www.intersec.co.uk

# intersec

The Journal of International Security

January 2020


## SEARCH AND DESTROY

Why TSCM remain vital

## DISASTER RECOVERY

Ensuring business continuity in the event of an incident

POLMIL®

# ON-GROUND RELOCATABLE SECURITY FENCING

POLMIL® CPNI ASSESSED

POLMIL® PAS 68 RATED
(Test Reports on Request)

POLMIL® MOB ATTACK TESTED

POLMIL® TESTED AND PROVEN

POLMIL® HOT DIPPED GALVANISED FOR COASTAL ENVIRONMENTS

POLMIL® WITH WATER BALLAST

POLMIL® IS A DIVISION OF BLOK N MESH UK LIMITED

THE QUEEN'S AWARDS FOR ENTERPRISE: 2016

## Specialists in the Design and Manufacture of CPNI assessed on-ground relocatable security fencing systems for Potential Target Sites


**UK Office -** Hammond Road, Knowsley Industrial Park, Liverpool, Merseyside, L33 7UL

**Tel: UK +44 (0) 151 545 3050**

**France Office -** Batisec, 67 Rue Du Creusot, 59170, Croix

**Tel: FR +33 (0) 3.20.02.00.28**

**Qatar Office -** 7th Floor, Al Reem Tower West Bay. PO Box 30747 Doha, Qatar

**Tel: Qatar +974 6652 1197**

**www.polmilfence.com**

intersec
Volume 30 Issue 1
January 2020

Cover photograph: Getty

**Editor**
Jacob Charles

**Principal Consultant Editor**
Maj. Gen.
Julian Thompson CB OBE

**Design & Production**
jellymediauk.com

**Published by**
Albany Media Ltd
Warren House
Earlsdown, Dallington
Heathfield, TN21 9LY

Tel: +44 (0) 1435 830608
Website: www.intersec.co.uk

**Advertising & Marketing**
Director of Sales
Arran Lindsay
Tel: +44 (0) 1435 830608
Email: arran@intersec.co.uk

**Editorial Enquiries**
Jacob Charles
Tel: +44 (0) 7941 387692
Email: jake@intersec.co.uk

**Subscriptions/Accounts**
Faye Barlow
Tel: +44 (0) 1435 830608
Email: subs@intersec.co.uk
www.intersec.co.uk

# EDITORIAL COMMENT

As we go to press it's safe to say that providing any meaningful comment about the ever-evolving situation in Iran is risky to say the least. The first time I sat down to write this intro the "World War III" hashtag was trending on Twitter and while it's probably fair to suggest that this is perhaps an overly alarmist response to the US assassination of Qassem Suleimani in early January, it's unclear at this early stage quite how things will progress.

Unsurprisingly, Donald Trump has demonstrated the sort of gung-ho stance that you'd expect from someone desperately trying to turn the public's attention away from his impending impeachment, mocking Iran on Twitter with claims that it will never have a nuclear weapon, while suffering widespread criticism for his threat to attack some of the country's cultural treasures. Elsewhere the dialogue appears to be more measured, with UK Foreign Secretary Dominic Raab suggesting the "overwhelming message that the Prime Minister and I are conveying to our European and American counterparts, and also critically our partners in the Middle East, is the importance of deescalating the tensions and finding a diplomatic way through this crisis."

Muddying the waters further is Iraq, which has relationships with both the US and Iran. Carefully navigating his way through a decidedly delicate situation, a spokesperson for Iraq's Prime Minister, Adel Abdul-Mahdi, told Reuters: "The Prime Minister stressed the importance of mutual cooperation on implementing the withdrawal of foreign troops, in line with the Iraqi Parliament's resolution, and to set relations with the United States on a proper foundation. He stressed how dangerous the situation is right now and its potential consequences, adding that Iraq is doing everything it can to prevent the descent into open war."

While Iran couldn't realistically hope to hit back at the US in traditional open warfare, one area that has received little media coverage is its potential threat when it comes to cyber attacks. As Dr Duncan Hodges, Senior Lecturer in Cyberspace Operations at Cranfield University, notes: "Iran is a credible offensive actor in cyberspace having moved in recent years to boost their military capability in this area – in the past, they relied on third-party groups and supportive hackers to carry out attacks... its history of cyber attacks has been more destructive rather than manipulative. They have looked to destroy and degrade infrastructure and hardware... They have also not traditionally been too worried about being identified after the event, using detection as a way to demonstrate their strength in this area... With the present conflict we could, for the first time, see cyber attacks used to escalate conflict." Though how this will play out remains unclear, you can be sure we'll be covering events in Iran in the future.

**Jacob Charles, editor**

**Editorial contact**
Please address all correspondence to The Commissioning Editor: jake@intersec.co.uk

**Subscriptions**
Annual Subscription Rates: UK £150, Europe £180.
USA post paid US$350
Other Countries air-speeded £220. Subscription Enquiries: subs@intersec.co.uk
Average net circulation per issue: 10,510
intersec (USPS No: 006-633) is published monthly except Jul/Aug and Nov/Dec combined issues, by Albany Media Ltd

Subscription records are maintained at Albany Media Ltd, Warren House, Earlsdown, Dallington, Heathfield, TN21 9LY

Issue Date: November/December 2019
All rights reserved. No part of this publication may be reproduced in any form or by any means, electronic, mechanical, photocopying, recording or otherwise without prior written consent of the publisher. Opinions expressed in articles or advertisements appearing in intersec are those of the author or advertiser and do not necessarily reflect those of the publication nor of its publisher.

# CONTENTS

January 2020 www.intersec.co.uk

intersec

## Features



## Regulars









MGT europe

# DroneTERMINATOR

**USING EVOLUTION JAMMER TECHNOLOGY**

- **DETECTS**
- **TRACKS**
- **NEUTRALIZES**

**DroneTERMINATOR utilizes RADAR on the Ku / X band, 2 Watt, 1 GHz bandwidth Long-Range Radar System to detect UAVs at a distance of up to 6 km, with micro-drones typically detected at 1-2 km realistically**

## JAMMING FREQUENCIES:

**400 MHz - 900 MHz - 1500 MHz - 2.4 GHz - 5.8 GHz in n. 2 bands**

**FEATURES:**

- *Fully modular smart design*
- *Precise and fully programmable operation mode for each R.F output*
- *Wideband, clean and precise band occupation*
- *Very good Narrowband and Wideband spectral purity*
- *Flexible and multiple User interface options*
- *Standard USB and Ethernet interfaces available for multiple purposes*
- *Software oriented approach allows for long product life expectations*
- *Careful D.C. Power source design choices for efficient power supply utilization*
- *Waterproof cabinet, rugged and reliable construction*
- *Linux based, User friendly Graphical User Interface with 7" LCD color Multitouch Display*

**MGT Europe** www.mgteurope.com

# 2019 ends with another preventable attack

**Major General Julian Thompson CB OBE** Principal Consultant Editor

**A recent summary of deaths caused by terrorism worldwide makes some interesting observations. Few will come as a surprise to readers of *Intersec*, but they are a commentary on the inward looking nature of the media in the UK; summed up by the statement: "Media coverage of terrorism is often disproportionate to its frequency and share of deaths". From reportage in the print, and other forms of media in the UK, one would be hard pushed to discover that, for example, 94 percent of deaths caused by terrorism in 2017 occurred in the Middle East, Africa or South Asia; in many cases the victims were co-religionists of the perpetrators.**

A table confined to covering terrorist incidents with more than 100 deaths in the first six months of 2019 supports this assertion. The Afghan Defence Ministry official figures for an attack by the Taliban in Madan Shar in January 2019 are 126 dead and 70 injured. In Kajaru, Nigeria, Fulani gunmen and Adara militia accounted for 140 deaths with an unknown number of injured. In Mali in March, 160 Fulani herders were killed and more than 70 injured in an ethnically motivated shooting. In April, it was the turn of Sri Lanka to suffer, with 259 dead and over 500 injured at the hands of homegrown terrorists probably assisted by Islamic State. In May there were no incidents with more than 100 deaths. In June, it was Africa that topped the statistics. In Khartoum local security and paramilitary forces got out of hand and killed at least 118 people and injured more than 650. At the same time, shootings by militias in the Democratic Republic of the Congo accounted for more than 240 deaths and an unknown number of injured.

Just in the month of November, there were a total of 13 terrorist incidents recorded worldwide; with car bombs accounting for the majority of deaths and injuries; more may be listed as time goes by and records come in. Islamic State claims the top score in November 2019 with 54 dead in Northern Mali. The last of such incidents in November are the two deaths and three injuries at London Bridge. The attacker was a 28-year old convicted terrorist called Usman Khan, who stabbed two people, and was also wearing what turned out to be a fake suicide belt. He was shot dead by the police. Islamic State claimed responsibility for the attack, but without giving evidence.

Of all the incidents listed above, the London Bridge attack was arguably the most preventable and its outcome the most predictable. Neither of these comments should be taken as denigrating the courage of those who tackled Usman Khan, thereby undoubtedly saving many more lives and preventing further injuries. Nor should they be taken as criticism of the two young people who were killed while attempting to rehabilitate Khan in a session at the Fishmongers Hall in the City of London, just North of London Bridge.

Picture credit: Getty

**Police rush to the scene of the London Bridge attack, but should it have been prevented?**

Why was the incident when seen against the other incidents worldwide in November 2019 possibly the most preventable? Usman Khan was a convicted terrorist operating in a country with one of the best police services in the world, and who had been released after serving half his sentence. He was allowed to enter Fishmongers' Hall without even the kind of rudimentary security check that the average British citizen, like the writer of this piece, has been and still is routinely subjected to before being allowed entry to public spaces. It would be interesting to know whether this lack of security was a conscious decision, one whose outcome proved fatal for two unfortunate people, simply because the fact Khan was carrying two knives was not discovered. Even the most half-baked check would have revealed the knives and/or fake suicide vest.

The incident might not have occurred had those who decided to let Khan back into the community been aware they had been duped. There doesn't seem to have been any assessment of the threat, which included the possibility that Khan as a student and personal friend of the Islamist extremist Ajem Choudary, might be lying to fool officials into believing that he was no longer a threat. The Hadith, the words of the prophet Mohammed, make it clear that Muslims are allowed to lie to unbelievers in order to defeat them or protect themselves. This can take several forms including Tawriya, intentionally creating a false impression, or Muruna, blending in.

The outcome was also predictable in that politicians of varying political persuasions took the opportunity to deflect blame away from themselves for the state of affairs that enabled Khan to fool the authorities or the legislation governing early release of terrorists. While the usual suspects in the media did not disappoint by jumping on the bandwagon and mouthing sanctimonious platitudes about not using the incident for political point scoring.

Picture credit: Getty

# TECHNICAL SECURITY REALITY

**Paul D Turner** *explains why technical surveillance counter measures (TSCM) remain as vital as ever in the current climate*

**It is a well-established fact that cyber security generally sees the lion's share of the available budget and support resources often at the expense of a formal technical security programme. Confused? There is a difference between cyber security and technical security and it is essential that the often-subtle overlapping differences be understood and addressed by the organisation. A formal technical security programme is an often-overlooked professional discipline, mainly because those responsible mistakenly presume that somehow it is covered adequately under the cyber security or physical security banner.**

A formal technical security programme must include a competent and wide-ranging Technical Surveillance Counter Measures (TSCM) component, which is just as important – and in some instances more so – to preventing the compromise of everything worth securing within the targeted organisation, including certain aspects and human factor vulnerabilities of the cyber-security programme.

Each of these professional disciplines has a different focus and related functions, however, they also share a number of important overlapping and common goal objectives and work together for the common good. It is considered an essential business practice that both disciplines receive equal consideration in the private and public sector, from business and corporate entities, to the national security apparatus.

When both professional disciplines are interactively implemented on a proactive basis, the financial impact of a technical compromise or discovery of an undocumented

**Members of Serbia's secret service remove listening devices hidden in the walls above a minister's office**

vulnerability can be managed, minimised or mitigated, reducing liability. When a formal technical security programme is not given equal consideration, the cyber-security programme is often weakened or compromised as a direct result.

Cyber security is considered to be a 24/7 function and those responsible for the cyber-security programme would never consider turning on the corporate firewall for perhaps only an eight-hour period a few times a year. Unfortunately, this is how the TSCM programme is often treated by the vast majority of organisations.

The Probability of Detection (POD) is shockingly low when the technical security programme is not implemented at the proper professional service level consistent with the perceived or ultimately determined threat level.

## CONSIDERING ALL ASPECTS

A well-rounded technical security programme looks at the facility, uniquely from all sides and establishes a security posture baseline, across physical security vulnerabilities, human factors, counter-intelligence, counter-espionage, counter-terrorism, sabotage and many other areas of vulnerability, including the cyber-security programme. The importance of a formal externally implemented and managed technical security review on a monthly or quarterly inspection basis is considered an essential business practice and must be administered in conjunction with the application of a managed Remote Spectrum Surveillance and Monitoring (RSSM) component (a modern version of in-place monitoring), to provide a competent due diligence approach – this is what a formal TSCM inspection programme is all about.

During the past decade wireless threat technology has continued to advance in both sophistication and commercial availability. Much of this threat technology has ventured well beyond the capability of general-purpose detection equipment commonly marketed for TSCM applications, or administered by persons who are not trained in the technical aspects of modern threat technology.

Consider that virtually everyone in modern society now has a substantial grounding in using quite advanced technology in general at the consumer level, and a troublesome picture begins to emerge. Add to the mix a limitless number of consumer devices that are easily considered dual-purpose technology, many of which can be utilised for the intended purpose as designed or for purposes that they were not intended to be used for, either as is, or with simple modifications.

The Cold-War era is dead from a threat technology perspective and we are now faced with complex technology at the consumer and commercial level that rivals the sophisticated offensive tools of law enforcement, government and military of only a decade ago.

Modern threat technology has created a demand for advanced detection resources that are firmly based on versatile Software Defined Radio (SDR) technology and more importantly, a modern TSCM approach methodology.

Professional technical operators are faced with advanced surveillance technology that are frequency, power and modulation agile, making the identification of such assets all but impossible with obsolete equipment resources, ineffective techniques or an inadequate approach methodology.

Extremely sophisticated low-energy emitters are not only difficult to detect on their own merits, but when SDR anti-detection, anti-identification methods are used, you have a smart device that makes localisation extremely challenging and exponentially complex when compared with Cold War-era technology, on which the vast majority of general purpose TSCM spectrum analysers are based.

Within a defined modern moving target threat model, the professional technical operator, 'is the spectrum analyser' and becomes an extension of the hardware placing the technical operator back in control of the analytical process.

There is very little difference in today's modern threat environment as to the type of threat technology, the rationale for its use or the end result of a successful compromise within the private or public sector as there was in the past. State-sponsored espionage, competitive intelligence gathering and facility-level penetration for the purpose of social engineering attacks, access to computer resources, confidential and classified information theft, sabotage of critical data, disabling and/or circumventing network or physical security protocols, occur every day in virtually every protected environment.

## WE ARE NOW FACED WITH COMPLEX TECHNOLOGY AT THE CONSUMER AND COMMERCIAL LEVEL

Perhaps the most troublesome aspect of TSCM accountability in a modern moving target threat model is the lack of understanding relating to Probability of Detection (POD) when reactive rather than proactive technical security programmes are implemented. The end-user expectation is that POD is 100 percent for any given inspection request, or at a minimum the expectation is that POD is extremely high.

Unfortunately, very few technical operators are willing to openly challenge the end-user's unrealistic expectations or talk about the POD reality with a perspective or established end-user client. This is always an excellent teaching moment and a brilliant opportunity to demonstrate the importance and need for more than a single annual inspection with the end user. Let's consider POD by the numbers and compare this with the end-user's expectations and explain that there are approximately 8,760 hours in a year, and if the organisation contracts an annual TSCM inspection of perhaps the executive office space, say 5 percent of the total office space compared with the total facility square footage. The inspection is likely to be conducted overnight or on the weekend, when the facility is not operating in a normal capacity; computers, office equipment, processes, *etc.* are off-line and the electronic sweep team is given, approximately eight hours to complete the entire inspection from beginning to end.

How we look at POD can be subjective, but let's take an honest look at the variables by the numbers and then add in other limiting factors. First and foremost, the POD is calculated as 8,760 x 8-hours (percent) (annually) = 0.08 percent POD. If, for example, the inspection programme provided 100 hours of time

on target, we would see a 1 percent POD annually. We establish this as 100-hours annually at 8.3 hours monthly, or 25 hours quarterly from a time-on-target perspective. We need to compensate for the actual frequency of inspections as the greater the frequency of inspections – just like increasing the hours – improves the time-on-target, yielding (at least in theory) an improved Probability of Detection by the numbers. If an eight-hour annual inspection yields a POD of only 0.08 percent and is considered the good news part of the story, POD on its own only means that the threat was detectable during the time-on-target window.

## WIRELESS THREAT TECHNOLOGY HAS RAPIDLY ADVANCED IN SOPHISTICATION

It does not mean that the equipment resources utilised were actually capable of detecting the Signal of Interest (SOI), or that the operator has the experience or knowledge to observe any potential threat or is able to perceive the signal event as potentially hostile; assuming the signal is not dismissed as an ambient spectrum event.

The hostile emitter may well be a burst transmitter or include a store and forward component that is not scheduled to burst during the limited time-on-target. So, the POD by the numbers must be negatively enhanced to represent a number of practical considerations and is now worse than the good news story at 0.08 percent. All of this is simply a reality check in determining the best approach to maximise time-on-target for any given threat level. When technical operators, manufacturers of test and measurement or TSCM equipment claim 100 percent POD for their respective hardware and software-based products, remember that POD by the numbers must be an integral part of a formalised reality check to look at the Probability of Detection from a mission critical perspective and used to implement a technical security programme that meets the intended objectives.

When the client initiates reactive rather than proactive TSCM inspections of the ambient RF environment, there is little confidence that any given threat technology present and operating will be detected in a single inspection without a historical baseline being previously established, and if such a signal is detected, there is no guarantee that the threat will be properly identified by the operator within a snap-shot (point in time) inspection.

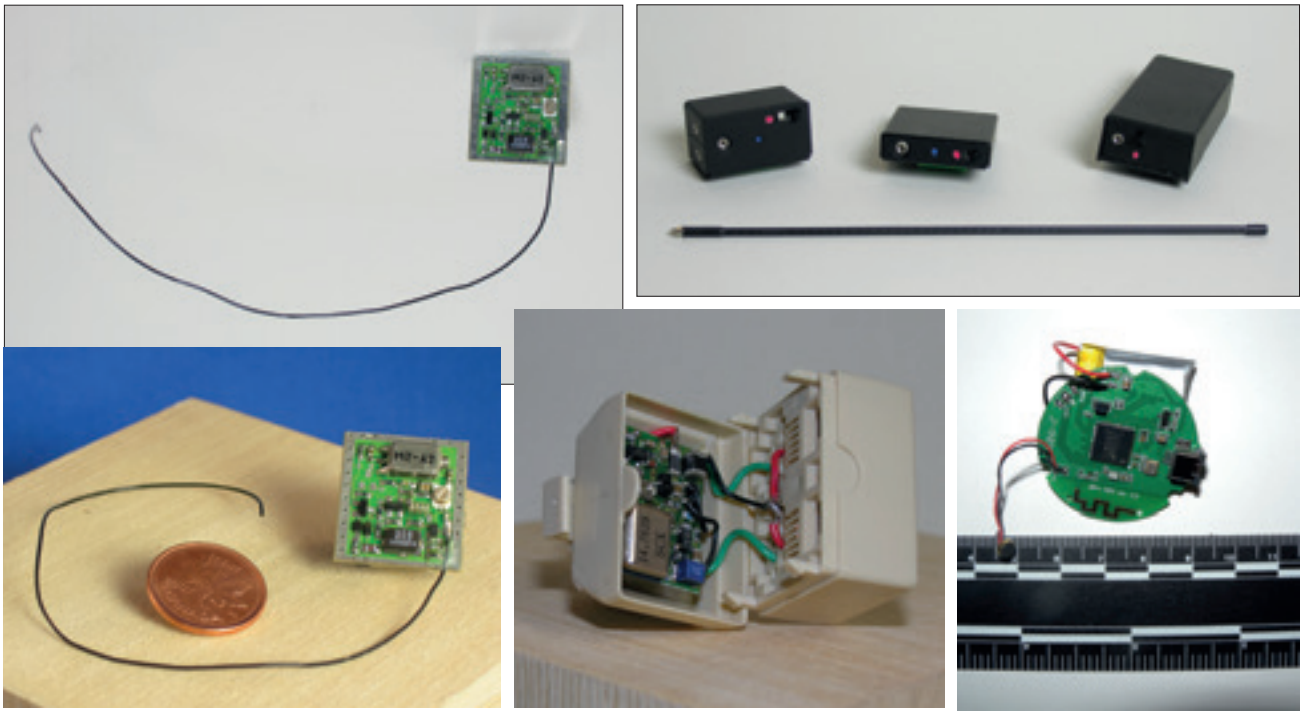
### AN ABSOLUTE MUST

Remote Spectrum Surveillance and Monitoring (RSSM), when combined with the advanced aspects of TSCM focused geo-location heat mapping, RF propagation modelling, RF visualisation and multiple receiver (operation and hand-off), has become an absolute must in a modern moving target threat model and part of a modern threat detection methodology that significantly enhances the Probability of Intercept (POI) and Probability of Detection.

These modern TSCM methodologies are well entrenched in government and military circles, and are available to commercial operators to provide the operator with enough information to have a fighting chance of identifying any given detected signal or unknown energy as a potentially hostile threat signature ●

**So how do we advance the Probability of Detection and improve Probability of Intercept exponentially through the application of the RSSM methodology? See part two of this feature next month when we will explore this in more detail.**

**Paul D Turner TSS TSI** is the President/ CEO of Professional Development TSCM Group Inc. and is a certified Technical Security Specialist (TSS) and Technical Security Instructor (TSI) with 40 years' experience in providing advanced certification training, delivery of TSCM services worldwide, developer of the Kestrel TSCM Professional Software and manages the Canadian Technical Security Conference (CTSC) under the operational umbrella of the TSB 2000 (Technical) Standard.



**A selection of UHF crystal-controlled audio intercept transmitters (top row), a UHF audio transmitter with M2 mic, crystal control telephone audio intercept and a miniature bluetooth audio transmitter (bottom row, from left)**

Picture credit: Professional Development TSCM Group Inc.

HS SECURITY
INTELLIGENT PROTECTION

hssecurity.solutions

TOGETHER WE STRIVE TO KEEP PEOPLE AND PROPERTY PROTECTED AROUND THE WORLD

Meet us at Intersec - Hall S2, Stand C34

Temporary Security

Building Hardening

High Security Access Control

Perimeter Protection

ATG ACCESS
BARKERS Fencing
bristorm
HARDSTAFF BARRIERS
PARKING Facilities Limited
TECHNOCOVER

Picture credit: Genetec

# STUDENT SECURITY

**Dan Meyrick** *reports on the challenge of keeping students safe from enrolment to graduation*

From kindergarten to high school and all the way through university, we spend a considerable amount of our lives attending educational institutions. Apart from enabling learning, these vital places have a responsibility to keep their students safe. Unauthorised visitors, theft and increasing acts of violence and terror threats on campuses across the globe have brought school security firmly to the top of the agenda. Yet, the sheer size of many campus areas combined with thousands of students and personnel with varying levels of granted access have proven a real challenge for those attempting to keep educational institutions and their perimeters safe – while offering effective and seamless operations.

Students must be offered the highest degree of security without complicating their daily lives with unnecessary obstacles. But it is not enough to safeguard the classrooms to keep students safe. A comprehensive perimeter security infrastructure needs to be built around them, which not only keeps unwanted people out, but also ensures authorised visitors are granted access to the area in a timely manner, without them feeling unwelcome or unduly stressed by the process.

Educational institutions have a responsibility to keep their students safe

Educational institutions can have new students enrol, graduate, drop out and attend standalone lectures and events on a daily basis. In order to keep up and grant access on a rolling basis, campus administrators need the right technology to support this process. With the vast size of most campus perimeters, and the number of people needing access to varying areas, it is no longer feasible to expect this all to be done by an admin person behind a counter – at least not if you want this process to run like clockwork. A centralised credential management system streamlines access control operations and manages all cardholder requests from a single location. It can also issue and manage access credentials both to and within the campus area, which brings us to the next – and often overlooked – level of access control.

A campus area houses a wide range of facilities like classrooms, research labs, libraries, sports complexes, teachers' lounges, administrative facilities and sometimes even dormitories. Therefore, having an access control system merely designed to grant visitors entry to the premises is not enough when designing a comprehensive security infrastructure. A person – let's say a student – obviously needs access to the campus, but should by no means be able to access areas designated for teachers or even all classrooms. After a person has been identified and verified as a legitimate visitor, administrators need a system to easily and quickly tick the boxes of which areas they are allowed to access – not only for safety purposes, but for operational efficiency.

## UNIFIED SECURITY

Advanced access control is only the outer layer of a rounded security system, however. The next step is to secure the indoor areas, and protect students from a number of potential threats while they're in the building. And this is where a unified security system makes a real difference. Not only does it make access management much easier and quicker, but it also allows those in charge of safety to monitor the entire campus and its facilities without needing to hop from system to system. This increases situational awareness, which in turn allows for faster reaction times to incidents, significantly enhancing overall security. It also cuts security costs, as it helps reduce inefficiencies and administrative costs by allowing operators to monitor multiple sites, even the most remote campuses, from a single location – which has proven particularly valuable to multi-campus educational institutions.

Modern physical security solutions like video surveillance, access control, video analytics and even number plate recognition systems are all aimed at providing campuses the protection they need. However, the way they are managed will be crucial to how effective they'll end up being. When ran separately, these security systems can often cause more headaches than benefits to security officials, as keeping track of them all is highly labour intensive and inefficient. By unifying these security components into a single system, those in charge of securing the campus and its perimeters can rest assured all incidents will be available for them to assess and provide an appropriate response, enabling a more proactive approach to security measures and eliminating time wasted on running systems in siloes.

When an incident occurs, first responders must get the right information to act quickly and effectively. A unified security system can enable information sharing with emergency services when need be, enhancing preparedness by including established connections and communication pathways with relevant law enforcement and other authorities. Having the ability to provide responders with access to video surveillance feeds from the scene of the event can significantly help responders understand all the factors of an emerging incident or event, and thereby help security personnel resolve situations quickly or before they occur. This increased situational awareness can vastly improve campus security and can even save lives in time-sensitive emergency situations.

A modern security solution is designed not only to deliver a unified approach to security operations, but to make everyday life in campus environments run as smoothly as possible. Hosting more than 16,000 students and around 2,500 employees and academic staff, the University of Hull was desperate to upgrade its outdated system into one that could do both. With over 50,000 card holders, access control was at the heart of the upgrade, and it needed one that could be expanded on later with the hardware of its choosing, without being tied to one particular provider. Students, teachers, parents and service people move through education institutions every day – identifying and counting each of them is essential for security, but also for the campus flow. Today's security systems can establish and track access of all campus occupants, lock a facility down in case of an emergency, integrate smoke and intrusion alarms to better manage movement at the campus. By opting to invest in an open architecture unified access control security system, the University of Hull was able to achieve all its security goals while keeping costs low and enhancing the campus experience overall.

**WHEN PICKING A SYSTEM, A MAJOR FACTOR IS HOW WELL IT PLAYS WITH OTHER SECURITY SYSTEMS**

Unification means, in simple terms, that all physical security components are not only run from the same user component but are, essentially, the same system. When used in a campus setting, the solution can maximise usage of the security infrastructure in place and thereby rationalise the investment. It makes updates seamless and provides a comprehensive cyber security management platform – but also introduces a fresh set of challenges. Technological advances have allowed us to take security to a new level, but today's digital age has also brought to life a new threat: cyber criminals.

Cyber security is also an often-overlooked aspect in campus environments, especially when referring to connected security systems. We've witnessed a significant increase in hacking and cyber attacks in most industries, not least the educational sector. With more sophisticated methods than ever before, cyber criminals are able to use the physical security equipment as a potential entry point to the campus network. A poorly secured camera, unencrypted communications between a server and client application or out-of-date software can all easily be exploited by cyber criminals. Ransomware attacks are particularly costly, and have been known to target educational institutions in particular due to the sensitive data they hold. Most physical security solutions are a work in progress with new devices being added to expand the system or to replace outdated or broken

products. The process of adding new equipment – perhaps from a different manufacturer with different security standards – is another opportunity for a vulnerability. No access control provider will be able to perfect a product that has no vulnerabilities, but they should have solid protection in place as well as a process that quickly and completely addresses any vulnerability.

## FIRST RESPONDERS MUST GET THE RIGHT INFORMATION TO ACT QUICKLY AND EFFECTIVELY

Due to often tight budgets, educational institutions may be reluctant to transform their security systems. When selecting an appropriate solution, a deciding factor should be how well the new solution plays with other systems. Today, the access control industry is moving away from closed, proprietary systems where only specific hardware is compatible with the chosen software. Instead, we are increasingly moving towards open architecture, where the latest software can be installed to existing hardware, enabling upgrades to be made as needed – without having to sacrifice existing hardware investments. This infrastructure allows for flexibility in choosing systems and the ability to upgrade both software and hardware as needed with time, and according to budgetary restrictions. By supporting the ever-growing collection of open architecture access control modules, readers, controllers and electronic locks, an open-platform access control system futureproofs the investment.

Educational institutions are responsible for creating positive learning environments. Advances in technology have resulted in unified campus security solutions that can deliver comprehensive video surveillance, access control and related functions that not only maximise security, but also offer a multitude of additional benefits. Because administration and security are tasked with protecting students, staff and visitors – usually on a strict budget – it's imperative that campuses invest in a security system that supports this effort today, but is also adaptable for the security challenges of tomorrow ●

**Dan Meyrick** is Sales & Business Development Manager at Genetec. He has 20 years of experience in the physical security industry, focused predominately on open-architecture security software platforms, products and solutions.

**A unified system allows those in charge of safety to monitor the entire campus without needing to hop from system to system**

Picture credit: Genetec

**Kestrel TSCM ® Professional Software**

*RF Sweeps, Capture, Analysis, and Remote Spectrum Surveillance and Monitoring, have Never been this Easy!*

**Signal Intelligence Support System ™**

*Developed in Canada, Kestrel TSCM ® is well Positioned to Hunt in a Complex Signal Environment!*

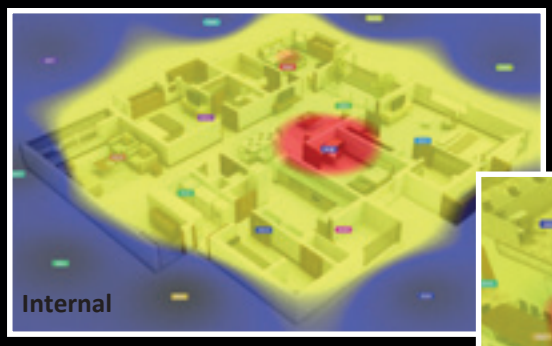
**Not Just Another TSCM Spectrum Analyzer! | Now You Can Have Tomorrows TSCM Software — Today!**

# Kestrel TSCM ® Professional Software

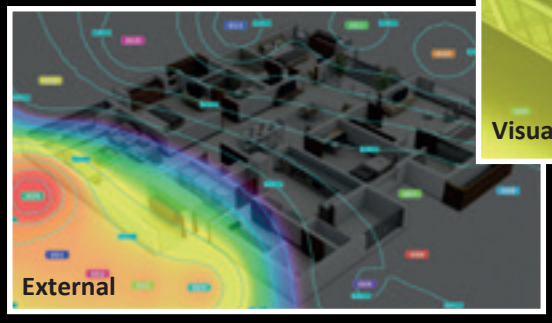
## *Visualizing RF Propagation is Now a Powerful New Reality When You Deploy our Tap Capture Plot (TCP) ™ RF Visualizer (RFV) ™ Display Mode*

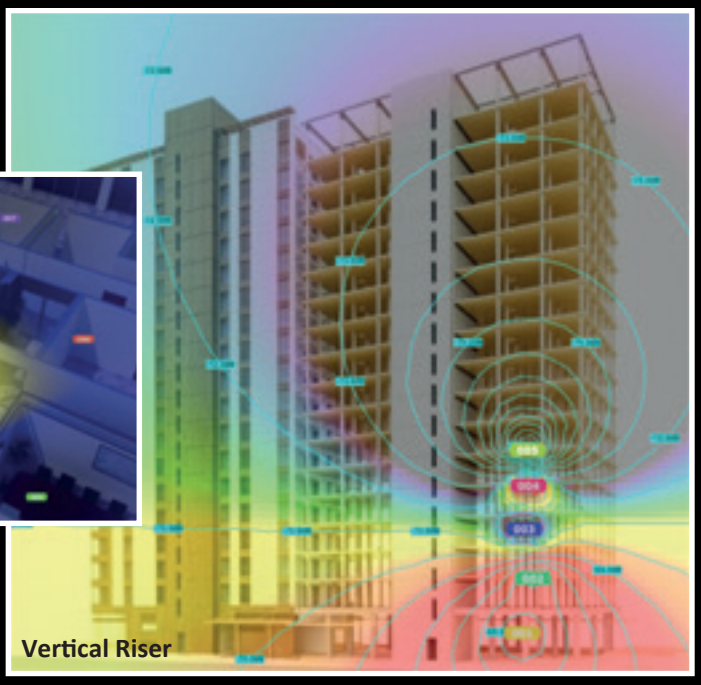
***Dimensional TSCM Spectrum Propagation Modelling that Develops Before Your Eyes!***

*The ability to capture a wide Location Differential Signal Analysis (LDSA) ™ Range of Interest (ROI) Plot and produce a powerful channelized operator interactive geo-location heat map with our new RF Visualizer (RFV) ™ technology, all on a single SDR radio is now possible with precision RF propagation contouring down to 1/10 of a dB.*








*100% Canadian Scientific Research and Engineering Development with Strictly Controlled Software Defined Radio (SDR) Source Code*

**Kestrel-net ™**

Actionable **RF** Intelligence

## Professional Development *TSCM* Group Inc.

*"Innovation is Simply the Beginning..."*

www.kestreltscm.com | www.pdtg.ca | www.ctsc-canada.com

*Telephone:* ***1-647-293-7384*** *Email:* ***pdturner@pdtg.ca*** *Contact:* ***Paul D Turner,*** *TSS TSI*

Picture credit: Patriot One

# ARTIFICIAL INTELLIGENCE

**Martin Cronin** *examines the growing importance of the role of technology in security, potentially detecting threats before they occur*

**Today's threat landscape is unpredictable and volatile, made even more so when set against the challenging backdrop of increased pressure on police forces, budget constraints, political instability and rising international threat levels. It cannot be denied that police and intelligence services are doing their utmost to protect society against the ongoing threat of attacks. But it may not be enough on its own. It demands a security response that is proactive, adaptable and dynamic. New technologies, such as artificial intelligence (AI), can dramatically improve the effectiveness of today's security systems.**

Many current security measures that are relied on only offer retrospective intelligence and do little to prevent attacks ahead of time. The London Underground, for example, is monitored by surveillance cameras that prove invaluable when it comes to identifying individuals in the aftermath of

**Using sensors to scan individuals for weapons allows security personnel to address a threat before the weapon is even drawn**

attacks, as was the case with the London tube bombings of 2005. These terrorists were later seen on CCTV entering the station before the bombing.

There is a fundamental lack of systems in place that can detect a weapon or other active threat ahead of time. Instead, police are called to the scene after an attack has happened and are then reliant on the accounts of eyewitnesses or CCTV to identify and catch the assailant.

In order to better protect citizens, physical security measures need to become more proactive to the detection of threats before a tragic incident occurs. Technology is the key to achieving this. These new technologies can be used in conjunction with existing security systems to create stronger defences.

In many cases, reactive systems simply can't prevent loss of life. This is where innovations in physical security technologies come into play. By integrating existing CCTV systems, with AI-driven object-recognition software, detection of visible threats, such as guns or knives, can be realised before an attack happens and can help to minimise the horrific impact by alerting security and law enforcement in real-time of the location and nature of the incident. These new video capabilities can help fill the gaps that may be present in existing video management systems (VMS), so that on-the-ground security can be engaged sooner, to ultimately save lives.

Terrorists, particularly trained groups, are increasingly exploiting gaps in technology to plan and execute complex attacks, making it difficult for law enforcement to detect, intercept and stop. Furthermore, the increasing trend of individual assailants is becoming more challenging for security services to detect and prevent. In order to keep up with these challenges and protect ourselves most effectively, we must harness the latest advances in technology to ensure our defences can face up to the ongoing threats against us.

As referenced above with object recognition software for VMS systems, other recent advances are being driven by AI. Today, AI is leading the development of smart sensors that can not only detect visible threats, but also identify concealed weapons before attackers have the opportunity to use them. This breakthrough covert threat detection technology means the burden on law enforcement agencies can be lessened. Security personnel are better able to operate more efficiently by responding to a potential attack before it happens.

A particular benefit of using data-driven algorithms to identify threat objects, like rifles, handguns, knives and bombs, removes human bias in identifying suspicious individuals, helping law enforcement to feel more confident in their unbiased decision making. AI-enabled technologies can be completely objective in a way that is innately difficult for people. The benefits of this should come as a welcome relief for today's law enforcement who are constantly under scrutiny for profiling potential suspects.

The capabilities of today's physical security technologies are astonishing. Computer vision technology has existed for over a decade. Now, with the power of real-time AI software, integrated with current VMS systems, threat objects held in an assailant's hand can be identified for immediate response at schools, houses of worship, transportation hubs and event venues. This same technology can also learn the normal behaviour of a crowd in specific settings, so when unusual behaviour occurs, security can be alerted to pay extra close attention.

The AI approach to learning visible objects and human behavioural patterns can be applied to discovering those hidden threat objects, too. Using microwave radar and magnetic sensors to scan individuals and bags for threat objects and mass casualty weapons will not only protect individual identity, but also allow for security personnel to proactively address a potential threat before the weapon is even drawn or used.

There are also sensor technologies that can detect trace chemicals, like gunpowder, explosives and chemical agents, to parts per billion by 'sniffing' the air at a safe stand-off range; again, helping security track and stop terrorists before they act.

## DESPITE THE POTENTIAL OF NEW TECHNOLOGIES, THE ROLE OF PEOPLE MUST NOT BE DISREGARDED

All these technologies can be covertly deployed, integrated into a complete threat-detection platform within a security command and control operations centre, monitored by trained professionals. Combining multiple sensors into a single platform can provide an all-encompassing, proactive security approach, for a wide range of venues, such as schools, office buildings, event venues and transport systems. The result is a comprehensive, non-obstructive approach to safeguarding the general public from harm.

With the advent of so much technological innovation, we must also exert a certain level of caution. Despite ongoing global debate on the topic, there remains very little regulation about the use of AI in security. One thing is certain; it must be deployed in the right place, at the right time with the right objectives. People do not want to live in a fortress. They do not want to be protected by omni-present, overbearing security systems that infringe on their privacy.

Equally as important, the public recognises that it is important to be protected in its daily lives, and looks to local, regional and national governments to provide that support. New technologies can offer valuable and effective enhancements to public safety, but the right balance must be struck to ensure that we don't sleepwalk into a mass surveillance society.

Decision makers have to find a way to strike a balance between safety and protection of civil liberties and a layered, covert, multi-sensor approach to threat detection offers a rational solution. By deploying sensor technologies that detect weapons and active threats first, before individual identification, the public concern about living in a 'Big-Brother' society is mitigated. People don't have to surrender their privacy to ensure their safety.

As these new AI-driven technologies become more mainstream, some may question whether this new technology will have a negative impact on

security jobs. As Price Waterhouse Cooper estimates that 30 percent of jobs will be at potential risk of automation by the mid-2030s, it's a perfectly natural question to ask. However, like many industries, the solution is not mass redundancy and layoffs, but the evolution of new skills. Training to help current security staff utilise and work alongside these new AI-driven technologies, which can provide real-time information on the presence of a potential threat. It will be essential to maintain a well-trained workforce to successfully implement these systems and respond accordingly when alerts are triggered. Security staff should receive continuous training on policies and procedure, as well as guidance on how to identify behavioural indicators that may be apparent prior to attacks.

## IT'S IMPORTANT TO HARNESS TECHNOLOGY TO ENSURE OUR DEFENCES CAN FACE UP TO THREATS

Despite the enormous potential of technologies that are beginning to transform the security industry, the role of people must not be disregarded. Technology can provide information and will alert security officers of a threat more efficiently, but it cannot negotiate with or physically stop an attacker. These technologies cannot reason with a disturbed gunman who is about to open fire on a school. These sensors cannot comfort the distraught, frightened parents of a young child who is lost in the chaotic aftermath of an attack. This is where the human element comes in. However advanced security systems become, the world will always need human engagement for action, as well as compassion and empathy, in moments of extreme crisis.

We need people, we need these new technology platforms, and we need policies and procedures working together to create safer public and private spaces. Technology on its own can only go so far. As a standalone solution, it is not the silver bullet to solving the UK's security problems.

In order to be most effective, technology must be embedded into national security policies and become an integral pillar of security training programmes. Decision makers need to have a comprehensive understanding of how to best implement and integrate the technology for it to be successful and effective. Collaboration and integration are key to creating a safer country. The emergence of smart and innovative solutions will arm today's security professionals with the tools they need to enhance and modernise security systems to defend against today's omnipresent threat ●

**Martin Cronin,** CEO & President, Patriot One is an expert in counter-terrorism, conflict resolution, and government/corporate interface. His career includes over 20 years' experience of international diplomacy with the British Government.


**Technologies can be integrated into a complete threat-detection platform within a security control operations centre**

Picture credit: Patriot One

Milipol
QATAR 2020

# 13th International Event for Homeland Security & Civil Defence


Organized by

STATE OF QATAR
MINISTRY OF INTERIOR

وزارة الداخلية
Ministry of Interior

**26 - 28 October 2020**

Doha Exhibition & Convention Centre (DECC)

#MilipolQatar

www.milipolqatar.com

# Looking for the world's

## ORION 2.4 HX

The new ORION 2.4 HX is for detecting hidden electronic devices, regardless of whether they are radiating, hardwired or even turned off. It will locate them in walls, floors, ceilings, fixtures, furniture or containers. Transmitting at 2.4GHz the ORION is perfect for detecting small electronics such as SIM cards and mobile phones.

## VPC 2.0

The new VPC 2.0 Video Pole Camera extends the view of surroundings above drop ceilings, behind immovable objects, around corners or other difficult to reach areas, even dark situations. It records video and still images and can extend up to 12ft 6in (depending on model).

## OSCOR Blue

The OSCOR BLUE is specifically designed as a Counter Measures Receiver detecting illicit eavesdropping signals. With its ease of use coupled to an incredibly fast scan speed, it is the first choice of governments and professional sweep teams around the world.

**Hidden state of the art bugging devices are very hard to find – you will need a combination of some of the world's best TSCM equipment.**

**For more than twenty five years I.P.S. (Overseas) Ltd have been the first choice of governments and professional sweep teams around the globe to provide the world's leading equipment, manufactured by Research Electronics International (REI), together with the associated training.**

# leading TSCM equipment?

TALAN™

Voice-over Internet Protocol (VoIP) phone systems present a new form of security risk to communications. With new enhancements built into the TALAN software interface, users can now test internet protocol (IP) packet traffic on VoIP phones and systems.

ANDRE™

The ANDRE is a handheld broadband receiver that detects known, unknown, illegal, disruptive or interfering transmissions. It quickly mitigates threats such as eavesdropping and electronic bugging. Technical specialists will appreciate the portability and responsiveness.

# ...You've just found it.

INTERNATIONAL PROCUREMENT SERVICES (OVERSEAS) LTD
118 PICCADILLY, LONDON W1J 7NW E: sales@intpro.com
T: +44 (0)20 7258 3771 F: +44 (0)20 7569 6767 www.intpro.com

IPS

# DISASTER RECOVERY

**Peter Groucutt** *explains why it's so important and why organisations need to keep it font of mind*

**As a society we are increasingly dependent on technology to keep businesses running smoothly. While tech has brought many benefits, our reliance on it can mean that any type of incident – whether a premeditated criminal cyber attack, human error, technical glitch or natural disaster – can result in data loss and downtime.**

To make sure organisations are as resilient as possible they must have a Business Continuity Plan (BCP) plan in place. Within that plan, comprehensive IT Disaster Recovery (DR) capabilities – to ensure minimal disruption in the wake of an incident – are essential.

Over the last few years there have been hundreds of examples of cyber attacks having a severe impact in both the public and private sector. In 2017, the NHS was seriously affected by what Mikko Hypponen, chief research officer at F-Secure, called: "the biggest ransomware outbreak in history", when WannaCry malware infected hospitals and doctors' surgeries across England and Scotland. This forced staff to turn away patients and even cancel appointments.

The NHS is not the only public service to fall victim to this type of attack, as a recent Freedom of Information request revealed that local authorities and councils in the UK were hit by more than 263-million cyber attacks in the first six months of 2019.

The private sector has suffered in much the same way, with high-profile attacks on global aluminium company, Norsk Hydro in June and shipping services company Pitney Bowes in October. These examples illustrate just how important it is for appropriate BC plans to be in place so operations can continue in the event of a crisis.

For large enterprises with multiple offices in different locations it also highlights why it is essential for seamless and coherent communication between internal IT, security and BC teams. By working together closely and sharing information it is easier to assess the potential risk and therefore coordinate a unified response.

Although cyber attacks are dominating the headlines, more seemingly mundane technical faults can wreak just as much havoc, as the financial services sector has experienced recently. In April last year, TSB suffered a systems migration failure after attempting to move customer records onto its own platform. The company was forced to pay approximately £330-million in fines and suffered reputation damage that forced CEO Paul Pester to resign.

In June 2018, a hardware problem at Visa resulted in around 5.2-million failed payments, affecting customers in the UK, Europe and abroad. Just five months later, a glitch in Barclays' online banking systems meant customers were locked out of their accounts.

These incidents prompted the government to debate the issue as part of its recent Treasury Committee. The committee published a report on the 'unacceptable' number of IT failures across the financial services sector. The report recommends – and rightly so – that in our tech-dependent society, more must to be done to improve operational resilience and accountability. This shows that BC is rising up the agenda, which can only be a good thing.

IT resilience is especially significant in the current era of digital transformation, as organisations increasingly migrate from outdated legacy technology to take advantage of the agility offered by cloud service providers. The cloud services market is an oligopoly, dominated by Amazon Web Services (AWS), Microsoft Azure and Google Cloud Platform (GCP).

These platforms have revolutionised the way we deploy and manage IT, but relying on a small number of cloud providers centralises risk. You may think you are more resilient now because you use several different cloud services, theoretically reducing the chance of an outage affecting all systems at the same time. However, a large proportion of internet services and business operations could become inactive if one of the main cloud providers suffers an outage.

## TIGHT COLLABORATION BETWEEN IT OPERATIONS, CYBER AND BC TEAMS IS ABSOLUTELY VITAL

For example, an AWS outage in February 2017 affected services including Spotify, Dropbox and Trello. Another failure in 2018 impacted Atlassian, Twilio and Slack. AWS services went down again in October 2019, this time due to a malicious DDoS attack.

To make IT resilient and improve the ability to recover from incidents it needs to be clear where exactly DR sits within the wider Business Continuity Plan (BCP). The two terms are often conflated and we prefer to use the term *IT Disaster Recovery* to make the distinction clearer.

Business Continuity is the catch-all term for all aspects of resilience, including people, premises and suppliers. IT Disaster Recovery specifically refers to how an organisation recovers IT systems if it suffers an outage. It can feel like the IT DR is a large slice of the BC pie, and as

**Although cyber attacks dominate the headlines, more mundane technical faults can wreak just as much havoc**

a result, continuity planning sometimes takes a technology-first approach, but that is a mistake. The problem with technology-centric continuity is that it can produce rapidly recovered servers, but a team unable to use them. It can also encourage over spending on unnecessary capabilities. The best approach is to start with the real BC work first and set recovery objectives before thinking about backup, recovery and replication technologies.

The creation of the individual plans themselves (Business Continuity Plan, IT Disaster Recovery Plan) come relatively late in the 'enacting' stage. Once the team and scope has been decided, the biggest part of BC planning is assessing the risks (Risk Register) and the impact they could have (Business Impact Analysis).

Your Risk Register should be changing to reflect a higher likelihood of particular risks such as cyber attacks. It should also be updated to reflect the greater impact of other risks such as the outage of a major cloud provider.

One of the problems many businesses face is creating a joined-up approach to BC. As the cyber threat has grown, so too have cyber teams. In larger organisations, responding to a major incident will require BC, IT operations and cyber security staff working closely together to quickly diagnose, respond and rectify the problem.

Cyber-related incidents demand the unique skillsets of each team because they can be more difficult to recover from than traditional incidents. If there is a flood or fire in a data centre, the IT team can simply fail-over to a secondary data centre or cloud-hosted DR. The flood or fire might still be happening, but it will not affect the DR site and if staff are capable of working remotely, there may only be an IT outage of hours or even minutes.

With cyber incidents, failing over to a secondary site may not help as it carries the problem over. For example, when recovering from a ransomware attack, the IT and security teams may need to carry out several recoveries to retrieve a clean version of the data before the infection.

The cyber team is responsible for detecting attacks and eradicating any infection before operations can be safely restored by IT. Tight collaboration between IT Operations, cyber and BC teams is vital for an accurate understanding of risk and the potential impact of attacks.

The first step in reducing cloud risk is to get a handle on where cloud services are hosted. For Infrastructure as a Service (IaaS), it should be clear which data centres (or regions and zones) the data is hosted from. For Software as a Service (SaaS), investigation may be required to locate where these services are hosted from. They may run from their own data centres, or they too may be hosted in the public cloud with AWS, Azure or GCP.

The next step is to find out the level of resilience built into those respective cloud services. With IaaS, the tools are available to build resilience into every layer of infrastructure, from the data centres themselves, through storage, server and networking. But it is the customers' responsibility. In the early days of cloud computing, many

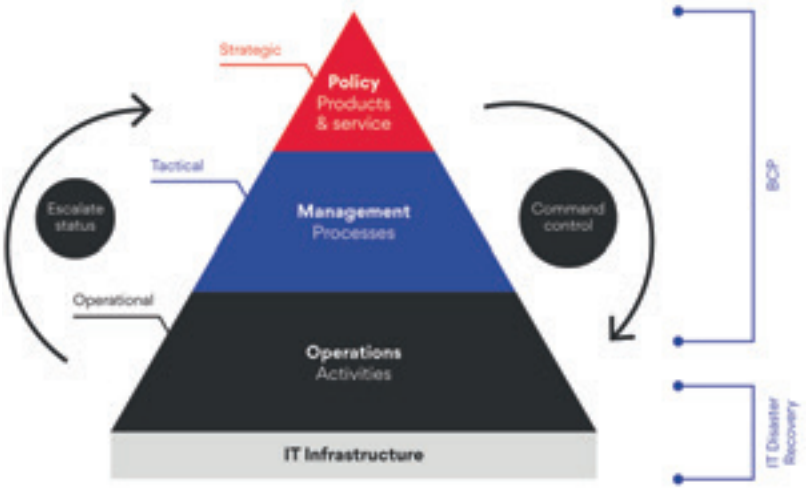
| | STAGE | ACTIVITY | |
|---|---|---|---|
| 1 | Policy | Identify scope of urgent business functions and create the Management Business Continuity Statement | |
| 2 | Select teams and determine responsibility | Selection and setting culture, attitude, behaviours | |
| 3a | Determine impact on the business | Business Impact Analysis (BIA) – people, premises, resources, suppliers | Planning |
| 3b | Risk/threat identification | Risk register and matrix | |
| 4 | Identify urgent functions (IT & other services) | Service catalogues & technology-service dependency mapping | |
| 5a | Implement mitigation strategies | Put the capability in place | Enacting |
| 5b | Agree activation plans | Writing the runbooks & communication plans | |
| 6a | Exercise & Test | Agree test scenarios, documentation and KPIs | Testing and Maintenance |
| 6b | Ongoing changes and maintenance | Plan exercises, maintain and keep BC & IT DR plans up to date | |

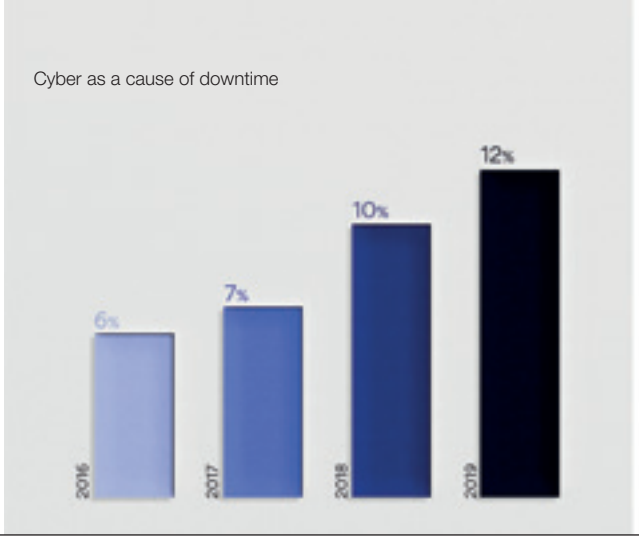
**Peter Groucutt,** Databarracks' Managing Director, founded the business in 2003 after working in risk management roles in the banking sector. Peter's main focus is to combine technology with a passion for customer service.

incorrectly assumed that DR was the sole responsibility of the cloud provider, but it actually works on a shared responsibility model. The cloud provider is accountable for some parts of the technology stack while the customer is for others.

Our final recommendation is to diversify risk by using more than one cloud provider. At a minimum, this means keeping a back-up copy of data outside the production cloud. It is also possible to build resilience across multiple cloud providers.

Containers and Infrastructure as Code (IaC) both allow you to build and destroy environments quickly and repeatedly across multiple clouds. The long-term benefits extend beyond resilience, by taking advantage of pricing and performance differences between cloud providers that enables greater freedom of movement ●





# Locating Hidden Electronics Requires Products with Special Skills

Well disguised surveillance devices - RF transmitters, hidden cameras, microphones, telephone taps, all require equipment with unique investigative skills in order to be detected and found. REI spectrum analysers, non-linear junction detectors, telephone and line analysers and physical search products are depended on by TSCM professionals for those skills.

Whether new to the business or a seasoned pro, the REI Training Center offers *the* best commercially available TSCM training. Contact IPS for more information or visit reiusa.net

**International Procurement Services (Overseas) Ltd,**
118 Piccadilly, London, W1J 7NW, Email: sales@intpro.co.uk
Phone: +44 (0)207 258 3771 Fax: +44 (0)207 569 6767

# SMART ACCESS SOLUTIONS

## LOCKEN *Launches first contactless access control solution for explosive environments*

**Access control within explosive environments must meet the requirements of health & safety regulator ATEX. The dangers of 'explosive atmospheres' have led to strict regulations, requiring the use of fully licensed equipment in high-risk areas.**

LOCKEN's electronic access control incorporates a new contactless technology patented by its parent company, ISEO, which allows it to meet the new standards for operating within explosive environments. The main areas concerned are the energy sector, notably gas and hydrocarbons, chemicals, timber and household waste. However, agri-food is also an industry requiring ATEX certified access - mainly because of the accumulated wheat dust in the silos.

An explosive atmosphere is formed mainly due to the presence of flammable gases or dust. The explosion can be triggered by a spark, mechanical or electrical, or by a local source, for example due to the friction of two pieces of metal.

An electric power-free opening for ATEX certified access control!

In the case of electronic access control, the danger comes less from the mechanical part of the key than from its electronic component. If the transmission of information between the key and cylinder is carried out through an electric contact, an electric arc can form and a spark will be enough to ignite the surrounding explosive materials.

By incorporating an inductive technology key, LOCKEN is the first to bring a complete access control solution designed for explosive environments.

The intrinsic characteristics of the key (label ib of «intrinsic safety»), and its maximum operating temperature (T4), allow it to be used safely in the presence of a gas as highly explosive as ethylene, as well as slightly less dangerous gases such as propane (II B).

### SAFETY AND PERFORMANCE

This revolutionary technology has two other major advantages:

**1.** It allows an almost instantaneous opening, since the exchange of information between the key and cylinder takes place in less than 80 milliseconds.

**2.** As communication between the key and cylinder is non-contact, it is not disturbed by potential damage, such as oxidation, wear or dust present in the cylinder. It offers unrivalled robustness.

Thanks to its Bluetooth module, the key can communicate with the user's smartphone via the MyLocken app, enabling control and management of access on a case-by-case basis and in real time, an additional guarantee of security, which is usually reserved for online access control.

Led by LOCKEN smart Access management software, the solution provides enhanced access management and perfect traceability.

**This state-of-the-art technology has enabled LOCKEN to obtain ATEX certification for its access control solution.**

**Approved to ATEX II 2 G Ex ib IIB T4, the solution is suitable for gas delivery and regulation stations, specific hydrocarbon processing and distribution infrastructures and chemical factory enclosures. It is also suitable for areas where an explosive mixture of gas, vapour or mist may 'occasionally' occur in 'normal operation'.**

**The new key transmits the information to the cylinder through an electromagnetic induction coil located at the heart of the key.**

LOCKEN
SMART ACCESS SOLUTIONS

# SMART ACCESS SOLUTIONS

## **LOCKEN** *Launches first contactless access control solution for explosive environments*

**Access control within explosive environments must meet the requirements of health & safety regulator ATEX. The dangers of 'explosive atmospheres' have led to strict regulations, requiring the use of fully licensed equipment in high-risk areas.**

LOCKEN's electronic access control incorporates a new contactless technology patented by its parent company, ISEO, which allows it to meet the new standards for operating within explosive environments. The main areas concerned are the energy sector, notably gas and hydrocarbons, chemicals, timber and household waste. However, agri-food is also an industry requiring ATEX certified access - mainly because of the accumulated wheat dust in the silos.

An explosive atmosphere is formed mainly due to the presence of flammable gases or dust. The explosion can be triggered by a spark, mechanical or electrical, or by a local source, for example due to the friction of two pieces of metal.

An electric power-free opening for ATEX certified access control!

In the case of electronic access control, the danger comes less from the mechanical part of the key than from its electronic component. If the transmission of information between the key and cylinder is carried out through an electric contact, an electric arc can form and a spark will be enough to ignite the surrounding explosive materials.

By incorporating an inductive technology key, LOCKEN is the first to bring a complete access control solution designed for explosive environments.

The intrinsic characteristics of the key (label ib of «intrinsic safety»), and its maximum operating temperature (T4), allow it to be used safely in the presence of a gas as highly explosive as ethylene, as well as slightly less dangerous gases such as propane (II B).

### SAFETY AND PERFORMANCE

This revolutionary technology has two other major advantages:

**1.** It allows an almost instantaneous opening, since the exchange of information between the key and cylinder takes place in less than 80 milliseconds.

**2.** As communication between the key and cylinder is non-contact, it is not disturbed by potential damage, such as oxidation, wear or dust present in the cylinder. It offers unrivalled robustness.

Thanks to its Bluetooth module, the key can communicate with the user's smartphone via the MyLocken app, enabling control and management of access on a case-by-case basis and in real time, an additional guarantee of security, which is usually reserved for online access control.

Led by LOCKEN smart Access management software, the solution provides enhanced access management and perfect traceability.

**The new key transmits the information to the cylinder through an electromagnetic induction coil located at the heart of the key.**

**This state-of-the-art technology has enabled LOCKEN to obtain ATEX certification for its access control solution.**

**Approved to ATEX II 2 G Ex ib IIB T4, the solution is suitable for gas delivery and regulation stations, specific hydrocarbon processing and distribution infrastructures and chemical factory enclosures. It is also suitable for areas where an explosive mixture of gas, vapour or mist may 'occasionally' occur in 'normal operation'.**

LOCKEN
SMART ACCESS SOLUTIONS

SCANNA

# High Performance, DR and CR X-ray systems from a name you can trust.. with x-ray generators you know and trust.

## SCANSILC EOD - DR X-RAY

- Lightweight intelligent x-ray panels in 10 x 12” and 14 x 17” formats.
- Impact and drop tested to over 1m. Dirt and water resistant to IP67
- No extra interface box or splitter required - unlike competitive systems
- Solid state, no moving parts and load resistant to 170 kgs

## SCANX SCOUT - CR X-RAY

A must in every bomb truck!

- Multi- size x-ray electronic free x-ray plates
- Wire free and flexible for tight access applications.
- Ground level imaging - no dead zone
- X-ray Multiple image plates in a single exposure. XTK software stitches your x-ray images together.
- Digital processor scans plates up to 130 cm long

All operating with the new Golden XR range of pulsed x-ray generators.

- Now with new higher performance Li-Ion battery power, custom pulses and custom delays!
- Simple to setup - no need to set kv or exposure time!
- Low radiation due to short nano-second bursts of x-ray!

XR150

XR200

XRS-3

Demonstrating in your area soon.
Email demo@scanna-msc.com

www.scanna-msc.com
info@scanna-msc.com

# MOBILE POLICE TECHNOLOGY

**Simon Hall** *investigates how the police use technology to bridge the generational divide on the frontline*

**After nearly a decade of austerity, UK police forces will soon be enjoying an influx of 20,000 new officers over the next three years. But how will they cope with so many new recruits in such a short time? Albeit highly welcome, and many would say long overdue, any recruitment drive after such a long freeze would be a challenge for any organisation to adapt to. But policing isn't just any organisation. Crime affects everyone, whether directly or indirectly, so how quickly and effectively these officers can integrate into their respective forces is important. The technology used by officers makes a big difference to this.**

These new officers will not be entering the same environment that their counterparts were enjoying prior to austerity. For example, many police stations have been sold off or mothballed, so where will these new officers operate from? Are there even enough lockers for them to store their kit?

## FRONTLINE POLICE IT MUST BE AS INTUITIVE TO USE AS ANY OTHER SMARTPHONE APP

Once deployed, 20,000 new officers will account for over 17 percent of the UK's total policing frontline. This is a huge number of individuals to skill up and integrate into an existing workforce in a relatively short space of time. But there is another aspect to this that must not be overlooked; such an influx of an entirely new generation of officers will change the face of UK policing significantly. Are our police forces geared up to make the most of this new generation? Can they avoid a 'Clash of the Generations'? It is fair to assume the majority of these new recruits will be of the post millennial or "Gen Z" generation (defined as those born after the mid-nineties), whereas the vast majority of their colleagues (and most certainly all of their superior officers) will be from the preceding generations – Generations X and Y specifically. This presents a unique challenge. The technological ambition and enthusiasm of these Gen Z recruits may clash with their more seasoned colleagues. Many serving officers will tell you they are tired of years of interference and changes to their working day; either from failed technology initiatives (such as the poorly executed BlackBerry rollout early in the millennium) to the inevitable changes to procedures and protocols that are typical of any large organisation over the years. Will these new recruits bring a refreshing wave of enthusiasm to do things differently or will their ideas clash with the way things have always been done?

Those hailing from each generation will have their own preferred way of working and skillsets, largely borne from the environment in which they grew up. Could this be a cause of tension? The incoming Gen Z (or post millennials) are regarded as being very tech-savvy, internet-native and highly politically active. They grew up with tablets and smartphones, and rarely use a 'traditional' PC. They have never known a world without the internet, they have had smartphones since they were teenagers, and they are used to having access to the world's data wherever they are. It only follows that they will expect data and technology to be embedded into every process of the workplace, and the devices they use to be intuitive to use and available to everyone. Clearly, they are in for a shock when they enter most workplaces, let alone many police forces!

For the millennials who came before Gen Z, technology is still a part of their DNA, but they came of age during the rise of the internet. They are still digitally savvy, but can remember a time before tablets and social media, so their digital expectations are a little more tempered. Before millennials we have Generation X, the children of the Baby Boomers. They have lived through a technical revolution like no other. In the workplace they have had to adapt to every change you can imagine – from paper-based working to the introduction of the mainframe, personal computers, the internet, and now smartphones and tablets. They have been asked to change how they work more often than any generation before them. They have seen technological changes for better and for worse, and I doubt they enjoy having to learn a new way of working every five to 10 years just to continue doing their job.

Every new employee entering an organisation must go through the inevitable induction process. While the breadth and depth of an induction varies from employer to employer, the process is broadly the same; you are shown your place of work, educated on the rules and processes that govern your employment and are handed the tools you need to do your job. In our highly digital economy, most employee tools are technological in nature – phone, computer, tablet *etc*. Most Police officers have these technological tools too, alongside their more traditional items like their uniform, handcuffs, truncheon, notebook, radio, *etc*. Policing, like everything else, is not immune to the digital transformation trend sweeping across every other organisation in the world. As a result, an officer's digital tools are becoming a far


Picture credit: Getty

more integral part of their kit than they ever used to be. Given the growing role of technology in UK policing, it has a very clear role to play in tackling the generational divide caused by the influx of Gen Z into the workforce. But with so many generations rubbing shoulders together, you cannot expect everyone to be on the same level of technical experience or, indeed, enthusiasm. There is no point in deploying new technology, no matter how good it is, if only those under the age of 25 can use it. Unfortunately, new technology has a habit of creating barriers between the generations, not reducing them. The opposite must be true if we want these 20,000 new officers to make the biggest impact they can. New technology must be adopted by everyone, irrespective of their time in the force, if it is to have a positive impact.

**There should be no distinction between working on a PC in the station or a mobile device on the street**

The only way for new technology to help the frontline is for it to be as intuitive as possible. Police IT needs to model the ease of use and intuitiveness of smartphones, where anyone over the age of three can use them proficiently within minutes. Did you ever read a manual to use Facebook for example? One of the most overlooked features of smartphones is their ability to cross the generations. If someone who has never even used a PC can FaceTime their grandchildren with ease, you know you've hit the cross-generational jackpot.

Frontline police IT must be as intuitive as any other smartphone app. This not only reduces training significantly, but for the first time, every generation of officer will be working to the same level of proficiency. This eradicates the digital divide that has existed in policing ever since the first typewriter landed on the inspector's desk. Senior officers will no longer be burdened with yet another training course just to keep up with the new recruits, and will never have to face

the embarrassment of asking a junior officer for help again. The best way to deploy an intuitive IT service that officers of every generation can use is to design a common working platform that can be deployed on any mobile and non-mobile device. There should be no distinction between working on the PC in the station and working on a mobile device in the car or on the street. Officers should have access to the same data and processes, using a consistent user interface/user experience (UI/UX), wherever they are, on whichever device they are using. So, for example, an officer could search the PNC on a mobile device in the same way as at the station, or file a police report from a mobile device as they would from their desktop.

## AN OFFICER'S DIGITAL TOOLS ARE MORE OF AN INTEGRAL PART OF THEIR KIT THAN THEY USED TO BE

Forces should be working towards this goal now, so that they have a clear pathway to deliver cross-generational technology that delivers more effective and efficient policing.

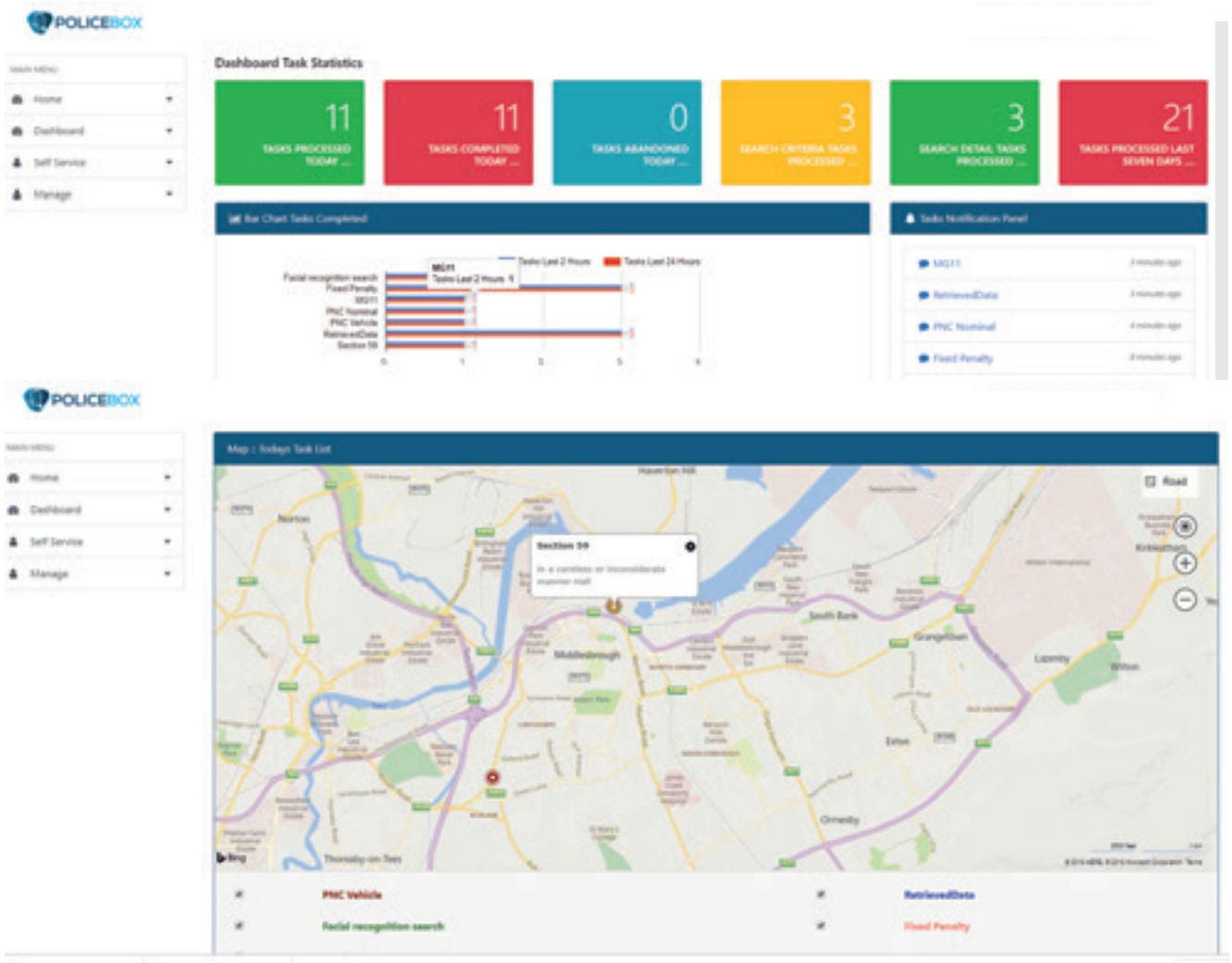
What's more, since officers are the ones who will use these IT tools, they should be more actively involved in their development and eventual implementation. This will not only ensure that they are 'bought in' to the technology (so are more likely to use it), but that the solution meets their needs. We need officers across the generational divide to be able to complete their tasks in the same way, using the same technology, thereby delivering better, more intelligence-led policing across each force. The days of notepads, personal phone usage and paper forms is coming to an end.

In addition to bridging the digital divide among officers, better IT processes will ensure the influx of new officers can hit the ground running from day one. We know that simply adding more officers will not bring policing back to the levels identified before austerity because the environment simply isn't the same. Every other community-facing organisation that interfaces with the police – from social services to healthcare – is smaller too. But by handing our new officers a mobile working device with a common IT platform that covers everything they need to do in a day, they at least will be able to work effectively with their colleagues from day one, shift one.

While we cannot get back the many thousands of years of collective policing experience that were lost when good officers left during austerity, we can at least make it easier for the new recruits to work efficiently with their colleagues. With that we can ensure that every one of the 20,000 new officers can make an enormous difference to the policing of our communities – even if they don't necessarily have anywhere to hang their hats just yet ●

**Simon Hall** is the CEO and co-founder of PoliceBox and Coeus Software. He is responsible for the company's overall strategy and direction. Under Simon's leadership, PoliceBox has successfully evolved into a leading digital mobile workforce specialist, transforming workplaces with its intelligent and award-winning solutions.

**Better IT processes will ensure the new officers can hit the ground running from day one**




Picture credit: Coeus Software

TSS International official distributor for:

RODGARD

HUTCHINSON

SEMA WORLD

B&G electronics

Téléflow

TSS HEAVY DUTY WHEELS

MOVIT

ProtecTank TSS

# YOUR MOBILITY SPECIALIST FOR ARMOURED VEHICLES

- *Flat tyres?...* ***Keep on driving***
- *Punctured fuel tank?...* ***No leakage***
- *Enclosed in armour?...* ***Barrier free communication***
- *Heavy armouring?...* ***Extra braking power***

TSS

**TSS INTERNATIONAL BV** ZUIDEINDE 30-34, 2991 LK BARENDRECHT. THE NETHERLANDS.
PHONE: +31 (0)180-618 922 FAX: +31 (0)180-611 326 EMAIL: SALES@TSSH.COM

WWW.TSSH.COM

Picture credit: Getty

# MISSION POSSIBLE

**Brigham Bechtel** *reports on the importance of optimising delivery of mission critical data*

**Growing volumes of data and improvements in artificial intelligence (AI) and machine learning (ML) are disrupting the traditional ideas of the Observe-Orient-Decide-Act (OODA) loop and now require new means to deliver the information effectively. It is widely acknowledged in national security circles that big data is key to harnessing mission critical insights necessary for commanders and policymakers to prevail over adversaries. However, the OODA loop begins to look more reflexive than deliberative as time is compressed. Those with the ability to ingest the volumes of available data and orient faster could decide and act before an adversary. In the case of AI, it means human input into algorithms must precede potential scenarios well in advance. Therefore, new means to manage data must be employed in order to accelerate information used in the loop for vital decisions and actions.**

Our understanding of the OODA loop is challenged from the outset by increases in the volume of data available. As more devices are able to connect to networks – vehicles, sensors, and equipment – more information is available to

**The advantage that optimising data management provides can make the difference between success and failure**

ingest and orient to inform key decisions. A vital advantage can be gained if one can make more accurate decisions, give precise instructions and launch calculated tactics faster than an opponent. The speed that's made possible with AI moves the emphasis away from the human calculus during such events.

Defence and intelligence organisations must find new ways to obtain real-time understanding for the "orient" portion of the loop from these huge volumes of data. In our systems now, algorithms represent the orient portion of the loop, which is where OODA's author, Colonel John Boyd, placed the emphasis on understanding the data ingested. 'Orient' takes account of culture, experience, and even genetic dispositions and biases. Here, analysis of potential outcomes moves to the 'decide' phase of the loop. For humans these factors represent years of training and education and some of it even becomes subconscious. For AI responses it requires humans training algorithms through neural networks well in advance of data input and then testing of the algorithm. The developers working with military professionals, or who are themselves operators, must train neural networks as they train themselves – making use of lessons learned, best practices, ethics and values – before deploying an algorithm to solve even the most mundane tasks.

## MANAGING THE DATA

The challenge now is to handle volumes of data at critical speeds to facilitate successful use of AI. Speed, volume, and variety of data – structured and unstructured – differentiate the AI process from previous methods of human analysis and response. In the information age, the broad spectrum of data sources – transmitted from distances, foreign language, different formats – arriving in massive volumes at near real-time speeds makes it harder to ingest and access all of the available reporting for use in decision processes. The data handling and availability must all occur at speed to respond defensively, or to intrude on an opponent's OODA loop. In conflict the adversary is likely to have AI-enabled systems too, which complicates efforts to disrupt their plans or defend your own.

Additional processing speed will not be enough for overloaded data systems to ensure the smooth ingestion and integrity of the data with context in order to support AI algorithms and thus complete the loop in time. Furthermore, the demands on AI are increasing for shorter response times in conflict scenarios as weapon systems and cyber weapons become faster. The problem is further complicated when an adversary's weapons are automated and enabled by similar algorithms. Faster responses are required of even seemingly mundane processes associated with things like supply chain management for loss replacement will be key in modern conflict.

In future, it may be that a general or admiral will not be part of a tactical response executed by an AI algorithm which could impact the success of his operation. Instead, a developer with some knowledge of military objectives, but an understanding of the mechanics of a system he writes for might have as great an impact on the outcome of an engagement as the officer who commands the forces employed. For example, a developer writing code for weapon systems to cope with a drone swarm effort to overwhelm a nation's air defences would write algorithms based on data from sensors, information about potential attacking drones, about the defensive weapons and about potential follow-on attacks. His calculations for algorithms would need to be vetted against the value of the drones, the targets, the follow-on forces, the defences in reserve and of course environments. All this would need to be accounted for in an algorithm well before any forces are employed by either side in the battle.

While OODA still has its relevant applications and remains widely taught in military circles, it may not be the most appropriate concept to apply when it comes to managing large and isolated data sets as the age of big data matures. The steps associated with OODA primarily described processes of how commanders or individual warriors won battles with the limited data available in the past. Is there still adequate time for a human to observe and orient or disrupt the adversary's OODA loop when the volume of data available grows exponentially? What

## BIG DATA IS KEY TO HARNESSING CRITICAL INSIGHTS FOR PREVAILING OVER ADVERSARIES

happens when all the available data is not accessible to our human-machine teams?

What is evident is that a much more agile and streamlined way to process data is required for speed of mission. Legacy relational models and large data storage solutions are not fit for the ingestion, curation, and provision of massive amounts of data at a speed that would enable AI to respond effectively. Things that hamper those systems include: relational models require ETL processes that inhibit speed and governance; relational systems have difficulty scaling quickly to meet demands; they cannot handle unstructured data; and legacy systems require too much human review for quality control and rapid integration.

Crucial data can often be difficult to access which challenges both the observe-and-orient processes of the OODA loop. The information can be trapped in silos and exist in unstructured formats or file types, anything from geographical coordinates to a written letter. There is also no guarantee a report is accurate. Even when data is accessed and ingested, its integration with other important data sources is what leads to the most vital insights for the frontline use and can be the most difficult step. The combining of information from multiple sources enables examination, corroboration or verification of details that power AI algorithms. File formats, sizes and volumes of data cannot be allowed to prevent the integration so vital for the orient process.

The advantage that optimising data management provides can be the difference between success and failure. It is imperative that military organisations use the best data management tools to ingest reports in various formats and derive useful insights. Tools that offer an 'as is' alternative to inefficient ETL processes can help data integration so users do not have to curate and sort it manually before use. This integrated data resulting from proper tools enables humans, algorithms and machine learning to power autonomous decision making.

Once data is ingested, a range of technologies are now available to make use of it faster. Machine Learning can quickly detect patterns in data sets and artificial intelligence can take action automatically. Intelligent devices that are connected to networks are now

operating on a two-way stream of information and can continuously make autonomous adjustments.

Consider an Unmanned Aerial Vehicle (UAV) tasked with surveillance on an enemy base, which can then fly autonomously based on pre-set flight plans combined with intercepted and triangulated transmissions. If the UAV receives data indicating a priority target is moving from a flight box, an algorithm can tell the drone to move to observe the target without waiting for pilot input or after a lengthy deliberative process. Instead of a slower command time going through the four steps of OODA, the machine can exploit the information because of the algorithm, speeding up responses to dynamic situations. This would not prevent command intervention to re-direct the drone, but it could save response time critical to maintaining coverage.

Another example could be sensors located on the aircraft that monitor its operating state and feed its maintenance algorithms. An automatic feedback loop could enable efficient ordering of replacement parts, which can feed a headquarters-based system to monitor supply chains. Crew chiefs can plan their workload based on AI, leading to higher readiness and availability of the airframe for more missions. Other benefits would be for the manufacturers knowing what is needed for a robust supply chain, more predictable supply requirements, and more efficient use of personnel and materials.

The importance of accessibility and quality data to support the processing capabilities of artificial intelligence in completing analysis is often overlooked. Professionals know artificial intelligence is only as powerful as the data it uses; it must be both accurate and complete because bad data leads to bad results. Many national security organisations pursue the promise of AI, but have difficulty solving the problems of data ingestion, governance and transmission with security and speed.

Artificial intelligence offers many advantages, but amidst the buzz, it is easy to neglect the importance of protecting the data. The connection of security to accuracy is ensuring the integrity of the information. Reports might be inaccurate from a source, but they cannot be inaccurate due to mishandling in the data management system. Secure means more than protection from theft; data must be incorruptible and safe from bad actors. Once data has been collected it must be stored with the capabilities for granular levels of control including who can access what data, when, and for how long. Analysts and data scientists tasked with assuring data quality must have systems that compliment their work.

Good data governance assures provenance and lineage while providing transparency into the movement of data and who edited it over time. Well-governed data also ensures the right people are accessing the right data as it moves and is transformed.

Having the correct technology in place to enable swift, secure processing of mission critical data can enable new technologies and replace some human OODA loop processes. This has the potential to provide commanders with a full intelligence picture in real time and enable AI when every second counts ●

**Brigham Bechtel** joined MarkLogic as a 31-year veteran of the United States intelligence community having served for more than 26 years in the Central Intelligence Agency with experience in leading operations, and in analysis. Mr. Bechtel has tours in field leadership with experience coordinating the work of the intelligence community, law enforcement and military partners.

**In future, a tactical response may be executed by an AI algorithm rather than a general**

Picture credit: Getty

# TSCM & TACTICAL SECURITY EQUIPMENT & TRAINING

Delivered by the Global leader in Cellular Threat Detection

## The threat of Eavesdropping & Cyber Eavesdropping has never been greater

As the world's largest TSCM company, QCC is the clear choice for TSCM equipment procurement & training - Why?

We don't just make and sell TSCM equipment, we use it & understand it.

## QCC solutions include:

TSCM & Tactical IMSI Capture solutions - **SearchLight Plus** & the new **BlackLight**.

TSCM equipment from all leading manufacturers, to cover all threats with training.

## QCC's other proven and ISO certified services include:

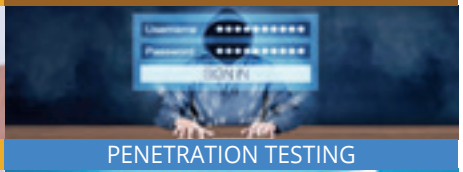

TSCM


CYBER TSCM


CYBER FORENSICS


MOBILE PHONE FORENSICS


SECURE COMMUNICATIONS


PENETRATION TESTING


PROTECTIVE SECURITY


EQUIPMENT

TRAINING

**LONDON OFFICE**
T: +44 207 205 2100
E: contact@qccglobal.com
W: www.qccglobal.com

**SINGAPORE OFFICE**
T: +65 3163 7100
E: contact@qccglobal.com
W: www.qccglobal.com

THE BRITISH ASSESSMENT BUREAU ISO9001 Certification No. 193274
THE BRITISH ASSESSMENT BUREAU ISO27001 Certification No. 197110
THE BRITISH ASSESSMENT BUREAU ISO14001 Certification No. 197108
THE BRITISH ASSESSMENT BUREAU OHSAS18001 Certification No. 197109

QCC – Keeping your business, ***your*** business !

# A WOMAN'S PLACE

**Dr. Joana Cook** *explores the changing role of women in US counter terrorism since the events of 911*

**In September we remembered the 18th anniversary of 9/11. 18 years. We now have a generation coming into universities that do not remember the day of 9/11 because they weren't even born. Yet, the events of 11 September continue to prove to be some of the most formative for the 21st-century global landscape.**

We have now seen two wars in Afghanistan and Iraq, old threats like al-Qaeda continue to expand their footprint around the world and new threats like ISIS becoming the most wealthy and successful terrorist group in history. We have seen the US train, equip and partner with countries around the world to manage terrorism better in their own neighbourhoods. We have seen both successful initiatives, but also dark practices that have deeply tarnished the reputation of the US, and which have even been counter productive to its own aims.

The financial and human cost of this ongoing campaign has also been exponential – it's estimated the US has now spent as much as $6.4-trillion in response to the events of 9/11. Beyond the nearly 7,000 US servicemen and women, and many others including from countries like Canada and the UK who have lost their lives fighting in these wars, nearly 500,000

Picture credit: Getty

persons have also died from war-related violence in countries like Iraq, Pakistan and Afghanistan. These figures are truly hard to fathom.

This campaign against terrorism has fundamentally impacted how my generation, and that coming up now, understands concepts like security, terrorism and what we should do to keep our countries safe. It continues to shape these perceptions today. Yet, despite all these global efforts, resources and losses, terrorism has not declined, but expanded, diversified and terror groups like al-Qaeda and ISIS have only seen their membership, physical presence and influence increase. It raises questions about what strategy has been employed over these years to confront and prevent terrorism and where (and why) it was fallen short.

What these 18 years have also highlighted is just what significant gaps in knowledge, policy and practice there has been in relation to women. There has been an absolute shortfall in tracing and understanding women's roles in this period at every step, and there have been significant consequences from this thus far. This is the focus of my new book, *A Woman's Place: US Counterterrorism Since 9/11*, which attempts one small step towards remedying this gap and building off a growing body of research looking at different aspects of women in relation to US counter terrorism.

**Women's roles in security continue to evolve in unique ways for a number of diverse reasons**

## IMPACT OF 9/11

*A Woman's Place* looks at 9/11 and the subsequent international counter terrorism response by the US through a neglected lens and considers how women have been agents, partners and targets of counter terrorism since. 9/11 has impacted the roles of women in relation to counter terrorism and terrorism in largely unrecognised and undocumented ways, with profound effects on the efficacy, impact and support of these efforts to prevent, address and recover from terrorism around the world. It is the aim of the book to examine how, where and why women have become visible in the discourses and practices relating to counter terrorism through the lens of international US efforts from 2001 to early 2019. It focuses on US and local women in Afghanistan, Iraq, Yemen and Syria, and does a number of things in relation to telling the story of women and counter terrorism over these 18 years.

First, it looks holistically at full-spectrum counter terrorism efforts. By full-spectrum I mean the 'soft' or 'indirect' approaches often associated with preventative measures – countering violent extremism and preventing persons from becoming associated with terrorist actors in the first place. It moves through how we respond to terrorism in foreign policy terms through country partnerships, aid and support; to 'hard' or 'direct' efforts such as offensive military, special forces operations, policing or intelligence efforts in place to stop a specific threat. Finally, it considers recovery efforts, including reconstructing and stabilising societies impacted by conflict to prevent their return as terrorist safe havens, which is often how they have been framed.

Second, it traces how women's roles in counter terrorism have evolved under President's Bush, Obama and Trump. What have their strategies and approaches to countering terrorism been? How have these evolved? How were women's roles understood within these, both within counter terror efforts, but also in the groups the US was targeting? There are both notable similarities and distinctions that become visible across these three administrations.

Third, it looks at how this understanding of women has trickled down into the Department of Defense, Department of State and USAID. Each of these institutions are examined in a separate chapter. One of the key arguments I make is that it is particularly at this institutional level we have to look at more closely as this is where women's roles become visible in policy and practice on the ground and evolve in unique ways for diverse reasons. Each of these chapters draws on interviews with key actors, case studies and examples, and highlights new policies, practices or units set up since 9/11.

In the DoD, these include American programmes such as Team Lioness, Female Engagement Teams, and Cultural Support Teams, programmes that developed as the US faced new challenges in the field such as growing insurgencies and had to overcome lack of capability to engage 'half the population' in their counter-insurgent efforts. It also looks at new programmes established that engaged and impacted local women, such as the development and training of all-female counter terrorism or special forces units established in Yemen and Afghanistan with women from those countries, or programmes like the Daughters of Iraq. It also touches on dubious cases of women, such as Lynndie England who became

**TERROR GROUPS HAVE INCREASED THE TACTIC OF SEXUAL AND GENDER BASED VIOLENCE**

infamous for the abuse of prisoners in Abu Ghraib.

In the Department of State these programmes focused on women's rights and empowerment through the lens of democracy promotion, where democratic societies were understood as most resilient against terrorist appeals. It discusses programmes like the Middle East Partnership Initiative, and shifts in State to start thinking more about engagement with women in civil society, or the promotion of women in policing, in relation to countering terrorist groups. It also considers women in the development of the first National Action Plan on Women, Peace and Security which began emphasising women in all aspects of foreign policy; steps to elevate diplomacy and development in full spectrum counter-terrorism efforts; and increased partnership with the DoD in inter-agency counter terrorism-relevant initiatives.

In USAID, this considers how an agency once largely outside of security becomes increasingly integral to this fight against terrorism, as the links between development and security become more emphasised, particularly in preventative CVE efforts challenging what are referred to as 'the underlying drivers' of terrorism. It also looks at the increasing interaction of civil and military actors during reconstruction and stabilisation work for example, or efforts to support female victims of terrorism, particularly as terror groups have increased the tactic

of sexual and gender-based violence (SGBV) in their activities as seen by groups like Boko Haram against local women or ISIS in relation to Yazidi women.

Fourth, it examines simultaneously how the roles of women in al-Qaeda and ISIS have evolved, and how this has been understood and responded to in counter terror efforts. We cannot develop effective counter terror efforts unless we fully understand these groups that engage terrorism, and their members, tactics, strategies and objectives. The book highlights how particularly as these groups have attempted state-building projects, how they engage women in their own efforts increasingly mirrors that of the state, and in fact at times draws off similar language discussing for example women's rights, or even debates about roles for women in their organisation.

Finally, it has created a framework or map that researchers, policymakers and practitioners can use to inform their own work. It outlines the primary *roles* women were often discussed in, in relation to counter terrorism. It highlights the key factors related to language, operational and institution-specific aspects around counter terrorism that drove evolutions to this. It also displays how the engagement of women was often justified by key actors. This is meant to help clarify thinking in terms of how or why women may be emphasised in certain ways, in certain periods, and for certain ends, and to question the implications of this when considering women more in our own policies and practices.

I hope to demonstrate how looking at the Global War on Terror through the lens of women actually helps clarify key shortfalls in this comprehensive approach to counter terrorism thus far, and drives us to envision a more effective, holistic approach to this concern going forward. This book is for academics and researchers, policy makers and practitioners. I believe we can do better going forward in how we understand women in all aspects of international security, and what we can do to consider, engage and support women at every step.

It is important that we learn from the mistakes of the past to strengthen responses to new and continued challenges we face today – whether it be the rise of far-right extremism, the continued concerns from jihadist groups or the thousands of women and minors affiliated with ISIS we continue to refuse to repatriate and deal with, there are many substantial concerns ahead. I fundamentally believe that better understanding, engaging and supporting women at every step in relation to responding to these groups, ideologies and actions will be crucial going forward, and I hope to convince you of the same ●

**Dr. Joana Cook** is a Senior Research Fellow at the International Centre for the Study of Radicalisation, Department of War Studies, King's College London and Adjunct Lecturer at Johns Hopkins University. *A Woman's Place: US Counterterrorism Since 9/11* is available via Oxford University Press in the US or on Amazon globally.

Picture credit: Getty

FRONTIER PITTS
PROTECTING YOUR WORLD

IWA 14 IMPACT TESTED

# HVM
# TERRA BI-FOLD GATE

- **WORLD FIRST**
- Double Leaf HVM Bi-fold Speed Gate
- Successfully impact tested to stop a Hostile Vehicle travelling at 30mph
- Aperture up to 8m
- Security Rated
- Minimal Penetration
- Made to order

FOR A SITE VISIT OR QUOTATION
CONTACT TECHNICAL SALES ON
+441293422800 OR sales@frontierpitts.com

# INCIDENT BRIEF

## Europe

**6 November, Amsterdam – Netherlands**
Part of Schipol Airport was closed off after a pilot on a plane set off a hijack alarm by accident, causing a major security alert.

**11 November, London – United Kingdom**
A Kentish Town street was cordoned off and a bomb disposal team was called to the scene to investigate a suspect device. Camden police subsequently issued a statement that no bomb had been found.

**25 November, Berlin – Germany**
Far-right terrorist group Combat 18 is believed to be behind a bomb threat emailed to Sehitlik Mosque, which claimed that plastic explosives had been planted on site.

**29 November, London – United Kingdom**
Two civilians were killed and three others injured in a mass stabbing by a convicted terrorist wearing a fake explosive belt who was shot dead by police. Islamic State claimed responsibility for the attack.

**29 November, The Hague – Netherlands**
Several people, including children, were wounded in a stabbing attack on a crowded shopping street in Grote Marktstraat in The Hague on Black Friday.

**29 November, Paris – France**
Gare Du Nord train station was evacuated after an alleged explosive device was found hidden inside an unattended bag. Police subsequently gave the all clear.

## Americas

**13 November, Virginia, Minnesota – United States**
The Saint Louis County Courthouse was evacuated after an anonymous bomb-threat phone call. After an extensive search, no explosive device was found.

**14 November, Santa Clarita, California – United States**
A 16-year-old Santa Clarita high-school student shot five of his classmates and then himself in a planned attack. Two of the victims died as a result of their injuries, as did the gunman.

**17 November, Fresno, California – United States**
Four people were killed at a backyard party after a shooter fired randomly into the crowd. Six others were injured.

**21 November, Washington, DC – United States**
A man was arrested after an unauthorised vehicle attempted to enter the White House complex. Roads around the White House were also closed as a precautionary measure.

**26 November, Washington, DC – United States**
Military aircraft were scrambled after a plane breached Washington, DC airspace. The situation led to a brief lockdown at the White House, Capitol and congressional offices.

**2 December, Seattle – United States**
The *Seattle Times* newspaper office was evacuated due to a bomb threat being received.

# Asia

### 2 November, Tell Abyad – Syria
A car bomb exploded in a market, killing 13 civilians and wounding more than 30 others. The PKK is suspected.

### 6 November, Yala Province – Thailand
The Patani United Liberation Organisation is suspected of being behind an attack on a security checkpoint, which left 15 dead and five injured.

### 10 November, Tell Abyad – Syria
The PKK is believed to be responsible for a car bomb detonation that killed eight people and wounded 26 others in the North-Eastern Syrian city.

### 11 November, Qamishli – Syria
Three car bomb detonations across the city left a total of six people dead and 21 others injured. The Islamic State of Iraq and the Levant claimed responsibility.

### 13 November, Kabul – Afghanistan
Targeting a security convoy in rush hour, a Taliban or Islamic State suicide bomber detonated his explosives, killing 12 others and wounding more than 20.

### 13 November, Medan – Indonesia
A suicide bomber detonated near police headquarters, injuring six people – four officers and two civilians. The attacker, who had connections with Islamic State affiliates, died in the explosion.

### 16 November, Al-Bab – Syria
The PKK is suspected of being responsible for car bomb detonations near a bus terminal, which resulted in the deaths of 19 people – with 50 others being injured in the multiple explosions.

### 23 November, Tell Abyad – Syria
At least 10 people were killed and 25 others injured in a car bomb explosion. The PKK is believed to be behind the attack.

### 26 November, Tell Halaf – Syria
A car bomb detonated in a village near the Syrian border, leaving 17 people dead and 20 others injured. The YPG and PKK are suspected of being responsible.

# Africa

### 1 November, Ménaka Region – Mali
Islamic State claimed responsibility for an attack on a military post in In-Delimane, near the Mali-Niger border, which killed 53 soldiers and a civilian, and left three others injured.

### 3 November, Maiduguri – Borno State
Six Boko Haram fighters were killed and an unspecified number wounded by Nigerian troops as they unsuccessfully attacked a military base to the North of the capital.

### 6 November, Fada N'gourma – Burkina Faso
Islamic State is suspected of being responsible for an attack on a mining company convoy, which left 37 people dead and 64 others injured.

### 18 November, Gao Region – Mali
A military convoy was ambushed in the Tabankort area of Gao Region: 43 soldiers were killed and 19 others were injured. Islamic State claimed responsibility. More than 17 terrorists were also killed in the ambush.

### 27 November, Yobe – Nigeria
The Nigerian army rescued 20 abductees, including a medical team, from Boko Haram after a battle in Yobe State. One terrorist was killed, the others withdrew and a rocket-propelled bomb was recovered.

### 27 November, Borno State – Nigeria
Nigerian Air Force fighter jets targeted and bombed a Boko Haram hideout near the Sambisa Forest Reserve, killing more than 30 jihadists.

### 27 November, Borno State – Nigeria
Three Boko Haram terrorists were killed by the Nigerian army during a clearance operation near the Sambisa Forest Reserve. The terrorists' ammunition was also recovered.

### 1 December, Hantoukoura – Burkina Faso
At least 14 people were killed and an unspecified number wounded after gunmen opened fire inside a church. At the time of writing, no terrorist group had claimed responsibility for the attack.

### 2 December, Lake Chad – Chad
Boko Haram is suspected of being responsible for the deaths of four Chadian soldiers in an attack on a recently established military outpost on Lake Chad. 13 jihadists were also killed.

# NEWS

## Europe

### UK to host 2024 Interpol general assembly

The UK will host the general assembly of the international police organisation, Interpol, in 2024 – the largest global gathering of senior law enforcement officials and heads of ministries. The general assembly is Interpol's highest governing body, comprising representatives from each of its member countries and responsible for major decisions affecting general policy and resources. Usually taking place over four days and attended by approximately 2,500 delegates, it also presents the opportunity to drive innovation and leadership in police cooperation, and tackle major crime trends and global security threats, including organised crime, terrorism and cyber crime. Home Secretary Priti Patel said that hosting the 2024 general assembly "highlights the UK's strong commitment to make the world a safer place" and demonstrates Great Britain's "vision as a global security leader, looking to invest in strong relationships with those who matter most to our security". Patel continued: "The UK is and will continue to be a global leader on security and justice. We are determined to build on that role by strengthening our international security relationships where it matters and enhancing our capabilities at a domestic, European and global level to protect the public. This includes investing in organisations like Interpol, that are best suited to tackling security threats we face."

### UK defence sector R&D spend reaches seven-year high

The latest data from the Office for National Statistics (ONS) shows that the UK defence sector has increased its annual spend on research and development (R&D) by 6.3 percent, taking it to a seven-year high. Defence businesses posted growth in R&D investment of £100-million, taking it to £1.7-billion, according to statistics. This is some way off the sector's peak of £2.4-billion in 2005, however, analysis by R&D tax relief specialist Catax shows. Crunching the ONS numbers, a total of 61 percent of UK defence R&D spending is funded by the Government. The amount remained static last year at £1-billion, but the amount sourced by UK businesses fell by 17.9 percent (£20-million) to £92-million. The amount that UK businesses across all sectors have invested in R&D continues to grow, however, rising £1.4-billion to £25-billion in 2018, an increase of 5.8 percent. The telecoms sector had the largest percentage increase in R&D spending, rising 25.4 percent to £947-million. "The defence industry is hugely important to the UK and it is encouraging to see strong year-on-year growth in R&D spending," said Mark Tighe, Catax chief executive. "However, it has still not returned to its pre-crisis peak, and this is what we need to see happening in the next few years if Britain is to continue to breathe life into the export success story that the UK defence industry has always been regarded as."

### UK National Cyber Deception lab unveiled

Cranfield University, Bedford, and the Defence Cyber School at the Defence Academy, Shrivenham, are working together to develop a national focal point for cyber deception – likely to be one of the most significant growth areas in cyber security over the coming years – and help the UK Ministry of Defence better defend its networks in cyber space. The National Cyber Deception Laboratory (NCDL), launched at the first National Cyber Deception Symposium in November, aims to bring together practitioners and researchers across Government, industry and academia to facilitate national security research and provide guidance. "Military networks need a full-spectrum military defence – existing civilian security approaches are simply not up to this task. Deception is all about creating errors in how our adversaries make sense of their world. It is about getting them to act in ways that suit our purposes, not theirs," said Darren Lawrence, director of the NCDL, senior lecturer in Behavioural Science and head of the Information Operations Group at Cranfield University. "Researching ways to shape attacker behaviour and deny them the freedom to operate within our networks will enable military cyber defence to move on to a more aggressive footing and deter future attacks," he added.

### £3-million Cyber-SHIP Lab for maritime security

A new research facility to address key cyber security challenges facing the shipping industry is being established at University of Plymouth. The £3-million Cyber-SHIP Lab, which is supported by funding from Research England, part of UK Research and Innovation, and industry, aims to bring together connected maritime systems currently found on a ship's bridge. Cyber security and information systems experts will then assess them for weaknesses and identify the technological changes needed to make them secure. The Cyber-SHIP Lab will feature cutting-edge tech – including radar equipment, a voyage data recorder and an automatic identification system – and will complement University of Plymouth's existing advanced maritime facilities, which include a state-of-the-art simulator for training professional seafarers. "Cyber attacks are a Tier 1 National UK threat," said professor Kevin Jones, executive dean for Science and Engineering, and principal investigator for the project. "Although the maritime sector is advancing technologically, it is not well protected against cyber or cyber physical attacks and accidents," he added. "Worth trillions, it has an unmatched reach across international waters, which exposes people and goods to a diverse range of factors, putting the shipping history at high risk. As such, this facility has never been more timely."

### Sophos and O2 collaboration good news for UK

O2 and IT security company Sophos have joined forces to offer Sophos products and services to the mobile operator's business customers in the UK. Under the new agreement between the two, O2 now offers small and medium-sized business customers Sophos' advanced security solutions for mobile devices, computers, servers and email, as well as its encryption software tools. O2 business customers that sign up to use Sophos via O2 will be granted access to the Sophos Central cloud-based security platform to configure and manage their services – making it quicker and easier for them to secure their organisation. All Sophos products bought through O2 are also complemented with a range of support services, including training and customer support. "As our customers become increasingly mobile and make greater use of cloud-based services, they have told us that a comprehensive security solution is key to keeping their business safe," said Maria Fernandez, director of SMB Sales, O2. "Sophos, with the O2 wraparound support, helps provide security our customers need, so they can focus on running their business."

# NEWS

## Americas

### KBR awarded $216-million DHA contract

Global aerospace and defence provider KBR has been awarded a $216 million contract to provide cyber security services for the US Defence Health Agency (DHA). KBR will assist the Naval Information Warfare Centre (NIMW) Atlantic with cyber security and risk management framework initiatives and provide support to the DHA Assessment and Authorisation Division. The DHA works closely with US Government agencies to deliver medical services to more than 9.4-million active duty personnel. Supplying a broad spectrum of IT services, KBR's work will include addressing independent validation and verification results, helping prepare an Enterprise Mission Assurance Support Service authorisation package and supporting the implementation of federal IT security regulations, directives and guidance.
KBR will support all Department of Defence Military Health System sites – which vary in size from 1,500 to over 60,000 servers and workstation assets – and assist with up to 430 programmes of record systems. The company will also provide these services at locations around the world. "KBR believes our military men and women deserve the best possible care," said president KBR Government Solutions US, Byron Bright. "We are proud to continue delivering our cyber security solutions to DHA as it ensures service members and their loved ones receive high-quality health services."

### Accenture unveils new American cyber ranges

Accenture has expanded its cyber security capabilities with the opening of three cyber ranges – two in the US; the third in Essen, Germany – to help industrial companies practice their response to cyber attacks across critical assets. The two American cyber ranges – located in Houston, Texas and Washington, DC – feature live-fire, multi-vendor capabilities. Housed within one of the company's innovation hubs, the Houston cyber range focuses on the oil and gas industry. The focus of the Washington range, in Accenture's Cyber Fusion Centre, is the utilities industry – from electric transmission to distribution. "We tailor security solutions to our clients' industries and help them build resilience across their entire value chains," said Jim Guinn II, who leads Accenture's cyber security business for the energy, utilities, chemicals and mining industries. "Our ICS cyber ranges are designed to help pressure test and improve the security posture of organisations so they can innovate safely and grow their businesses with confidence." The cyber ranges are controlled, interactive and hyper-realistic environments for cyber security training and software development used to assess network and other technical vulnerabilities of industrial control systems.

### JASK and Sumo Logic merge for "security intelligence for all"

Sumo Logic, leader in continuous intelligence, has acquired JASK Labs, a provider of cloud-native autonomous security operations centre (ASOC) software. The acquisition brings together Sumo Logic's industry leading Continuous Intelligence Platform, including its pioneering cloud SIEM and security compliance solutions, with JASK's ASOC offering to deliver a leading cloud-native security intelligence solution built for contemporary digital businesses that leverage modern applications, architectures and multi-cloud infrastructures. "Security in the modern world is moving from a human-scale problem to a machine-scale problem," said Ramin Sayar, president and CEO of Sumo Logic. "Customers are looking for a new approach to help them overcome the pain and complexity around an increasingly perimeterless world. The JASK team are experts in helping customers navigate this new world. By aligning our efforts as a single team, we are able to democratise security intelligence for all." As part of Sumo Logic's Continuous Intelligence Platform, the company will expand its security intelligence portfolio with the launch of the Sumo Logic ASOC solution, as well as a Spec Ops offering for threat hunting, which is expected to be available by the end of the year.

### US cloud security spending to reach $1.93-billion by 2021

According to PreciseSecurity.com, cloud security spending in the United States is expected to reach $1.93-billion by 2021. Putting this figure in perspective, in 2016, the US region spent $675-million on cloud security solutions in total – meaning it will triple in the following years. In comparison with other regions, the US also represents the leading cloud security spending region in the World, followed by Asia Pacific with $638-million cloud security costs expected in 2021. With $573-million in expenses on cloud security solutions by 2021, Europe takes third place on this global list. In the same period, the Latin America region is estimated to spend $86-million. Analysis of the difference between the 2021 and 2016 data reveals apparent changes in the global list. Although the US kept the leading position, the other dominant regions switched their places: for example, three years ago, Europe was the second-largest region on this global list, with $171-million in costs of cloud security services. At the same time, Asia Pacific positioned in fourth place with $63-million expenses. Statistics show that Asia Pacific has become the fastest-growing region in cloud security spending globally.

### Wolf appointed acting US Homeland Security secretary

In mid-November, Chad Wolf was appointed acting Homeland Security secretary. He is the fifth person in the role under President Trump and succeeds Kevin McAleenan, who had been in the post since April 2019 and resigned in October. Wolf's acting deputy is Ken Cuccinelli, supporter of Trump's anti-immigration policies. Wolf, who has served in other Republican administrations, was previously the department's Acting Under Secretary. According to the US Department of Homeland Security (DHS), since his appointment, Wolf has overseen the completion of the recently released DHS Strategic Plan, which establishes the department's long-term strategic goals, and led initiatives to counter international and domestic terrorism, prevent terrorist travel, safeguard the US electoral process and protect American trade interests. On his first visit to the Southern border, Wolf asserted that the Trump administration will continue to encourage Mexico to do more to stop migrants from reaching the US border. "There continues to be a big push and a big need for them to continue the actions that they've taken, and to do more," Wolf said at El Paso's main Border Patrol station.

# NEWS

## Africa

### Senegalese President calls for peace in Africa

The President of Senegal, Macky Sall, has called for "all necessary measures" to be taken "to achieve peace and development in Africa". The remarks came at a two-day Sustainable Peace, Security and Development in Africa forum held in Aswan, Southern Egypt, attended by presidents of other African nations, including Chad, Niger and Nigeria. Officials from the UK and US were also present. "There is no substitute for combating terrorism in African countries," Sall said, adding that fighting terrorism consumes 18-24 percent of the African continent's budget, resulting in deficit. At the forum's inauguration ceremony, Egyptian President Abdel Fattah al-Sisi also called for "decisive and collective action against countries supporting terrorism around the world". During his speech, he said that numerous African countries are blighted by terrorism, highlighting the Sahel and Horn of Africa regions as among the most affected. Nigerian President Muhammadu Buhari also called for a focus on conflict prevention in Africa, adding that the continent needs to invest more in education.

### FCO updates Africa travel advice

The UK Foreign and Commonwealth Office (FCO) has updated its advice for travel to Nigeria as it's believed that terrorists are "very likely" to try to carry out attacks in the country. Most attacks occur in the North-East, particularly in Borno, Yobe and Adamawa states. As of December, it advises against all travel to Borno, Yobe, Adamawa and Gombe states, and within 20km of the border with Niger in Zamfara state. Additionally, it recommends all but essential travel to the following Nigerian states: Bauchi, Zamfara, Kano, Kaduna, Jigawa, Katsina, Kogi and Abia. Since January 2018, the Islamic Movement of Nigeria has protested regularly in central Abuja and other cities. Such protests, particularly in Abuja, have the potential to turn violent, the FCO warns. It adds that additional checks are in place at the Nigeria-Benin international border at Seme, Lagos state. There have also been changes to travel advice regarding Mozambique. The FCO advises against all but essential travel to the districts of Nangade, Quissanga, Ibo, Macomia, Mocimboa da Praia, Palma and Meluco in Cabo Delgado province, Mozambique, including the islands off the coast, due to attacks by groups with links to Islamic extremism.

### Three African countries in top 10 of Global Terrorism Index

Nigeria, Somalia and Democratic Republic of the Congo are ranked at third, sixth and 10th respectively in the 2019 Global Terrorism Index of 138 countries, published in November. Nigeria's ranking remains the same from the last Index, which measures the impact of terrorism, but the other two African countries have each risen a position. Deaths from terrorism in Nigeria rose to 2,040 in 2018 – a 33 percent increase. According to the report, this increase was due to a substantial escalation of violence by Funali extremism. Following its deadliest year on record in 2017, Somalia recorded the second-largest reduction in terror-related deaths in 2018, behind only Iraq. Meanwhile, the Democratic Republic of the Congo recorded 135 incidents, 410 deaths and 145 injuries in 2018. Boko Haram is ranked among the four deadliest terrorists groups, alongside the Taliban, ISIL and the Khorasan Chapter of the Islamic State. Terrorism-related deaths committed by Boko Haram dropped by 42 percent in 2018 compared with the previous year – an 89 percent decline from their peak in 2014. Consistent with previous years, about 85 percent of attacks in 2018 were in Nigeria.

### Cyber attack education urgently needed in Africa

Published in December, the African Cybersecurity Awareness Report by integrated security awareness training and simulated phishing platform KnowBe4 shines a light on the pressing need to educate Africans to different types of cyber attack. More than 800 respondents across eight countries in Africa – South Africa, Kenya, Nigeria, Ghana, Egypt, Morocco, Mauritius and Botswana – participated, and the white paper's statistics reveal how much work in security awareness still needs to be done throughout the continent. For example, 53 percent of Africans surveyed think that trusting emails from people they know is good enough and 64 percent don't know what ransomware is – but believe they could easily identify a security threat. Furthermore, 28 percent have fallen for a phishing email and 50 percent have had a malware infection.

### BUI opens cyber security centre in South Africa

Johannesburg-based security solutions provider and official Microsoft Partner BUI has opened a state-of-the-art cyber security centre. Described by BUI as "a dedicated cyber security facility that leverages the intelligent cloud to help safeguard business organisations" and staffed round the clock by certified consultants, the BUI Cyber SoC facility is backed by world-class Microsoft security technology, including Azure Sentinal – the tech giant's cloud-native security information and event management software. "The combination of cutting-edge technology, industry-leading skills and award-winning service is what makes our Cyber SoC so distinctive," explained BUI security manager Hilton Ashford. "It's a cyber security resource unlike any other in South Africa. We aim to provide a comprehensive, compelling solution for organisations for their digital security. There's a new headline about cyber crime almost every day. And as the threats evolve, so too must our responses." The BUI Cyber SoC uses multiple data sources – on-premises or in any cloud – to monitor business environments continuously. Its system integrates with existing applications and products, including other security products and platforms, as well as custom enterprise tools to provide a robust security overview. Commenting on the new centre, Ashford also stressed that "effective cyber security is not a one-time operation" and that safeguarding sensitive data requires constant vigilance.

LOGOS IMAGING

Rugged, Reliable, Portable X-ray Solutions for Security Users Worldwide

NEOS III

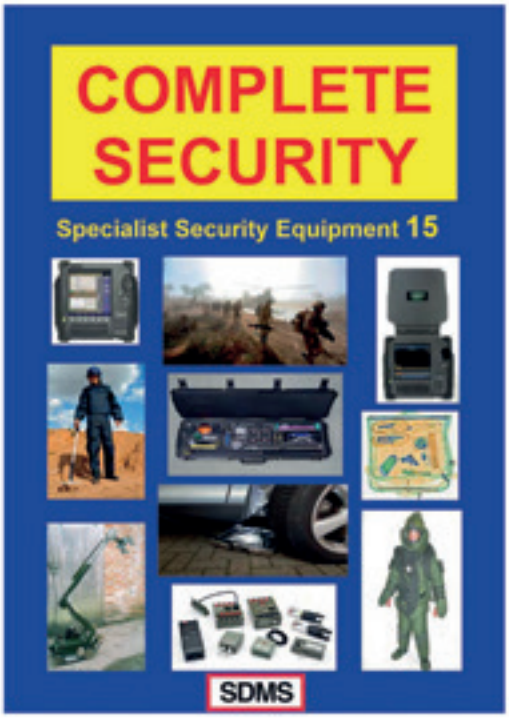
Logos Imaging's Small Format DR System

PRÓTOS

Logos Imaging's Ultra-portable DR System

(866) 939-4044
sales@logosimaging.com
WWW.LOGOSIMAGING.COM

## SUPPLIERS OF ANTI-TERRORIST EQUIPMENT




SDMS are suppliers of anti-terrorist and internal security equipment to the governments of over 130 countries worldwide, as well as to many large corporate clients. We supply top-quality equipment at highly competitive prices. Most equipment is also supplied on our "sale or return" basis whereby, if a client is not completely satisfied with equipment we have supplied, it can be returned to us for a complete refund.

SDMS also undertakes specialist training assignments, utilising some of the UK's most experienced and highly qualified ex-government instructors.

* Anti-terrorist
* Surveillance
* Methods of entry
* Search - explosives, weapons and drugs
* Personal protection
* Counter-surveillance
* Property protection
* Police & special forces
* Training

SDMS Security Products UK Limited, Elysium House, 126-128 New Kings Road, Fulham
LONDON SW6 4LZ
Tel: +44 (0)20 7731 8417 Fax: +44 (0)20 7610 9927 Email: sales@sdms.co.uk

# NEWS

## Asia

### ASD director-general announced

Rachel Noble has been appointed the new director-general of the Australian Signals Directorate, which intercepts electronic communications from foreign countries. Noble leaves her role as head of the Australian Cyber Security Centre (ACSC) – where she is responsible for leading the Australian Government's cyber security capabilities, responding to cyber security threats and incidents, and collaborating with Government, industry and the community on cyber-security matters. Not only the first woman to be appointed to lead ASD, Noble is also the first woman to head a major intelligence agency in Australia, and steps into the role in February. "Noble's deep experience in intelligence strongly positions her to lead ASD in executing its important national security mission," Prime Minister Scott Morrison said. "She has vital technical expertise having previously worked in ASD and has a strong understanding of the role the organisation plays in the National Intelligence Community. ASD plays a critical role in supporting the Australian Government and the Australian Defence Force through intelligence, cyber security and offensive operations, defending Australia from global threats while advancing our national interests."

### Deutsche Telekom AG opens SOC in Singapore

Good news for APAC: Deutsche Telekom AG has opened a new cyber defence and security operation centre (SOC) in Singapore. The new facility is only slightly smaller than the SOC in Bonn, Germany, which is Europe's largest security operation centre. Its team will now observe the Asia-Pacific (APAC) region round the clock for known malware and anomalies. Responding to the constant evolution of the cyber security landscape, SOCs use Deutsche Telekom's Correlated Data Feeds to detect attacks at an early stage. "We are proud to bring our state-of-the-art technology and German data privacy standards to Asia in order to make our customers more secure in real time," said head of Telekom Security, Dirk Backofen. "Our 17 integrated cyber defence and security operation centres around the globe are interconnected. They analyse up to 2.5-billion security-relevant events per day in more than 3,300 data sources. Pre-stages of artificial intelligence help us to do this." Its 'Sharing is for Caring' initiative also brings together security and incident response teams to improve the exchange of threat information. The coalition consists of cyber security industry heavyweights such as FIRST.org, Cyber Security Sharing & Analytics and Trusted Introducer.

### Indian Railways propose introducing facial recognition

Indian Railways is planning to roll out facial recognition and artificial intelligence technology at train stations. Reportedly, the Railway Protection Force (RPF) – Indian Railways' security arm – aims to link its proposed system with existing criminal databases from the Crime and Criminal Tracking Network and Systems using bridge software. "With this, we will have access to a huge database of criminals and our facial recognition system software can easily be used to fetch photos of potential criminals and match faces," an RPF official explained. "If we are able to install this across all our major stations, it will be a huge security breakthrough. This is preventive policing." The proposals are controversial, however: concerns have been raised that this may not only violate passenger privacy, but also put their data at risk. "For now this is completely illegal, as there is no legal authority or framework for any such projects which are being tested as well as already deployed in India," said Apar Gupta, executive director of the Internet Freedom Foundation, a non-Government organisation that works for online freedom.

### EY Australia acquires Aleron

Ernst & Young Australia has acquired Sydney-based cyber consultancy Aleron. The move strengthens EY's position as the largest cyber security provider in the Australian professional services sector. Aleron specialises in cyber security strategy, architecture design and implementation across a broad range of sectors including financial services, retail and government. As part of the acquisition, EY will acquire Aleron's cyber security analytics and risk reporting platform – eDNA – a tool that enables companies to view the health of IT systems in real-time and identify where to focus efforts and budget to reduce cyber risk. EY plans to scale the platform globally in addition to its existing suite of cyber security capabilities. Anthony Robinson, EY Oceania Cybersecurity Leader, said the acquisition strengthens the firm's position as the largest cyber-security provider in the professional services sector: "The acquisition of Aleron will build on our growing capability to deliver end-to-end cyber resilience for clients as they embrace new and disruptive technologies such as cloud, robotics and internet of things."

### Australia invests $15-million into anti-terror database

South Australia plans to pump $15-million into a new computer system to monitor potential terrorists more effectively. The system, expected to be rolled out at the end of 2020, aims to ensure that sensitive information about offenders is accessible by all law-enforcement agencies throughout the region and across the entire country during operations. According to Police Minister Corey Wingard, the new system will allow correctional services officials to improve the collection, sharing and storage of details of offenders that could help to prevent future crimes and potential terrorist attacks. The Government is expected to select a supplier for the system in the second half of 2020. "There have been a number of high-profile terrorism incidents in Australia in which the offenders were known to correctional services," Wingard explained. ""An inquiry following the Lindt Cafe siege (in Sydney in 2014) made several recommendations relating to information sharing and proposed, among other things, a new system to enable the speedy transfer of data from one agency to other relevant agencies that might assist in the response to an act of terrorism."

# DIARY DATES

## 2020 Conference and Exhibition planner

### 3-4 February Network Centric Warfare 2020
Rome, Italy
Organiser: SMi
Tel: +44 (0)20 7827 6000
Email: events@smi-online.co.uk
www.smi-online.co.uk

### 18-20 February GPEC 2020
Messe Frankfurt, Germany
Organiser: EMW Exhibition & Media Wehrstedt GmbH
Tel: +49 34 743 62 090
Email: info@gpec.de
www.gpec.de

### 4-5 March Enforce Tac 2020
Nuremberg, Germany
Organiser: OTSA Ltd
Tel: +44(0)207 886 3121
Email: marleen.meyer@otsa.net
www.enforcetac.com

### 15-16 April International Disaster Management Exhibition 2020
ExCel, London
Organiser: IDME
Email: ryan@idme.london
www.idme.london/

### 28-30 April The Security Event 2020
Birmingham NEC, UK
Organiser: Western Business Exhibitions Ltd
Tel: +44 (0)7552 237848
Email: tristan@thesecurityevent.co.uk
www.thesecurityevent.co.uk

### 19-21 May IFSEC International 2020
ExCel, London
Organiser: IFSEC International
Tel: +44 (0)20 7921 8166
Email: ifseccustomerservice@ubm.com
www.ifsec.events/international

### 19-21 May Counter Terror Expo 2020
ExCel, London
Organiser: Clarion Defence and Security Ltd
Tel: +44 (0) 20 7384 8232
Email: sales@counterterrorexpo.com
www.ctexpo.co.uk

### 8-12 June Eurosatory 2020
Paris Nord Villepinte Exhibition Center, France
Organiser: COGES
Tel: +33 (0)1 44 14 51 06
Email: visit@eurosatory.com
www.eurosatory.com

### 15-20 June Interschutz 2020
Hannover, Germany
Organiser: Deutsche Messe
www.eurosatory.com


MCQUEEN TARGETS

LIVE FIREARMS TRAINING TARGETRY

THREAT ASSESSMENT TARGETS

Various hostile/non hostile situations can be created by using the overlay solutions. All targets are designed to fit onto standard NATO backing boards – 458mm x 1143mm (18" x 45").

LIFESIZED 3D FOAM TARGETS

Manufactured in separate parts with repairable foam to withstand 3-4000 rounds. Create your own realistic shoot/no shoot scenario's. Full range of replica accessories available.

STANDARD POLICE AND MILITARY TARGETS


McQUEEN TARGETS, Nether Road, Galashiels, Scotland, UK, TD1 3HE
Tel: +44 (0) 1896 664269 Email: targets.ukgal@sykes.com W: www.mcqueentargets.com

ALL PRODUCTS HOSTILE VEHICLE MITIGATION APPROVED ANTI-TERRORIST BARRIERS


Safetyflex Barriers at Redfern Station in Sydney, Australia.

# Safetyflex Barriers

**A world-leading British manufacturer of anti-terrorism security measures acclaimed for its innovative products could be setting a new design trend with its latest project in Australia.**

Bollards made by Coventry-based Safetyflex Barriers have been given a striking makeover for an installation to help secure one of the busiest railway stations in Sydney from potential vehicle attacks.

Indigenous artists have put their stamp on the bollards outside Redfern Station, a major transport hub within the inner-city suburb with more than 70,000 journeys a day, which can stop attacks from vehicles travelling up to 80mph.

The installation at Redfern Station was carried out as part of a new entrance being created by the News South Wales Government to improve the movement and safety of passengers.

The heritage-listed station has strong ties with the local Aboriginal community which has been reflected in the design of the new entrance and the bollards.

The artists have transformed the look of the slim line steel bollards with Aboriginal symbols to mirror designs on the windows within the entrance.

It is the latest project to have been completed with Australian distributors EZI Security Systems as Safetyflex Barriers continues to expand its global reach as a leading force in providing preventative measures to counteract terrorist threats.

Marcus Gerrard, director at Safetyflex Barriers, said: "We have a growing presence in Australia and are helping to secure numerous locations there to protect people and key locations from potential vehicle attacks.

"This was a particularly enjoyable project as it formed part of major improvement works to a high-profile station in Sydney and involved local Aboriginal artists transforming our bollards.

"Aside from providing superior protection against terror threats involving vehicles, our bollards have a stylish aesthetic which means they do not detract from the appearance of sites they help secure.

"This is the first time that our bollards have been given a makeover but the resulting design makes a fantastic statement in reflecting the culture of the local community and the new look of the station entrance.

"The feedback has been great and we are expecting this to signal an exciting new trend with more locations that we are working with both in the UK and overseas looking to put their own stamp on our bollards to reflect their identity and surroundings."

The company's innovative range of barriers and bollards help to secure areas at risk such as shopping centres, sports stadiums, government and military buildings, utilities and key infrastructure centres.

It has recently been recognised with the ADS Security Innovation Award by the Home Office, and Product of the Year Award at the Australian Security Industry Awards.

**02476 662116**
**www.safetyflexbarriers.com**

safetyflex
ANTI-TERRORIST BOLLARDS BARRIERS & CRASH FENCES

MGT europe
Bespoke Surveillance & Counter Surveillance Electronics

Unit 12, Hamilton Business Park
Stirling Way - Borehamwood
Hertfordshire, WD6 2FR
London - UK

www.mgteurope.com info@mgteurope.com

# MGT NOTE-33

## *DIGITAL STEREO AUDIO RECORDER*



## *FEATURES*

- *Digital stereo audio recording to removable Micro SD Card.*
- *Dust protected Micro SD Connector.*
- *Compact sturdy aluminum case.*
- *Easy to use and set-up with Windows PC software or Android App.*
- *Android App for recorder settings and audio listening (through USB OTG cable).*
- *Headphone output for audio quality check.*
- *Cable remote control switch.*
- *Uncompressed, best quality audio files with embedded time and date (.WAV file format).*
- *Low power high SNR audio Codec.*
- *Differential (balanced) microphone audio inputs.*
- *Manual and automatic microphone gain control (AGC).*
- *Optional audio files encryption (AES 256).*
- *High quality, reliable LEMO connectors for microphone inputs.*
- *One button recording start-stop.*
- *Recording initiated by button, voice activation, schedule or remote switch with cable.*
- *Line level possible with adapter (ll-36-p).*
- *Audio playback using (CTL-44-P adaptor).*

© MGT Europe
Unit 12, Hamilton Business Park, Stirling Way, Borehamwood, Hertfordshire, WD6 2FR - London - UK
T: +44 (0) 208 207 0079 - F: +44 (0) 208 953 9162 - M: +44 (0) 7770 390 324

# SHOWCASE

## Meesons unveils UK's slimmest speed gate

Meesons unveiled its new EasyGate Superb at this year's International Security Expo in London. EasyGate Superb is an ultra-slim, fully customised Speed Gate that is an ideal solution for controlling access to offices, schools, universities or government buildings and at 99mm, its cabinets are the slimmest of any speed gate on the market. The range includes unique and innovative features, such as an optional integrated card collector and QR code/ barcode reader. EasyGate Superb can be specified in colours to match a customer's corporate identity. The EasyGate Superb is the only Speed Gate on the market with such a slim design featuring the ability to integrate an optional card collector with a card return function. Where required, a third-party card reader can be built into the EasyGate Superb. The QR scanner, another optional feature, will help improve the efficiency of visitor management making, it possible for an external visitor to receive a QR code on their mobile phone – allowing unimpeded entry to the facility on arrival without having to verify credentials.

## Abloy sets new standard for padlocks

Abloy UK has announced its PL330 padlock has achieved the highest rating during testing to simulate a criminal attack. The PL330 extends Abloy's padlock range to achieve LPS 1654. The padlock achieved a 1+ rating from the Loss Prevention Certification Board against standard LPS 1654, which focuses on the time taken to compromise a padlock and gain access to the asset it is securing. A '1' grade replicates an opportunist attack by physical force or stealth, while the '+' symbol indicates that the padlock's key mechanisms are resistant to manipulation methods outlined in Annex A.6 of BS 3621:2007 and LPS 1242: Issue 2. Abloy's PL330 padlock is protected by a hardened, free-spinning protection plate that prevents drill bits from penetrating the lock. The design also includes stainless ball bearings that lock the shackle at both ends, and a rotating disc cylinder system, which means it is effectively pick proof. The padlock is available with award-winning PROTEC, PROTEC2, PROTEC2 CLIQ and SENTRY mechanisms, and can be master-keyed with door cylinders.

## Elbit Systems introduces MAGNI

Elbit Systems has launched MAGNI, a fully autonomous and robust Multi-Rotor Vertical take-off and landing unmanned aerial system designed to enhance the situational awareness capabilities of mobile forces. Compact and lightweight (2.5kg) MAGNI enables rapid deployment and launch (in less than one minute) from any combat vehicle, transforming it to an effective intelligence-gathering platform. The MAGNI system includes a thermal payload, communications suite (dual S-Band or LTE), automatic co-ordinate tracking capability and built-in interface with battle management systems. Carrying up to 350g of payloads it offers a range of up to 3km, a maximum operational altitude of 4,000ft and 30 minutes of endurance. Operated by a single user, MAGNI enables vehicle-mounted forces to generate beyond-the-hill visual intelligence during day and night and seamlessly feed target information to command and control systems. Its unique size, weight and power parameters make it well suited for squad, platoon and company levels.

## Security innovation makes bridges safer

An innovative bridge protection system, which can withstand the force of a 7,500kg truck travelling at 30mph, is now available to protect pedestrians from vehicle ramming attacks. The Bridge Protection System has been developed by ATG Access and allows bollards to be fitted into a shallow foundation structure, making it uniquely suitable for bridge protection. With its foundation depth of just 40mm, minimal excavation is required and the structural integrity of the bridge is maintained. The system has been successfully tested to both the IWA 14 and PAS 68 standards, stopping 7,500kg vehicles travelling at 30mph with less than 0.5m of penetration. While the system was tested with ATG Access' Westminster high security bollard, the foundation and socket can also be used with other bollard types and shapes to suit individual security and aesthetic requirements. Robert Ball, engineering director at ATG Access, told *Intersec*: "Our Bridge Protection System is an industry first, and will help to safeguard the general public by both deterring potential perpetrators from attempting to commit these ramming attacks."

## Meprolight showcases ultra-smart solutions

Manufacturer of electro-optical systems, thermal and night vision equipment, Meprolight, introduced its multi-spectral MEPRO NYX 200 uncooled thermal sight, MEPRO FORESIGHT and MEPRO MicroRDS sight at Milipol Paris in November. The MEPRO NYX-200 is available in two configurations: thermal channel with digital low-light camera or thermal channel with digital day camera, enabling operation in harsh sight conditions such as total darkness, smoke and fog. By combining a thermal channel and digital day camera, it can be used as a sight for both day and night operations – eliminating the need to change sights. The MEPRO FORESIGHT is an augmented sight, which provides essential tactical data projected directly on its transparent optical lens in real time and equipped with a digital zeroing mechanism. The sight is integrated with Meprolight's mobile App (Android and iOS) through a Bluetooth interface, enabling storage and easy upload of up to 10 preset weapon zeroing settings or user profiles. Finally, the MEPRO MicroRDS offers rapid target acquisition at close distances with both eyes open and is designed for pistols and small arms. It serves as either the main weapon's aiming sight or as a backup sight for rifles' magnifying optics.

# SMART SECURITY SOLUTIONS

**DTP 320DV**

DUAL VIEW PASSENGER VEHICLE AND VAN
X-RAY INSPECTION SYSTEM

**DTP 7500LVR**

RELOCATABLE VEHICLE X-RAY INSPECTION SYSTEM

AI POWERED

TRANSMISSION X-RAY TECHNOLOGY

AI ARTIFICIAL INTELLIGENCE

**CONPASS SMART 5AI**

UNIQUE HIGH INSPECTION SPEED BODYSCANNER

**BV STREAM**

SMART, SIMPLE AND FLEXIBLE THREAT IMAGING
SOLUTION FOR SCHOOLS, UNIVERSITIES, HOTELS,
CASINOS, RESTAURANTS AND OTHER PUBLIC ESTABLISHMENTS

0480-SPI5112019

## X-RAY SECURITY SCREENING SYSTEMS

info@adanisystems.com
www.adanisystems.com

ADANI