they work remotely, undetected for months or years.

IT Security as the "Gold Standard"

When most of today's best practices were documented, the IT approach to security was seen as the ideal for control systems as well. "If we could only find a way to manage control system

networks the same way as we manage IT networks," we were told, "then all would be well." In the last 5 years though, it has become clear that this guiding principle has failed us.

The beginning of all IT-centric security systems is the corporate firewall, protecting the IT network from attacks coming across the Internet. The problem with IT firewalls is that they are designed to be porous. Electronic mail, web pages, web requests, remote access connections and many other kinds of messages must be exchanged through the firewall between computers

on "protected" IT networks and the Internet. Fundamentally, IT firewalls are designed to exchange messages between "protected" and "untrusted" networks. Every one of these messages may contain an attack. Firewalls try to filter attack messages from benign messages, but no such filtering is perfect. With millions of messages exchanged with the Internet every day, all firewalls permit some number of attacks through to the "protected" IT network.

To a degree, IT best practices do recognize these fundamental limitations of firewall technologies. With IT network perimeters porous by design, IT best practices recommend a host of sophisticated software measures, access controls, and intrusion detection systems to provide additional protections for IT networks.

Encryption is a universally-deployed measure, especially for remote access to corporate systems. With a mobile and



distributed workforce, most IT networks permit interactive remote access across an encrypted VPN tunnel. One way modern attacks defeat encryption is by targeting encryption's endpoints. A well-crafted phishing email, compromising a corporate laptop or workstation, is a routine first step. With a first machine compromised, the attacker now waits until the computer's user establishes a highly-encrypted, extremely-secure VPN connection into a trusted asset, such as a database server, or control system historian server. The attacker then launches a second phase attack right across the highly-encrypted, extremely-secure VPN. Encryption and VPNs offer a degree of protection against man-in-the-middle attacks, but offer no significant protection against a compromised endpoint.

Antivirus is a nearly-universally-deployed measure as well, and is widely regarded as protection against phishing attacks. The truth though, is that antivirus solutions are a signature-based defense and are only effective against known attacks. Signatures do not exist for new malware and signatures are generally not included in an antivirus solution until the new malware has been found in high-volume counts; targeted phishing attacks generally do not reach this level of volume. Attackers adapting malware to a specific target generally make small changes in the malware so that it is "new" and test that new variant against all major antivirus vendors to ensure the "new" variant is not detected.

IT security best practices also demand that control systems be fully patched with security updates, but these programs are ineffective in the face of modern,

targeted attacks. When a targeted attacker has taken control of a machine using phishing or other social engineering, there is no longer a need to "attack" software on that machine or on any other equipment the compromised machine or compromised user is authorized to operate. This is in addition to "watering hole" attacks that, for example, compromise software update websites for popular corporate or control system vendors. Watering hole attacks defeat security update programs by embedding malware in otherwise legitimate security updates.

Intrusion Detection

IT security best practices recognize that IT firewalls are porous by design, and that secondary IT defenses are of limited value. This is why the pinnacle of every IT "defense in depth" security program is an intrusion detection system (IDS). IT security departments generally deploy trained IDS specialists to interpret and investigate alarms, and incident response teams to remediate intrusions. When IT

computers are damaged by an intrusion, the response teams restore those systems from backups.

All of this takes time. Intrusion statistics show that detecting a system compromised by a modern, targeted attack takes an average of 2-3 months, and the average time to remediate a compromised network is over one month. When applied to critical infrastructures, for all of this time, an unauthorized, unqualified intruder is remotely operating equipment on critical control system networks. Worse, some of these attacks result in highly-trained, qualified attackers deliberately mis-operating our networks. These are unacceptable risks to the reliability of our critical infrastructure, to costly equipment at infrastructure sites, and even to employee safety and sometimes public safety.

Solid Security Foundation

The solution to this critical infrastructure control system security problem starts in the same place as IT security started:



at the network perimeter. The interior of control system networks is every bit as “soft” a target as the interior of IT networks, and even more so in most cases. Why then, does it make sense to protect the perimeter of control system networks with porous-by-design firewalls?

Encryption, antivirus, security updates, IDS and other software security controls have a role in modern control system security programs, but these “soft” protections only make sense when supported by a solid foundation of perimeter defense. Modern control system security advice is all moving towards recommending at least one layer of Unidirectional Security Gateways at control system network perimeters rather than just firewalls.

Unidirectional Security Gateways allow information to flow out of control system networks, without ever forwarding even one message back into those critical networks, not one message, not one character, not even one bit of information. The gateways gather information from control system servers and devices, such as plant historian databases, OPC servers, and even Programmable Logic Controllers and other plant equipment. The gateways transmit that information to corporate networks through unidirectional hardware. The hardware is physically able to send information out of a



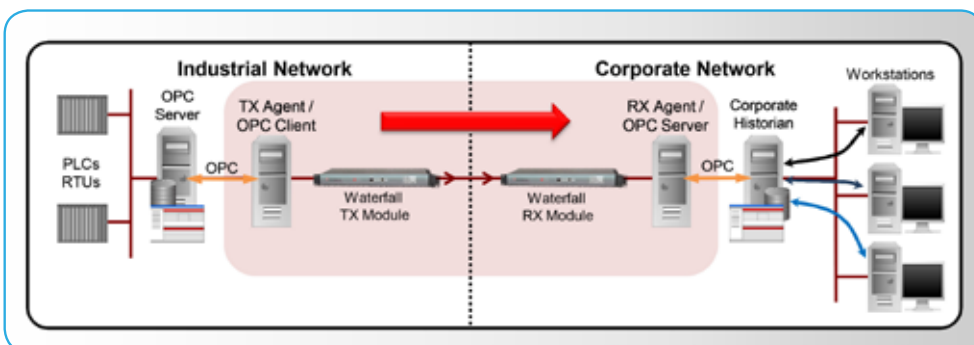
control system network and is physically unable to send anything at all back into those networks. On the corporate side, Unidirectional Security Gateways populate replicas of control system databases and servers, and emulate other servers and devices. Corporate systems needing access to real-time data can query the replica servers on the corporate network and be confident of receiving the same answers from the replicas as would have been received from the originals.

Unidirectional Security Gateways provide corporate systems with continuous, real-time access to control system data, without ever introducing the risk of external network-based attacks into our control system networks. In particular, Unidirectional Gateways make modern, interactive remote control attacks impossible, because no remote control command can penetrate the gateways.

Evolving Best Practice Advice

Standards and guidance bodies around the globe are recognizing that the traditional approach to ICS security is no longer effective against modern attacks. In 2014, France’s Agence Nationale de la Sécurité des Systèmes d’Information (ANSSI) published a new set of control system security standards that take modern, expert opinions into account. The ANSSI standards require unidirectional protections on the connections between the most critical control system networks and any less-critical networks. The ANSSI standards also prohibit any form of Internet-based remote access to the most critical control system networks, whether or not that remote access is over an encrypted VPN.

Similarly, the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) version 5 standards recognize Unidirectional Security gateways as being stronger than firewalls. When Unidirectional Security Gateways are deployed to protect certain kinds of critical control system networks, the CIP V5 standards reduce the number of security controls required for those networks, thereby dramatically reducing the cost of compliance for unidirectionally-secured



networks. The latest draft of the revised National Institute of Standards and Technology (NIST) 800-82 standard for control system security also contains paragraphs of information relating to Unidirectional Gateways and to the roles the gateways have in control system environments.

Training and Awareness

All security standards and best practice guidance recommend a long list of security controls and program elements, but provide little guidance as to the relative importance of these elements. With porous-by-design firewalls connecting control networks to corporate networks, the "barn door" is open to attackers. Why would attackers resort to more sophisticated attacks when they can simply reach into their target

networks through firewalls? With the firewall "barn door" well and truly walled over by Unidirectional Security Gateways, investments in training, awareness, USB device control and many other program elements can finally bear fruit.

Expendable Control Networks?

Best practices, standards and guidance must continue to evolve to address modern, evolving cyber threats. Many layers of security do little to make an organization secure, if all of these layers are essentially porous. Robust control system security programs are built on a solid foundation of network perimeter protection, in the form of modern, Unidirectional Security Gateways. Given how long it takes our IDS experts to detect and our response experts to remediate compromised

equipment, is it acceptable to allow an attacker to remotely control critical equipment for all of this time?

In light of modern attacks and modern best-practice guidance, the question we all need to start asking is "which of our critical infrastructure control systems, and which of our industrial sites are so expendable that we can afford to protect them with porous firewalls and porous security software alone?"

Michael Piccalo is Director of Industrial Security, Waterfall Security Solutions

This article is based on his presentation at this year's Critical Infrastructure Protection and Resilience Asia 2015.



The **European Centre for Information Policy and Security (ECIPS)** focuses on the critical infrastructures and global security threats, cyber threats and pragmatic solutions, that aids to the risks of security, justice and its policy in public domain.

ECIPS are launching their annual conference for providing a key industry platform to deliver a leading conference for informing and educating government and commercial organisations on developing cyber security and cyber resilience strategies, in light of the ever increasing threats from organised criminal activities, boutiques and cyber espionage.

The conference programme will investigate the cyber threats against government departments, corporations and commercial organisations, as well as highlight the challenges and solutions for organisations to consider as part of their overall cyber security strategy.

Join us in Brussels for a unique discussion and insight into future cyber security threats and challenges to your organisation.

The essential cyber security conference for your organisation

The ECIPS conference will be a high level discussion on policy, practice and technology for the following:

- Government agencies and departments responsible for national cyber security and emergency/contingency planning, including:
 - o Law Enforcement
 - o Police and Security Agencies
 - o Serious/Organised Crime
 - o Intelligence
 - o Counter-Terrorism
 - o Digital Forensics
- Local Government
- Heads of Departments in governmental organisations or corporations
- CEO / Managing Director
- Chief Information / Technology Officers
- IT, Cyber Security and Information Directors/Managers
- Security Directors/Managers
- Network Architects / Digital Security

For further information visit:

www.ecips.eu/conference

US Correctional Facilities: Strip Search or Scan?



FACT: In excess of 13 million people are admitted each year to Correctional Facilities in the USA

FACT: In 2012, the United State Supreme Court ruled that strip searches are permitted for all arrests, including non-indictable minor offences before being admitted to correctional facilities, even if officials have no reason to suspect the presence of contraband. <http://www.supremecourt.gov/opinions/11pdf/10-945.pdf>

The debate will rage on over the rights and wrongs of strip searches.

Some people may say that if a "body" is in prison, then they are there for a reason, and as such normal propriety human rights should not exist.

Others like Amnesty International say that it is these very people who are subject to breaches of human rights that need protecting in particular women enduring humiliating full body cavity strip searches by male prison officers.

It is without question that inmates need to be protected from those that wish to do them harm, even from themselves. It is also of paramount importance that Prison Officers and staff are protected, hence the need for strict search procedures on any "body" entering a correctional facility – be that State or County.

Current procedures in most correctional establishments mean that any prisoner having

had a contact visit with a person from outside the institution, be that with a family member or attorney, after court appearances, community service details, hospital visits, and shifts at prison jobs will be subjected to a body search, and in some States, a Full Body Cavity search, exposing their body cavities for visual inspection.

It is a necessary evil for a body to be searched after a contact visit to ensure that no contraband, be that alcohol, drugs, mobile phones, alcohol or weapons can be taken into custodial establishments.

However the degrading practice of an intimate body search where body cavities, (mouth, vagina and anus etc) are visually inspected for any hidden contraband, has led to a number of lawsuits. A number of which have been successful particularly when a person is strip

searched by someone of the opposite sex.

Many jails in the US are bursting at the seams with addicts who have committed petty crimes to fund their habit, who in turn then become prisoners with a habit and attempt to bring drugs into the prison. Other prisoners will bring drugs into the prison system to sell to this ever expanding market.

Current figures (April 2015) from the Federal Bureau of Prisons state that 48.7% of inmates offences were drug related. http://www.bop.gov/about/statistics/statistics_inmate_offenses.jsp

With traditional strip searches missing hidden contraband, many prisons in the US are now changing the way they search inmates after outside contact, with the introduction of body scanners that can see inside



inmate's bodies.

Despite this, inmates will still take deadly chances to smuggle drugs into the correctional facilities, internally, in body cavities, secreted on their person, and even between dentures and gums.

As recently as 8th May, 2015 the Frederick County Sheriff's Office arrested Brittany Ann Sapp, age 23 of Hagerstown, on charges of possession of a controlled dangerous substance (CDS), and possession of contraband in a place of confinement.

Following a traffic stop for a traffic violation on Interstate 70 the vehicle was searched and heroin was located and seized. Sapp was arrested without incident and transported to the Frederick County Adult Detention Center's (FCADC) Central Booking Unit for processing. A body scan was conducted on Sapp with the FCADC body scanner and revealed inconsistencies. Through the investigation it was determined Sapp had transported a baggie of approximately 1.7 grams of heroin in her vagina into the FCADC.

Sheriff Chuck Jenkins commented, "This find of heroin

on the prisoner demonstrates the importance of this technology in the detention center. Very obviously, if the heroin had not been discovered by normal search procedures the inmate would have been at immediate risk along with the fact that the heroin could have entered the facility, jeopardizing the safety and security of the facility and other inmates. In the end it would have created a situation in which the Sheriff's Office would have been liable for any bad outcome. In my opinion, the body scanner has more than paid for itself with this first discovery of heroin on this inmate."

Sheriff Jenkins pointed out that other Sheriff's Offices had already made inquiries about the body scanner and one agency very recently visited the facility for a demonstration.

Heroin is cheap and highly addictive. A sugar packet-sized dose of one gram sells on the street for \$150. Heroin addicts, though, often use it in smaller, cheaper quantities – as little as \$20 – that would be even easier to conceal and to get into the jail.

Some people knowing that they will be arrested for a crime, will purposefully swallow drugs to excrete at a later time; thereby giving them a supply of drugs to

sell inside the prison.

This happens with alarming regularity. Rather than the degrading process of squatting and coughing, this is high on man power, degrading to the inmate, unpleasant for the officer and not at all 100 percent efficient. Only a Body Scanner, such as the SOTER RS by Texas headquartered OD Security North America, will highlight ingested or inserted contraband.

In Westmoreland County, PA the County Prison Board has viewed a proposal from OD Security North America, which sells full-body scanners to jails.

Company President John Shannon said the System, which detects drugs, tobacco, weapons, cell phones and other contraband, would cost \$118,750 to purchase. They offer a leasing program to Agencies that allow the technology to be introduced for under \$20,000 a year.

The company, who are the only US manufacturer of this type of technology, has grown its Client Group since the first installation in 2014 into 9 States.

Warden, John Walton says "every inmate entering the county jail has been strip-searched. The jail, which has 592 inmates, admits between 11 and 15 inmates every day."



During a month-long period last year, four inmates were placed in disciplinary lockup when blood tests showed they used drugs behind bars and last year found 62 stamp bags of heroin a female inmate had smuggled into her cell.

County commissioners ultimately will decide whether a scanner will be added to improve security at the jail.

However it is not just drugs and weapons that are smuggled. At the time of writing, an investigation is being carried out into how two convicted murderers Richard Matt (48) and David Sweat (48) escaped from Clinton Correctional Facility in Dannemora NY on 6th June 2015 using amongst other tools, a hacksaw blade, chisel, punch and screwdriver. Joyce Mitchell, a prison tailoring shop instructor has been charged with supplying



the contraband to the two felons. A second prison worker, Gene Palmer has been arrested and charged with promoting prison contraband in the first degree.

Richard Matt was shot and killed, and David Sweat is back in custody. This was the first escape since Clinton opened in 1839.

In the US some States have now opted to scan not only the inmates before entering the correctional facilities but now include staff members, visitors, contractors etc.

If this had been the case in Dannemora then two convicted murderers would probably still be serving their life sentences rather than costing the US Tax payer \$1 million a day to hunt them down, according to Clinton County N.Y., District Attorney Andrew Wylie.

While Full Body Scanners may not offer a total panacea for the issue of contraband in US Correctional Facilities they will certainly make the issue of choice between "Strip Search" or "Scan" for drugs an easy one.

critical infrastructure
PROTECTION & RESILIENCE ASIA
Including Critical Information Infrastructure Protection



15th-16th June 2016
Bangkok, Thailand
www.cip-asia.com

Save The Dates

Developing resilient infrastructure for a secure future

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

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

On a country level, there are strategies to deal with infrastructure protection issues. On a regional level, there is the Association of Southeast Asian Nations (ASEAN) Agreement on Disaster Management and Emergency Response (AADMER), under which several teams have been set up to deal with disaster management in general, but none is geared towards the protection of critical infrastructure.

Cyber security is also becoming more prevalent, and as more critical infrastructure becomes connected to the internet and exposed to the dangers of cyber security attacks, new strategies and systems need to be developed to mitigate these threats.

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

www.cip-asia.com

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

How to Exhibit

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

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

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

Tony Kingham
Exhibit Sales Director
T: +44 (0) 208 144 5934
M: +44 (0)7827 297465
E: tony.kingham@worldsecurity-index.com

Owned & Organised by:



Supporting Organisations:



Media Partners:



Is ASEAN's Critical Infrastructure fully prepared?

critical infrastructure
PROTECTION & RESILIENCE ASIA



Last month Bangkok hosted the inaugural Critical Infrastructure Protection and Resilience Asia.

The event was co-hosted by Thailand's Department of Disaster Prevention & Mitigation (under the Ministry of Interior), the Ministry of Information & Communication Technology and the Electronic Transactions Development Agency. It was supported by the Ministry of Transport and sponsored by Thailand's Provincial Electricity Authority.

At the opening keynote address Thailand's Minister of Information and Communication Technology Minister Rujiprapa set the tone for the two days of discussions when he said: "We are aware how important critical infrastructure is to our economy, our society and our way of life. Today the infrastructure is crucial to all of us because it provides life necessities, from water and food to electricity and gas. It also provides the telecommunications services that help us conduct our business; and it supports the banking and finance system that keeps our economy running".

"Several years ago, the systems and networks of the infrastructure operated separately. However, they are now so tightly integrated,



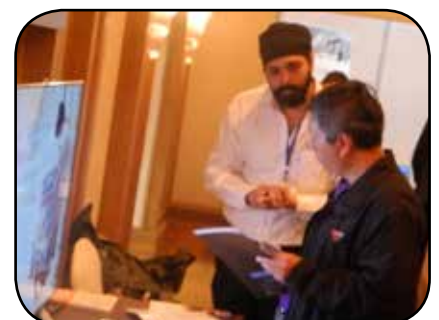
especially with the introduction of "Internet of Things". We must take a totally new path to safeguard our critical infrastructure, and also strengthen our resilience to threats whether they be from terrorism, natural disasters or cyber-attacks".

"We are living in a whole new age of criminal activity. In the past, infamous criminals could have driven across different states. But these days, criminals can commit a thousand robberies on the same day in many countries, without ever leaving their homes. That is the challenge we face today".

"In addition, the recent devastating earthquakes and increasing terrorist activities in Southeast Asia highlight the

need for ASEAN to be prepared and secure against the changing threats. When there is so much at stake and there is no room for failure, no single agency or organization is capable enough, to match the scope and scale of the challenge. We need cooperation among all critical infrastructure partners including government agencies, private owners and operators. We need unity. And it is the reason conferences like this are so important".

Over two days experts from around the world had the chance to share knowledge, expertise and experiences with one purpose in mind, to protect the safety and security of its citizens. The event will be returning to Bangkok 15-16th June 2016.



The Department of Homeland Security (DHS) Science and Technology Directorate (S&T) has announced that another cybersecurity technology has been licensed for commercialization.

This is S&T's third technology that has successfully gone through the Transition to Practice (TTP) program and into the commercial market. The Network Mapping System (NeMS), developed by Lawrence Livermore National Laboratory, is a software-based tool that tells users what is connected to their network so that they know what needs to be protected. This new technology is being licensed to Cambridge Global Advisors, an Arlington, Va. based strategic advisory services firm.

"The brilliant minds of the nation's network of national laboratories are coming up with incredible technologies and solutions," said DHS Under Secretary for Science and Technology Dr. Reginald Brothers. "Transitioning those ideas into the commercial market where they can be put to practical use is a primary objective for S&T."

In 2012, the TTP program identified NeMs as a promising candidate for transition to the commercial marketplace. By mapping a network environment, this technology helps operational users understand what is on their

Third Licensed Technology

» TRANSITIONED

Transition Through Partnership

network, so they know how to better protect it.

"TTP's goal is to find technologies with the potential to strengthen our nation's cybersecurity posture and assist those technologies in making the difficult journey from the research lab to the commercial marketplace," said TTP Program Manager Mike Pozmantier. "And as long as these innovative technologies are transitioned to a commercial or government end-user we're making a positive impact on the cyber landscape."

Established in 2012 as part of S&T's Cybersecurity Division in an effort to support the Department's mission of improving the nation's cybersecurity capabilities, the TTP program looks to transition federally-funded cybersecurity technologies from the laboratory to enterprise consumers. The

program, led by S&T's Michael Pozmantier, also seeks to create institutional relationships between the cyber research community, investors, end users, and information technology companies by showcasing the technologies throughout the country to develop pilot and commercialization opportunities. The next TTP technology demonstration event will be featuring fiscal year 2015 technologies to the finance sector and will be held in New York City on August 19, 2015. While this event targets the finance sector, registration for this event is free and is open to all cyber security practitioners, technology investors, systems investigators and IT companies.

Each year the TTP program selects eight promising cyber technologies to incorporate into its 36-month program. S&T introduces these

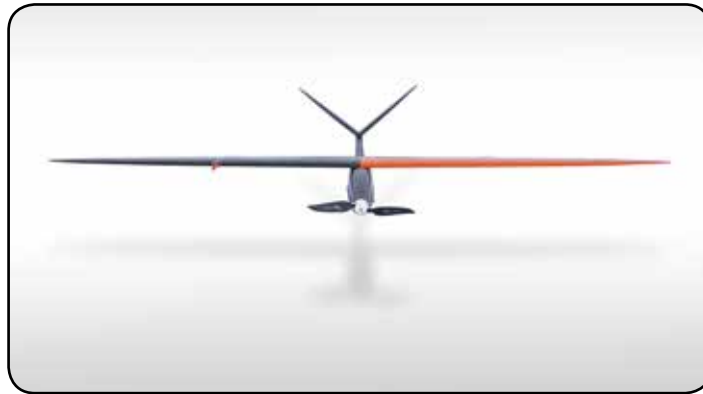
technologies to end-users around the country with the goal of transitioning them to investors, developers or manufacturers that can advance them and turn them into commercially viable products.

Now in its third year, TTP has 24 technologies (eight from Fiscal Year 2013, nine from FY 2014 and seven from FY 2015) that are ready for transition to the marketplace. Of those 24, three technologies—Quantum Secured Communication, Hyperion, and now NeMS – have successfully transitioned into the marketplace through commercial licenses. In the next few months S&T will introduce eight new technologies into TTP's FY16 class and will start to showcase these technologies to critical infrastructure sectors and potential investors.

"With the success of the NeMs technology transition, S&T hopes commercial technology partners and end-users will take notice of other technologies, not only in the TTP program, but in the entire government research and development community, as solutions to complex problems," said Pozmantier.

Delair-Tech creates and commercialises the first civil drone connected to 3G network

eDelair-Tech, French civil drone manufacturer and Telefonica Business Solutions, a provider of a wide range of integrated communication solutions for the B2B market, have signed a unique partnership to connect DT18 and DT26X drones to 3G network.



terrains and situations, such as steep reliefs and mountainous areas, or over long distances to monitor infrastructure like pipelines or railways. With this enhanced and enlarged monitoring ability, the possibilities that this partnership enables really are endless.

Using 3G network to pilot drones beyond visual line of sight. Thanks to this strategic roaming agreement to utilise Telefonica's Smart m2m solution, Delair-Tech will be able to offer its customers the ability to communicate with their drones regardless of distance and across several countries and territories. This opens up a

wealth of new possibilities and perspectives for the use of mini drones in industry. For the first time a Telefonica 3G SIM card can be embedded into the drones and then delivered to Delair-Tech customers.

A new step in the conquest of the BtoB market by Delair-Tech
Thanks to their

manoeuvrability, autonomy and the precision of their footages, the DT18 and DT26X drones created by Delair-Tech are perfectly adapted to the control and monitoring of any sites whether industrial or natural. From now on, the 3G connectivity will enable customers to lead operations in difficult

This agreement reinforces Telefonica's position as a provider of telecommunications services to multinationals in the French market where the telco has recently announced the creation of a joint commercial organization with Bouygues Telecom to generate new business sales both within France and internationally.

Smiths Detection Inc. Announces \$27m order from U.S. Army for Mobile Medical Shelters

Smiths Detection Inc. (SDI) has received a \$27.7 million follow-on production order from the Department of the Army for Chemical Biological Protective Shelters (CBPS).



SDI's CBPS-M8E1 systems are specialized, highly mobile medical shelters. They are designed to military specifications, are highly resistant to chemical and biological threats and can be used in natural disasters and other

emergencies, such as a potential terrorist attack response. They build on SDI's chemical and biological detection and identification expertise by providing the military a highly mobile, chemical/biological agent-free environment and safe

haven for patients in which to administer healthcare without the need for protective clothing. CBPS systems are manufactured at Smiths Detection's U.S. headquarters in Edgewood, Maryland.

Terry Gibson, SDI President, said: "Our mission is to deliver technology solutions for a safer world. The highly innovative CBPS not only provides soldiers and caregivers with a safe working environment, its dual-use mobility can also give civilians shelter in times of need. This program clearly aligns with our mission and unwavering commitment to bring to life smart, versatile technology to help safeguard society."

Raytheon delivers operational border security capability to Hashemite Kingdom of Jordan under DTRA contract

Raytheon Company has delivered operational capability under a \$79 million Defense Threat Reduction Agency (DTRA) contract to help the government of the Hashemite Kingdom of Jordan (GoHKJ) secure its borders with Syria and Iraq. The contract included the delivery of key command, control, communications, and surveillance (C3/S) capabilities to the Jordanian Armed Forces. The operational capability, provided three months ahead of project completion, is now in use by Jordanian Armed Forces (JAF) to help safeguard the kingdom.

The contract was celebrated at a recent ribbon cutting ceremony at the Border Security Operations Center (BSOC). The ceremony was attended by His Royal Highness Prince Faisal bin Hussein, other Jordanian officials, U.S. Ambassador Alice G. Wells, DTRA leaders and Raytheon executives.

"Raytheon delivers border



security capabilities across the globe that help protect countries from a wide range of threats," said Dave Wajsgras, president of Raytheon Intelligence, Information and Services (IIS). "This work is vital in the Middle East, and we are particularly pleased that we were able to deliver these critical security capabilities to Jordan ahead of schedule."

"We use a product-agnostic approach and tailors border security solutions to the host nation's specific needs," said Todd Probert, vice president of Mission Support and Modernization at IIS. "Our team has delivered on

that model supporting DTRA border security contracts across the world in southeast Asia, eastern Europe and in Jordan. In total, the systems we have installed protect 4,500 miles of borders."

Raytheon will also be providing additional capabilities and services, which includes:

- Design, implementation and testing of a complete C3/S system that includes radars, electro/optical infrared cameras, communications, and command and control software
- Design, integration and testing of 18 quick reaction team vehicles
- Design, acquisition and

testing of solar-based renewable power systems

- Integration of all sensors into a common operating picture using Raytheon Clear View™ Security Solutions
- Upgrades to the BSOC, a training center, maintenance workshop and an equipment warehouse
- Training of operators, administrators and maintainers of the system and transition of system and sustainment capability to the JAF Border Guard Forces

The event in Jordan follows the recent opening of a Raytheon-implemented National Coast Watch Center in the Republic of the Philippines and award of a contract to continue border security work in that country. Raytheon's border security work supporting DTRA is part of the cooperative Threat Reduction Integrating Contract (CTRIC II), awarded in April 2011, as a multiple award indefinite delivery, indefinite quantity contract.

WorldSecurity-index.com

The Homeland Defense and Security Database

Metrasens launch of Cellsense® Plus™ for cell phone, weapon and contraband detection

Metrasens has announced the launch of new Cellsense® Plus,™ which joins the Cellsense line of search and detection products used to target cell phones, weapons and other concealed contraband.

Stopping illicit prison use of cell phones blocks inmates from intimidating witnesses, threatening victims, organizing crimes and plotting escapes.

Simon Goodyear, PhD, Metrasens' CEO stated "Compared with the best performing competitive products, Cellsense Plus has twice the detection sensitivity



and is also much better at cutting interference from surrounding activity, resulting in 50% fewer unwanted alerts. The result is that Cellsense Plus will detect smaller concealed items even in the most challenging

environments. With its patented CrossBeam™ technology, Cellsense Plus enables secure-area protection so you can rapidly create and move restricted zones within your facility."

Cellsense Plus joins the

present Cellsense product line, the leading detector of contraband and all cell phones, used in facilities across the United States and around the world, in 38 countries to date.

Recognized as the most versatile detector, it adapts quickly and simply for portable or checkpoint searches of people or objects, indoors or outside. Cellsense is portable or wall-mounted for head-to-toe walk-by screening of subjects, providing a faster and more thorough search that finds small blades and all cell phones, on or off, concealed on or inside the body

BCB lands surveillance drone orders

BCB International have successfully delivered the first orders of a newly developed small vertical take-off and land (VTOL) Unmanned Air Vehicle (UAV) which weighs less than a typical large loaf of bread.

The company produce a range of unmanned air systems which vary in sizes and can be deployed in confined spaces, maritime environments as well as in search and rescue operations.

BCB International's Managing Director, Andrew Howell, said: "Following successful trials and



training in India as well as an unspecified European Country, the first deliveries of our SQ4 unmanned air system represent an important milestone for the company.

"The customers had quite different needs. One of the end users is a Police special surveillance team and the other a specialist military

force. While the end use is different, both had similar evaluation trials in so far as the flight duration of 35 minutes and range at 2.4km were both rigorously tested and proven."

BCB International also had to prove as part of the training package that the SQ4 was quick to launch and easy to operate.

Andrew Howell added: "Set in full auto mode a mission can be activated within minutes and the SQ4 can be left to conduct the mission in a fly and forget method which can be overridden at any time during the flight. This function allows the soldier or police officer to carry out their duties without having to become a pilot."

Weighing in at under 600 grams (battery included), the small, powerful and agile SQ4 falls into less rigorous regulatory controls than larger and heavier UAVs with comparable performance characteristics."

FLIR Systems Receives Production Order Totaling \$19.5 Million From U.S. Customs and Border Protection to Support Mobile Surveillance Capabilities

FLIR Systems has announced that it has received a production order totaling \$19.5 million for its Mobile Surveillance Capabilities (MSC) systems, the second option exercised for the procurement of additional units under its five-year firm-fixed price

contract with the U.S. Department of Homeland Security, U.S. Customs and Border Protection (CBP).

FLIR's MSC system is an integrated mobile surveillance and detection vehicle made to operate day and night in rugged

areas of the U.S. southern border, and features FLIR's TacFLIR 380HD long-range stabilized multi-sensor system and a long-range radar integrated into a vehicle-mounted surveillance tower. The contract builds on FLIR's long-term history of providing

U.S. CBP with advanced surveillance systems.

Production of the MSC systems will be performed in FLIR's facility in Elkridge, MD, and fulfillment of the option is expected to occur over the next 12 months.

UTC Aerospace Systems launches low cost, 320-MicroSWIR™ camera, making Sensors Unlimited SWIR more affordable and more exportable

UTC Aerospace Systems introduces the Sensors Unlimited 320CSX, the latest in its line of MicroSWIR™ high performance short wave infrared (SWIR) video cameras. The low-noise, rugged SWIR camera provides customers with an unprecedented opportunity to get the size, weight, power (SWaP) and capability of a Sensors Unlimited MicroSWIR™ camera at a very affordable price, and without ITAR restrictions.

This SWIR camera's performance, reliability and low SWaP make it ideal for use in a variety of industrial applications that include process monitoring, enhanced vision and persistent surveillance.

"Many of our industrial customers have been



asking for a more affordable, small SWIR imager and our product design team did a great job of answering the call," said Bob Jones, director of sales for Sensors Unlimited. "We're very proud of this new addition to the Sensors Unlimited MicroSWIR™ family, and look forward to sharing the experience with our customers."

On the front end, the 320CSX offers an industry standard C-mount lens interface, which allows

it to adapt to a variety of commercial-off-the-shelf lens options. On the backend, the camera offers a modular output, which will initially provide RS170 analog video, CameraLink® digital video, and RS232 command and control, but may be expanded to offer other industry standard interfaces.

At its core, the 320CSX camera provides ¼ VGA resolution (320x256 pixels, 12.5 micrometer pixel

pitch), weighs less than 55 grams, measures 1.25 inches on each side, uses less than 2 watts of power at 20 degrees C, operates from -40 to 70 degrees C case temperatures, and provides a range of features to optimize imagery in a wide variety of lighting conditions.

Like all members of the MicroSWIR™ product family, the 320CSX was built for rugged operation and includes the assurance of MIL-STD-810G environmental testing.

UTC Aerospace Systems designs, manufactures and services integrated systems and components for the aerospace and defense industries. UTC Aerospace Systems supports a global customer base, with significant worldwide manufacturing and customer service facilities.

J&S Franklin target Middle East airports

With two key UK airports already protected by Defencell Profile, J&S Franklin is looking to build on its success, particularly in the Middle East, where sales manager Jeremy Milton says talks are ongoing, with potential customers in the United Arab Emirates and Saudi Arabia.

Public places like airports are incredibly vulnerable to vehicle borne improvised explosive devices (VBIED's), one of terrorists most devastating weapons.

DefenCell is already widely deployed protecting airports like Gatwick and Belfast as well as military and government establishments worldwide, including some in the Middle East.

Jeremy goes on to say that "Profile 300 is especially suited for inconspicuous deployment at public buildings such as airports and other critical infrastructure, particularly in environmentally and visually sensitive locations where it can be easily grassed or planted, and quickly blends into the surroundings whilst still providing proven



protection from terrorist attack and environmental threats."

Defencell is a cellular, polypropylene geo-textile containment system or container, which when looked at from above gives it a honeycombed appearance. It is this cellular design and specialised material that gives it its strength and flexibility. The cells can be filled with a variety of locally sourced materials such as soil, sand, gravel or small rocks, to build a wide variety of structures for perimeter security protection. The cellular system means that

any impact is dissipated along the length of the barrier rather than at the point of impact, unlike concrete which is forced backwards. This means that the barrier is able to stop an 18.5-tonne truck travelling at 40 mph (64 km/h). It also has very good blast mitigation properties to protect against car bombs and VBIED's.

It is incredibly quick and easy to erect and requires little training. With a standard mechanical digger and compacting tools 30 to 50 m of protective barrier can be erected in a single day. That makes it ideal

for emergency barriers in times of heightened security, which can then be easily dismantled once the security threat has passed.

Defencell containers are able to be stacked to create walls, barriers or berms, which can stay in place for 20-30 years with minimal maintenance or pulled down and recycled cheaply and quickly.

Defencell has a number of logistical advantages as well, a single standard pallet of DefenCell weighs less than 350kgs and provides sufficient units to build a 2 metre high wall more than 40 metres long, which means it can be easily stored locally in a warehouse or store room and deployed quickly by hand if necessary by airport staff.

Unlike many other barrier systems, DefenCell has multiple uses; it can be used to build collective protection areas, entry control chicanes and guard posts, and has also been deployed very effectively by the US military as flood barriers.

Cubic Awarded New Maritime Security Contract Covering Ports in Mexico and Colombia

Cubic Applications, has received its fourth contract to provide seaport assessments and security training from the Secretariat of the Inter-American Committee

Against Terrorism of the Organization of American States (OAS).

Cubic's new contract covers security services for the Mexican ports

of Ensenada, Mazatlan, Puerto Vallarta and Salina Cruz, and the Colombian port of Turbo and is a follow-on to an award received last year for assessments and training

in the Mexican ports of Cozumel, Cabo San Lucas, Coatzacoalcos and Manzanillo as well as the Colombian port of Buenaventura.

IPS (International Procurement Services Limited) has launched a new Web Site for Government, Law Enforcement and Corporate Clients

IPS supply security solutions, debugging sweep team services, countermeasures and consultancy services, and are the leading international distributor for Research Electronics International (REI) and the only company in the UK authorized to offer certified training on REI technical surveillance counter measures equipment, including the OSCOR GREEN, ORION & TALAN.

The new Web Site (www.intpro.co.uk) is broken down into 6 areas of specialisation; OSCOR Green (Countermeasure Receiver), Counter Surveillance Equipment, Surveillance Equipment, Counter Terrorism Equipment, IPS Counter Surveillance Sweep Team and a new Restricted Area, accessible only by username and password. Included in the new web site are several new products, including the REI ORION 2.4HX Non-Linear Junction



Detector which is now available in either 3.3 or 6.6 watts versions with several added features over the standard 2.4 version.

The ORION 2.4HX is a smaller, lighter Non-Linear Junction Detector with an operational weight of less than 1.4kg whilst providing an overall extended length 147cm. Utilizing a 2.4 GHz digital spread spectrum transmit frequency for better sensitivity, a transmit power of 6.6 watts, manual or auto power control and a digital transmit modulation of 1.25

Mhz. There are over 60 transmit channels, which can be selected either manually or automatically.

The ORION 2.4 HX has a completely new polycarbonate body and antenna head design providing a variety of new user benefits. It has a new touch screen controller built into the handle, an antenna mounted display and bar graph display. It also has the same extendable pole mounted line of sight antenna display as the ORION 2.4. It has no cables,

pole sections or transceivers, making set up quick, quiet and easy. An antenna mounted LED headlamp provides illumination of surfaces and low lit areas, especially beneficial at extended lengths. Customer user settings and screen captures can be saved to micro SD cards and a USB port can be used for future software updates.

The ORION 2.4HX NLJD comes complete with 2 rechargeable Lithium batteries, providing more than 4 hours of life per battery and a charge time of 2.5 hours.

The ORION 2.4 and ORION 2.4 HX introduce a new generation of NLJDs, made to detect and locate hidden electronics, regardless whether the device is radiating, hard wired, or turned off, including eavesdropping devices, recording devices, cell phones and other electronic contraband.

Lattice Awarded Homeland Security Contract for Smuggled Currency Detector

Lattice Incorporated, a provider of advanced technological solutions to key government agencies and enterprise customers, announced today that its wholly-owned subsidiary Lattice Government

Services, Inc. has been awarded a prime contract by the Department of Homeland Security (DHS) to develop a demonstrable prototype device able to search for and identify bulk

quantities of currency.

To address the challenges of bulk currency detection, Lattice Government Services has teamed with the University of Washington

to research, design and develop a special purpose concealed sensor platform specifically targeted to identifying large quantities of U.S. and Canadian concealed currency as well as Euros.



Blighter
Surveillance Systems

+44 1799 533200
www.blighter.com
sales@blighter.com



SAS ROD
THE LATEST IN
CONTRABAND
TECHNOLOGY

Find Out More



THE MOST FLEXIBLE AND EFFECTIVE
TRANSMISSION X-RAY FULL BODY
SCREENING SYSTEM

ADANI
From Ideas to Solutions

DETECTION CAPABILITY:
Objects hidden internally and externally
on the body; within prosthetic devices,
artificial limbs, shoes etc.

COMPASS DV

DUAL VIEW
- DUAL GENERATOR
- DUAL IMAGE
- DUAL EFFECTIVENESS

www.adanisystems.com

World Security Report



World Security Report is a quarterly electronic, fully accessible e-news service distributed to over 40,000 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.

Targeted Solutions to your PR & Marketing Needs

KNM MEDIA

Specialising in the
Aerospace, Defence and
Security Markets

smiths detection



Checkpoint security solutions for today and tomorrow

www.smithsdetection.com

World Security Report



World Security Report is a quarterly electronic, fully accessible e-news service distributed to over 40,000 organisations globally. It tracks the full range of problems and threats faced by today's governments, security and armed forces and civilian services and looks at how they are dealing with them. It aims to be a prime source of online information and analysis on security, counter-terrorism, international affairs and defence.



HIDDEN TECHNOLOGY
systems international ltd.

Discrete tracking devices for personal protection and vehicle security.

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


In use by Police, Military and Government organizations worldwide.

www.hiddentec.com

Border Security Matters



Border Security Matters is the quarterly newsletter of BORDERPOL, the World Border Organisation, delivering agency and industry news and developments, as well as more in-depth features and analysis to over 10,000 border agencies, agencies at the borders and industry professionals, policymakers and practitioners, worldwide.



SOTER RS
security bodyscan - safety only takes a few seconds

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

Download the latest version of our brochure

your partner in the fight against drugs and terrorism



Wagtail International
leading specialists in detection dogs and dog handler training



Click here to view our profile



DEFENCELL

PROFILE 300 & DC BARRIERS
HOSTILE VEHICLE MITIGATION

www.defencell.com

International Procurement Services (IPS)



Electronic Countermeasures
Equipment Sweep Teams
Training

www.SECURITYSEARCH.Co.Uk

August 2015**16-19**

APCO 2015, Washington, USA
www.apco2015.org

18-19

Midwest Security & Police Conference/Expo,
 Illinois, USA
www.mspce.com

18-20

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

26-27

Africa Commercial and Corporate Security Summit,
 Johannesburg, South Africa
<http://africaccsecuritysummit.com>

August 2015**2-4**

IFSEC South East Asia
 London, UK
www.ifsecsea.com

September 2015**8-10**

Security Middle East Show
 Biel, Lebanon
www.smesbeirut.com

9-11

Kazakhstan Security
 Astana, Kazakhstan
www.kss-expo.kz/en

14-16

Oman Fire, Safety & Security
 Muscat, Oman
<http://muscat-expo.com/ofsec>

15-18

DSEI
 London, UK
www.dsei.co.uk

15-19

Prague Fire & Security Days
 Prague, Czech Republic
www.fsdays.cz



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

October 2015**20-21**

National Security & Resilience Conference
 London, UK
www.nsr-conference.co.uk

November 2015**17-18**

The ECIPS Conference, Brussels, Belgium
www.ecips.eu

December 2015**8-10**

4th World BORDERPOL Congress, The Hague,
 Netherlands
www.world-borderpol-congress.com

March 2016**2-3**

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

June 2016**15-16**

Critical Infrastructure Protection & Resilience Asia,
 Bangkok, Thailand
www.cip-asia.com

WorldSecurity-index.com

The Homeland Defense and Security Database



4th World BORDERPOL Congress

8th-10th December 2015

The Hague, Netherlands

Speakers include:

- Pol. Mj. Gen. Apichat Suriboonya, Head of INTERPOL NCB Thailand, Commander of Foreign Affairs Division, Royal Thai Police
- David Parradang, Comptroller, Nigeria Immigration Service
- Goran Stojkovski, Border Management Officer, OSCE Office in Tajikistan
- Ricardo Baretzky, President, CYBERPOL
- Krum Garkov, Executive Director, EU-LISA
- Didier Clergeot, Coordinator, INTERPOL IBM Task Force
- Florian Forster, Head, Immigration and Border Management Division, International Organisation for Migration
- Mark Singleton, Director, International Centre for Counter-Terrorism
- Clarence Yeo, Chief Commissioner, Immigration & Checkpoints Authority
- Major Issa Al Shaibi, Passenger Information Centre Manager, Royal Oman Police
- Hans de Moel, Royal Netherlands Marechaussee

Enhancing collaboration in global border protection and management challenges.

REGISTRATION NOW OPEN

Book online today and save with the Early Bird.

The World BORDERPOL Congress is the only multi-jurisdictional transnational platform where the border protection, management and security industry policy-makers and practitioners convene annually to discuss the international challenges faced in protecting not only one's own country's borders, but those of neighbours and friends.

Join us for developing co-operation and collaboration through high level discussions and presentations on the future for border protection and management.

Visit www.world-borderpol-congress for further details and the Congress programme.

We look forward to welcoming you to The Hague, Netherlands on 8th-10th December 2015 for the next gathering of border and migration management professionals.

www.world-borderpol-congress.com

Owned & Organised by:



Supported by:



Media Partners:

